universität wien

MASTERARBEIT / MASTER'S THESIS

Titel / Title

„$e^{\pi\sqrt{163}}$ is almost an integer“

verfasst von / submitted by

Carol Soppelsa BSc.

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien / Vienna, 2025

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	UA 066 821
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Mathematik
Betreut von / Supervisor:	Mag. Dr. Harald Grobner Privatdoz.

Abstrakt

Eine der bemerkenswertesten Kuriositäten der Zahlentheorie ergibt sich aus dem Wert

$$e^{\pi\sqrt{163}} \approx 262\,537\,412\,640\,768\,743.99999999999925,$$

der erstaunlich nahe an einer ganzen Zahl liegt. Auf den ersten Blick mag dies wie ein bloßer numerischer Zufall erscheinen, doch tatsächlich spiegelt es tiefe Zusammenhänge zwischen algebraischer Zahlentheorie, Modulfunktionen und der Theorie elliptischer Kurven wider. Diese Arbeit untersucht diese Zusammenhänge anhand der Betrachtung elliptischer Kurven mit komplexer Multiplikation, der Arithmetik von Modulfunktionen und expliziten Konstruktionen von Klassenkörpern über die Kubikwurzel der j-Funktion, γ_2. Durch die Kombination analytischer und algebraischer Techniken werden die Integritätseigenschaften relevanter Modulinvarianten gezeigt und erläutert, wie diese Ergebnisse die nahezu ganzzahlige Erscheinung von $e^{\pi\sqrt{163}}$ erklären.
Als motivierende Perspektive wird in der Fachliteratur häufig betont, dass jeder Mathematiker zumindest einmal eine klare Erklärung für dieses Phänomen kennenlernen sollte. Ziel der vorliegenden Arbeit ist es, zu einem solchen Verständnis beizutragen.

Abstract

One of the most remarkable curiosities in number theory arises from the value

$$e^{\pi\sqrt{163}} \approx 262\,537\,412\,640\,768\,743.99999999999925,$$

which comes astonishingly close to being an integer. At first sight this appears to be a mere numerical coincidence, but in reality it reflects deep connections between algebraic number theory, modular functions, and the theory of elliptic curves. This thesis explores these connections through the study of elliptic curves with complex multiplication, the arithmetic of modular functions, and explicit constructions of class fields via the cube root of the j-function, γ_2. By combining analytic and algebraic techniques, we establish the integrality properties of relevant modular invariants and demonstrate how these results explain the near-integrality of $e^{\pi\sqrt{163}}$.

As a motivating perspective, it has frequently been emphasized in the literature that every mathematician should at least once encounter a clear explanation of why this phenomenon holds. The aim of the present work is to contribute to such an understanding.

Acknowledgements

First and foremost, I would like to express my deepest gratitude to my supervisor, Mag. Dr. Harald Grobner, for their invaluable guidance, insight, and patience throughout this project. Their expertise, thoughtful feedback, and careful attention to detail have been essential in shaping both the content and clarity of this thesis. Beyond their academic guidance, their encouragement and support helped me navigate the most intricate aspects of the subject, instilling confidence in my work and helping me bring it to its final form. I am truly grateful for their mentorship, which has made this journey both intellectually stimulating and deeply rewarding.

Words cannot express how profoundly grateful I am to my family. Their unwavering love, support, and encouragement have been my anchor throughout this journey. They celebrated my successes, no matter how small, and provided comfort and reassurance during moments of doubt. They patiently listened to my endless musings about mathematical challenges, offered thoughtful advice when I needed it most, and reminded me to take a step back and breathe when the work felt overwhelming. Their belief in me and their constant presence have shaped who I am today and made this thesis not only possible but deeply meaningful. I am endlessly thankful for the warmth, patience, and care they provided, which transformed what could have been a solitary and demanding endeavour into a journey filled with love, support, and inspiration.

I would like to thank my friends for their companionship, encouragement, and support throughout this journey. In particular, I am especially grateful to Benjamin, whose love, patience, and shared curiosity have been a constant source of strength. His countless stimulating discussions, thoughtful suggestions, and unwavering support during an especially stressful time in my life helped me stay motivated, discover confidence in myself during the most challenging moments, and approach this work with both dedication and lightness. His presence has made this journey not only deeply enriching but truly memorable.

I would also like to acknowledge my cat, whose playful curiosity, comforting presence, and occasional interruptions provided both amusement and emotional support throughout this journey. Their companionship reminded me to pause, smile, and find joy in small moments, even during the most intense days of research.

Above all, this thesis has been more than an academic endeavour - it has been a journey that fostered personal growth. It has given me confidence, resilience, and a deeper understanding of my own capabilities, lessons that will stay with me far beyond the completion of this work. I am grateful not only for the knowledge I have gained but also for the perspective, strength, and self-assurance this journey has brought me.

Contents

Introduction

In April 1975, Martin Gardner amused the readers of *Scientific American* (a popular-science magazine) with a clever prank: he claimed that the number

$$e^{\pi\sqrt{163}}$$

was exactly an integer, attributing this remarkable fact to a result mentioned by the Indian mathematician S. Ramanujan in his 1914 paper (see [5, p. 126]). A few months later, Gardner admitted that it had been an April Fools' joke. Yet the claim, though playful, was not entirely unfounded: the number is astonishingly close to the integer

$$262537412640768744,$$

differing from it by less than a trillionth. In number-theoretic terms, this makes it an example of an "almost integer", a number whose distance to the nearest integer is extraordinarily small.

The reference to Ramanujan's paper was, however, legitimate. In his 1914 work on modular equations and approximations to π ([9]), he had already observed such almost integers, noting values like $e^{\pi\sqrt{58}}$ and $e^{\pi\sqrt{67}}$. He was fully aware that none of these values were actually integers. Later, the remarkable value $e^{\pi\sqrt{163}}$ emerged as an extreme example of this phenomenon and came to be known as *Ramanujan's constant*. What may first appear to be a numerical coincidence in fact reflects deep connections between algebraic number theory, modular functions, and elliptic curves. The goal of this thesis is to explain, step by step, the mathematical structures underlying this phenomenon, highlighting its deep connections with the theory of complex multiplication.

The underlying theme of this work is the remarkable interplay between three perspectives on the same objects

- *Analytic*, through lattices in $\mathbb{C}$ and the associated elliptic functions such as the Weierstrass $\wp$-function and its companions.
- *Geometric*, via elliptic curves realized as quotients of $\mathbb{C}$ by a lattice.
- *Algebraic*, through the arithmetic of imaginary quadratic fields, orders, and their class groups.

The theory of complex multiplication lies precisely at the intersection of these perspectives, providing both a conceptual explanation and concrete formulas.

The central theorem around which this thesis is built is the *First main theorem of complex multiplication*. It establishes a precise link between the Galois action on j-invariants of elliptic curves with complex multiplication and the action of the ideal class group of an imaginary quadratic order. This fundamental result not only explains the algebraicity of certain modular invariants but also leads to explicit class field constructions. In the case of discriminant -163, these ideas culminate in the near-integrality of $e^{\pi\sqrt{163}}$.

Overview of the thesis. The presentation is organized into seven chapters, each developing a key part of the argument explaining the remarkable value $e^{\pi\sqrt{163}}$.
Chapter 1 is mainly devoted to recalling basic results that provide the foundation for many of the discussions in the later chapters.
Chapter 2 introduces lattices in the complex plane and explains how they give rise to elliptic curves, thereby establishing the analytic-geometric dictionary that underlies much of the later theory. This correspondence not only provides intuition but also equips us with concrete tools to pass between algebraic and analytic viewpoints.
Chapter 3 develops the theory of complex multiplication. Here we describe elliptic curves whose endomorphism rings are larger than usual and show how such curves are organized by the ideal class group of imaginary quadratic orders. This chapter makes the arithmetic structure encoded in the geometry of elliptic curves precise.
In Chapter 4 we turn to modular functions. Starting with congruence subgroups and the classical j-function, we study how these functions generate fields of modular functions and how their algebraic properties connect with the arithmetic of elliptic curves. This prepares the ground for studying elliptic curves and their invariants within a number-theoretic framework.
Chapter 5 is devoted to the proof of the First main theorem of complex multiplication, a central result of the subject. This theorem describes in exact terms how the Galois action on elliptic curves with complex multiplication corresponds to the action of the ideal class group, thereby forging a deep link between geometry and arithmetic.
Building on this foundation, Chapter 6 introduces a specific cube root of the j-function, denoted γ_2. This function, though less classical than j, plays a crucial role in explicit class field theory: its values generate ring class fields in cases where the classical j-invariant does not generate the full field.
In Chapter 7 we address the integrality of the Fourier coefficients of the j-function by constructing γ_2 algebraically and relating it to j. While the integrality result already suffices for the main goal of the thesis, the construction also yields explicit formulas for γ_2, making the final conclusions especially transparent and bring the analytic and arithmetic viewpoints together in a concrete way.
Finally, Chapter 8 brings together all the previous results. Using the explicit formulas developed in the previous chapter, we numerically evaluate $\gamma_2(\tau)$ at the imaginary quadratic arguments corresponding to orders of class number one. This allows us to deduce the extraordinary near-integrality of $e^{\pi\sqrt{163}}$ and to conclude the thesis by illuminating how the abstract theory of complex multiplication explains one of the most remarkable numerical phenomena in number theory.

1 Preliminaries

As a preparation for the upcoming sections, we summarize some classical results and theorems. These will provide the necessary groundwork for our subsequent discussions.

Theorem 1.0.1 (Bolzano-Weierstraß)**.** *Every bounded sequence in $\mathbb{R}^n$ has a convergent subsequence.*

Proof. A proof can be found in [10, Thm. 2.42]. □

Theorem 1.0.2 (L'Hôpital's rule)**.** *Let I be an open interval and let c be an accumulation point of I (possibly $c = \pm\infty$). Let f and g be real-valued functions differentiable on $I \setminus \{c\}$, with $g'(x) \neq 0$ for all $x \in I \setminus \{c\}$. Assume that the limit*

$$\lim_{x\to c} \frac{f'(x)}{g'(x)} = L \in \mathbb{R} \cup \{\pm\infty\}$$

exists. If either

$$\lim_{x\to c} f(x) = \lim_{x\to c} g(x) = 0 \quad \text{or} \quad \lim_{x\to c} |g(x)| = \infty,$$

then

$$\lim_{x\to c} \frac{f(x)}{g(x)} = L.$$

The limit may be one-sided ($x \to c^+$ or $x \to c^-$) if c is a finite endpoint of I.

Proof. A proof can be found in [10, Thm. 5.13]. □

Theorem 1.0.3 (Cauchy's residue theorem)**.** *Let Ω be a simply connected open subset of $\mathbb{C}$, let U be a finite set of points in $\mathbb{C}$, $U_0 = \Omega \backslash U$ and let f be a holomorphic function on U_0. Let C be a positively oriented simply closed curve and denote by $\mathrm{Res}(f, p)$ the residue of f at the point $p \in U$. Then*

$$\sum_{p\in U} Res(f, p) = \frac{1}{2\pi i} \int_C f(z)\, dz.$$

Proof. See [2, Thm. 2.2]. There the general form of the residue theorem is established using winding numbers. Our formulation is the special case where C is a positively oriented Jordan curve, so the winding numbers reduce to 0 or 1. □

Theorem 1.0.4 (Cauchy criterion for series)**.** *Let $(a_n)_{n\geq 1}$ be a sequence in a complete metric space. Then the series $\sum_{n=1}^{\infty} a_n$ converges if and only if for every $\varepsilon > 0$ there exists $N \in \mathbb{N}$ such that for all $m > n \geq N$,*

$$\left| \sum_{k=n+1}^{m} a_k \right| < \varepsilon.$$

Proof. For a proof see [10, Thm. 3.22]. □

Theorem 1.0.5. *Let $(f_n)_{n\in\mathbb{N}}$ be a sequence of holomorphic functions on an open set Ω that converges uniformly to a function f on every compact subset of Ω. Then f is holomorphic on Ω.*

Proof. For a proof see [1, Thm. 5.1]. □

Theorem 1.0.6 (Liouville)**.** *Let f be a holomorphic and bounded function on $\mathbb{C}$. Then f is constant.*

Proof. For a proof see [1, p. 122]. □

For a non-zero complex function $f(z)$ that is meromorphic on an open neighbourhood of a point $z_0 \in \mathbb{C}$, we define

$$\mathrm{ord}_{z_0}(f) \coloneqq \begin{cases} n & \text{if } f \text{ has a zero of order } n \text{ at } z_0 \\ -n & \text{if } f \text{ has a pole of order } n \text{ at } z_0 \\ 0 & \text{otherwise.} \end{cases}$$

By convention, $\mathrm{ord}_{z_0}(0) = \infty$.

Theorem 1.0.7 (Generalized argument principle)**.** *Let γ be a simple closed, positive oriented curve, let Γ denote its interior, and let f be a function that is meromorphic on an open set Ω containing γ and Γ. Assume that f has no zeros or poles on γ and let g be a non-zero holomorphic function on Ω. Then*

$$\frac{1}{2\pi i}\int_\gamma g(z)\frac{f'(z)}{f(z)}dz = \sum_{\omega\in\Gamma} g(\omega)\mathrm{ord}_\omega(f).$$

Proof. A proof can be found in [14, Thm. 14.17]. □

When $g(z) = 1$, we recover the classical argument principle:

Theorem 1.0.8 (Cauchy's argument principle)**.** *Let γ be a positive oriented Jordan curve, let Γ denote its interior and let f be a function that is meromorphic on an open set Ω containing γ and Γ. Assume that f has no zeros or poles on γ. Then*

$$\frac{1}{2\pi i}\int_\gamma \frac{f'(z)}{f(z)}dz = Z - P,$$

where Z and P denote the number of zeros and poles of f in Γ, counted with multiplicity.

Theorem 1.0.9 (Maximum modulus principle)**.** *Let $\Omega \subseteq \mathbb{C}$ be a connected open set, and let $f : G \to \mathbb{C}$ be holomorphic. If there exists a point $z_0 \in \Omega$ such that $|f(z_0)| \geq |f(z)|$ for all $z \in G$, then f is constant on Ω.*

Proof. For a proof, see [2, Thm. 6.1.1]. □

Theorem 1.0.10 (Primitive element theorem)**.** *Every separable field extension of finite degree is simple.*

Proof. For a proof see [4, Thm. 14.25]. □

Theorem 1.0.11 (Vieta's formulas, discriminant of a polynomial)**.** *Let* $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ *be a polynomial with* $a_i \in \mathbb{C}$ *for* $1 \leq i \leq n$ *and* $a_n \neq 0$*. Then we have*

(i) Let $e_1, e_2, \ldots, e_n \in \mathbb{C}$ *denote the (not necessarily distinct) roots of* $P(x)$*. Then the coefficients of* $P(x)$ *are related to its roots by*

$$\sum_{1 \leq i_1 < i_2 < \ldots i_k \leq n} \left(\prod_{j=1}^{k} e_{i_j} \right) = (-1)^k \frac{a_{n-k}}{a_n}.$$

(ii) The discriminant of $P(x)$ *can be expressed in terms of its roots and the Vandermonde determinant as*

$$\Delta(P) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (e_i - e_j)^2.$$

Proof. For a proof see [7, Exc. 33, p. 257-258]. □

2 The correspondence between lattices and elliptic curves

One of the central ideas in the theory of elliptic curves is that their geometry can be described both in algebraic and in analytic terms. Over $\mathbb{C}$, this dual perspective takes the form of a precise correspondence between elliptic curves and lattices, a theme that will guide this chapter. We will examine this correspondence in both directions: starting from a lattice, we construct the associated elliptic curve, and conversely, given an elliptic curve over $\mathbb{C}$, we recover a lattice that encodes its analytic structure.
The chapter is organized into five sections. The first two provide background material: we recall the basic definitions and properties of elliptic curves, and we introduce lattices and complex tori. In the third section, we develop the analytic side of the correspondence by constructing elliptic functions on the torus and showing how these functions define a corresponding elliptic curve. The fourth section describes explicitly the isomorphism between the complex torus and its associated elliptic curve, a construction that will also serve as an important tool later on. Finally, the fifth section treats the converse direction: starting from an elliptic curve over $\mathbb{C}$, we recover a lattice that produces it, thereby completing the picture. This framework provides the analytic foundation on which much of the later theory in this thesis will build.

The exposition in this chapter is inspired by [3, §10 A-B, §11 A] and has been expanded and supplemented with additional results and proofs following [14, Lec. 14, 15].

2.1 Elliptic curves

We begin by introducing elliptic curves, their basic properties, and how they are described algebraically. This will provide the necessary background and notation for the constructions that follow.

An *elliptic curve* is a smooth projective curve of genus one with a distinguished point.

Over a field K with $\mathrm{char}(K) \neq 2, 3$, every elliptic curve can be defined by the set of solutions (x, y) of an equation of the form

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

with coefficients $A, B \in K$ and $4A^3 + 27B^2 \neq 0$ with the K-rational projective point $(0 : 1 : 0)$. This equation is called a *(short) Weierstrass equation* and the elliptic curve is said to be in *Weierstrass form*. The curve is required to be *non-singular*, meaning that the curve has no singularities (cusps or self-intersections), which is assured by

the discriminant of the polynomial $x^3 + Ax + B$ being non-zero, i.e. by the equation $4A^3 + 27B^2 \neq 0$. Therefore is the number $-16(4A^3 + 27B^2)$ called the *discriminant of an elliptic curve*, where the use of the factor -16 will become clear later in this chapter. When the coefficient field has characteristic 2 or 3, this equation is not general enough to include all non-singular cubic curves, so its place is taken by the *general Weierstrass equation*

$$y^2 + a_1yxy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_i \in K$, which can be transformed through a chance of coordinates into the short Weierstrass equation whenever the characteristic is not 2 or 3. Indeed, two elliptic curves are called *isomorphic*, if their Weierstrass equations are related to each other by a change of variables of the form

$$\begin{aligned} x &\mapsto u^2x + r \\ y &\mapsto u^2y + su^2x + t \end{aligned}$$

with $u, r, s, t \in \overline{K}$ and $u \neq 0$.

Elliptic curves defined over a field K can be viewed in two complementary ways: as algebraic curves and as abelian groups. As algebraic curves, they are defined by polynomial equations of the form $y^2 = x^3 + Ax + B$ and studied using morphisms, such as *isogenies*

$$\phi : E_1 \to E_2,$$

which are surjective maps that preserve the algebraic structure of the curves. On the other hand, elliptic curves also possess a group structure, with points on the curve forming an abelian group under addition. The corresponding group homomorphism

$$E_1(\overline{K}) \to E_2(\overline{K})$$

is a map between the sets of points $E_i(\overline{K}) = \{(x, y) \in \overline{K} \times \overline{K} \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}$ on the respective elliptic curves over the algebraic closure $\overline{K}$. Thus, ϕ serves as a map between the algebraic curves and as a homomorphism between their group of points, linking the algebraic and group-theoretic perspectives of elliptic curves.

There is a rich theory of elliptic curves over the rational numbers, finite fields, and p-adic fields. However, we will focus instead on elliptic curves defined over the field of complex numbers.

2.2 Lattices in $\mathbb{C}$ and complex tori

We now turn to the analytic side of the correspondence. Central to this perspective are lattices in $\mathbb{C}$ and the complex tori they define, which provide the geometric framework for constructing elliptic curves analytically.

Definition 2.2.1 (Lattice in $\mathbb{C}$)**.** A lattice in $\mathbb{C}$ is an additive subgroup $L = [\omega_1, \omega_2] = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ of $\mathbb{C}$ generated by two complex numbers ω_1 and ω_2, which are linearly independent over $\mathbb{R}$.

The condition that ω_1 and ω_2 are linearly independent over $\mathbb{R}$ ensures that the lattice spans a two-dimensional real vector space, making it a full-rank lattice in $\mathbb{C}$, which in this case is of rank 2. The set $\{\omega_1, \omega_2\}$ is called a *basis* of L.

Now that we have defined a lattice in $\mathbb{C}$ it is useful to explore its geometric properties. Specifically, we are interested in understanding how the lattice points are arranged in the complex plane. To do this, we introduce the next definition, which helps to capture the repeating structure of the lattice in a well-defined region of the plane.

Definition 2.2.2 (Fundamental and period parallelogram)**.** For a lattice $L = [\omega_1, \omega_2]$, the set

$$P_0 = \{\lambda_1\omega_1 + \lambda_2\omega_2 \mid 0 \leq \lambda_1, \lambda_2 < 1\}$$

is called fundamental parallelogram for L.
More generally, a period parallelogram P is any translate of the fundamental parallelogram given by

$$P = P_0 + h,$$

with $h \in \mathbb{C}$.

For two lattices L_1 and L_2 in $\mathbb{C}$ with $L_1 \subseteq L_2$, the *index of* L_1 *in* L_2 is defined as the number of cosets of L_1 in L_2, i.e.

$$[L_2 : L_1] = |L_2/L_1|,$$

which equals the number of distinct translates of L_1 that partition L_2.
Note that this quantity is finite, as both lattices are of full-rank by definition.

The fundamental parallelograms allow us to interpret the index of two lattices in terms of volumes and determinants. Writing the basis vectors for a lattice $L = [\omega_1, \omega_2]$ in terms of real and imaginary parts, $\omega_1 = x_1 + iy_1$ and $\omega_2 = x_2 + iy_2$, then the *volume* of the fundamental parallelogram spanned by the vectors ω_1, ω_2 in $\mathbb{R}^2$ is given by the absolute value of the determinant of the matrix whose columns are given by their coordinates:

$$\mathrm{vol}(P_0) = \left|\det \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}\right| = |x_1y_2 - x_2y_1| = \mathrm{Im}(\omega_1\overline{\omega_2}).$$

Even though different bases can generate the same lattice, the volume is uniquely determined by L and is invariant under a change of basis.
Now, suppose $L_1 \subseteq L_2$. Then the fundamental parallelogram P_0' of L_2 is contained within the fundamental parallelogram P_0 of L_1, which means that each coset of L_1 in L_2 corresponds to a distinct copy of P_0' in P_0 and the total number of such cosets matches the ratio of their volumes, leading us to

$$[L_2 : L_1] = \frac{\mathrm{vol}(P_0)}{\mathrm{vol}(P_0')}.$$

To express this in terms of determinants, let M_1 and M_2 be the matrices whose columns are the basis vectors of L_1 and L_2 respectively. Since L_1 is a sublattice of L_2, each basis

vector of L_1 can be written as an integer combination of the those of L_2, i.e. there exists an integer matrix A, called *transition matrix*, such that

$$M_1 = M_2 A.$$

Taking determinants and using its multiplicative property, we obtain $\det(M_1) = \det(M_2 A) = \det(M_2)\det(A)$. Thus the index of L_1 in L_2 can also be expressed as

$$[L_2 : L_1] = \frac{|\det(M_1)|}{|\det(M_2)|} = |\det(A)|,$$

explaining the link between algebraic and geometric interpretation of the index of two lattices.

Since $\mathbb{C}$ is an abelian group under addition, all of its subgroups are normal. Therefore, for a lattice L in $\mathbb{C}$, we can consider the quotient group $\mathbb{C}/L$, called a *complex torus*. Viewing $\mathbb{C}$ and L as topological spaces with the usual Euclidean topology and the discrete topology respectively, this quotient is also a compact topological group.

A natural way to represent the quotient $\mathbb{C}/L$ is through a period parallelogram by identifying its opposite edges to form a torus. This construction associates the points of the parallelogram with those of $\mathbb{C}/L$.

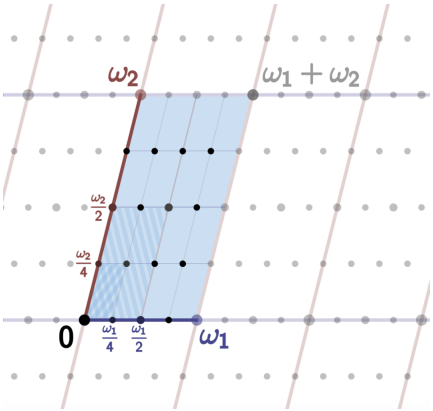

Figure 2.1: The complex torus associated to a lattice spanned by two periods ω_1 and ω_2. Corresponding edges are identified.
© Sam Derbyshire, *Lattice torsion points*, `https://commons.wikimedia.org/wiki/File:Lattice_torsion_points.svg`, accessed 13 Oct 2025. Licensed under CC BY-SA 3.0. Changes: none.

2.3 From lattices to elliptic curves

Having established the necessary background, we now develop one direction of the correspondence between lattices and elliptic curves by constructing, from a lattice L in $\mathbb{C}$, a corresponding elliptic curve. For this, we first introduce elliptic functions and Eisensteins series, then define the Weierstrass $\wp$-function, and finally show how any lattice naturally defines an elliptic curve over $\mathbb{C}$.

2.3.1 Elliptic functions and Eisenstein series

Having introduced lattices and complex tori, we now turn to the analytic tools that will allow us to construct elliptic curves explicitly. In particular, we study elliptic functions and Eisenstein series, which enrich these tori with additional structure and connect the analytic and algebraic viewpoints.

Consider the lattices $L = [\omega_1.\omega_2]$ and $L' = [1, \tau] = \{n + m\tau \mid n, m \in \mathbb{Z}\}$ in $\mathbb{C}$ with $\tau = \omega_2/\omega_1$ and consider the complex torus $\mathbb{C}/L'$. The bijective map $\mathbb{C} \longrightarrow \mathbb{C} : z \mapsto z\omega_1$ sends L' to L, so *multiplication-by-*ω_1 induces an isomorphism $\mathbb{C}/L' \cong \mathbb{C}/L$. This allows us to restrict our consideration to complex tori associated with lattices where $\omega_1 = 1$ and $\omega_2 = \tau$. Moreover, since the lattice generated by 1 and τ is the same as the lattice generated by 1 and $-\tau$, we may assume $\mathrm{Im}(\tau) > 0$.

Note that the complex structure on the torus depends on the lattice L. Also, the complex structure on $\mathbb{C}$ induces a complex structure on the quotient space $\mathbb{C}/L$, ensuring that the projection map $\pi : \mathbb{C} \longrightarrow \mathbb{C}/L$ is holomorphic.
For a fixed lattice $L = [1, \tau]$ and its associated complex torus $\mathbb{C}/L$ with projection map π, a function $f : \mathbb{C}/L \longrightarrow \mathbb{C}$ is meromorphic if and only if the composition $f \circ \pi : \mathbb{C} \longrightarrow \mathbb{C}$ is meromorphic, by definition of a complex structure on $\mathbb{C}/L$. We deduce that meromorphic functions on $\mathbb{C}/L$ correspond to meromorphic functions on $\mathbb{C}$, which are invariant under translation by elements of the lattice L, also referred to as *L-periodic*.

Definition 2.3.1 (Elliptic function)**.** An elliptic function for a lattice L is a meromorphic function f on $\mathbb{C}$, which is periodic with respect to L, i.e. $f(z + \omega) = f(z)$ for all $z \in \mathbb{C}$ and $\omega \in L$.

Note that if f is an elliptic function for L, then it is also elliptic for every sublattice of L, since it remains doubly periodic with respect to a finer lattice.
Moreover, sums, differences, products and quotients (as long as the denominator is not identically zero) of elliptic functions for L are again elliptic functions for L. Thus, the set of elliptic functions for a fixed lattice L forms a field, which we denote by $\mathbb{C}(L)$.

We conclude that since the points in any period parallelogram correspond to those in $\mathbb{C}/L$, and elliptic functions over $\mathbb{C}/L$ correspond to those over $\mathbb{C}$, elliptic functions over $\mathbb{C}$ are entirely determined by their behaviour on any period parallelogram. The following definition and theorem will provide a more explicit formulation of this result and simplify future references.

Definition 2.3.2 (Congruence modulo a lattice)**.** Let L be a lattice in $\mathbb{C}$. Two complex numbers z and ω are said to be congruent modulo L if there exist $n, m \in \mathbb{Z}$ such that

$$z = \omega + n + m\tau,$$

We then write $z \equiv \omega \bmod L$.

By the periodicity of an elliptic function f, we conclude that

$$f(z) = f(\omega), \quad \text{if } z \equiv \omega \bmod L. \tag{2.1}$$

Theorem 2.3.3. *Let L be a lattice in $\mathbb{C}$. Then*

(*i*) *Every point in $\mathbb{C}$ is congruent to a unique point in the fundamental parallelogram.*

(*ii*) *Every point in $\mathbb{C}$ is congruent to a unique point in any given period parallelogram.*

Proof. (*i*): For existence, let $z \in \mathbb{C}$ with $z = x + iy$ and consider the lattice $L = [1, \tau]$. Write $z = a + b\tau$ with $a, b \in \mathbb{R}$. Choose n and m to be the greatest integers such that $n \leq a$ and $m \leq b$ and set $\omega = z - n - m\tau$. Then $\omega = (a - n) + (b - m)\tau$ satisfies $z \equiv \omega \bmod L$ by definition of the lattice relation. By construction it follows that $\omega \in P_0$.
To show uniqueness, let $\omega, \omega' \in P_0$ with $\omega \equiv \omega' \bmod L$. Writing $\omega = a + b\tau$ and $\omega' = a' + b'\tau$, we have $\omega - \omega' = (a - a') + (b - b')\tau \in L$ and so $a - a', b - b' \in \mathbb{Z}$. But since $0 \leq a, a' < 1$ and $0 \leq b, b' < 1$, we get $a - a' = 0$ and $b - b' = 0$, thus $\omega = \omega'$.
(*ii*): Applying (*i*) to $z - h$ gives the statement (*ii*). □

We see that $L = [1, \tau]$ and P_0 give rise to a covering of the complex plane

$$\mathbb{C} = \biguplus_{n,m \in \mathbb{Z}} (P_0 + n + m\tau) = \biguplus_{\omega \in L} (P_0 + w).$$

Note that this union is disjoint by definition of P_0.
We conclude that an elliptic function f is completely determined by its values in any period parallelogram. It follows that knowing all the roots and poles of an elliptic function in some period parallelogram is sufficient to describe all the roots and poles of the elliptic function, as all other roots and poles are congruent to the former ones. Such a set of poles or zeros in any given parallelogram is called an *irreducible set of poles* or *zeros*, respectively.

This naturally leads us to a deeper study of the roots and poles of elliptic functions.

Proposition 2.3.4. *The number of zeros and poles of an elliptic function f in any period parallelogram is finite.*

Proof. Let $\{z_n\}_{n \in \mathbb{N}}$ be a sequence of poles of an elliptic function f with $z_i \neq z_j$ for $i \neq j$. Since a period parallelogram is bounded, the sequence has to have a convergent subsequence with a limit point z within the cell by the Bolzano-Weierstraß Theorem (1.0.1). This would imply that z is a non-isolated singularity of f, contradicting the fact that f is meromorphic. Hence, f has only finitely many poles within any period parallelogram. Moreover, since $\frac{1}{f}$ is also an elliptic function and the zeros of f are the poles of $\frac{1}{f}$, it follows that f has only finitely many zeros in any period parallelogram. □

Before stating the next proposition, we recall a definition:
The *residue* of a meromorphic function f at an isolated singularity p, denoted $\mathrm{Res}(f,p)$, is the coefficient of $(z-p)^{-1}$ in the Laurent expansion of f around p, i.e.,

$$f(z) = \sum_{n=-\infty}^{\infty} a_n (z-p)^n$$

for $0 < |z-p| < r$, where $a_{-1} = \mathrm{Res}(f,p)$.

Proposition 2.3.5. *The sum of residues over an irreducible set of poles of an elliptic function is zero.*

Proof. Let $L = [\omega_1, \omega_2]$ be a lattice with fundamental parallelogram P_0, let U be an irreducible set of poles and let $C = \partial P_0$ be the the boundary of P_0. Then C is a simple closed curve, assumed with positive orientation. Also, suppose that f has no poles in C (otherwise use another parallelogram, such that no poles do not lie on its boundary). By Cauchy's residue theorem (1.0.3), we get

$$\begin{aligned}\sum_{p\in U} \mathrm{Res}(f,p) &= \frac{1}{2\pi i}\int_C f(z)\ dz \\ &= \frac{1}{2\pi i}\Big(\int_0^{\omega_1} f(z)\ dz \ + \ \int_{\omega_1}^{\omega_1+\omega_2} f(z)\ dz \ + \ \int_{\omega_1+\omega_2}^{\omega_2} f(z)\ dz \ + \ \int_{\omega_2}^{0} f(z)\ dz\Big).\end{aligned}$$

Shifting the second integral by ω_1 the third by ω_2, we get

$$\sum_{p\in U} \mathrm{Res}(f,p) = \frac{1}{2\pi i}\int_0^{\omega_1} (f(z) - f(z-\omega_2))\ dz \ - \ \frac{1}{2\pi i}\int_0^{\omega_2} (f(z) - f(z-\omega_1))\ dz,$$

which vanishes by the double-periodicity of f. Therefore,

$$\sum_{p\in U} \mathrm{Res}(f,p) = 0.$$

□

Corollary 2.3.6. *The number of zeros of a non-constant elliptic function f in any period parallelogram P is equal to the number of poles in P. The zeros and poles are counted by multiplicity.*

Proof. Let f be an elliptic function and P any period parallelogram. Then also $\frac{f'}{f}$ is an elliptic function and by Proposition 2.3.5, we get $\int_{\partial P} \frac{f'(z)}{f(z)}\ dz = 0$. Then the statement follows from Cauchy's argument principle (Theorem 1.0.8), since

$$\frac{1}{2\pi i}\int_{\partial P} \frac{f'(z)}{f(z)}\ dz = \#(\text{zeros of } f \text{ in } P) - \#(\text{poles of } f \text{ in } P).$$

□

Proposition 2.3.7. *An elliptic function with an empty irreducible set of poles is constant.*

Proof. An elliptic function f with no poles in a period parallelogram P cannot have any poles at all, since any pole outside P would necessarily have a congruent pole inside P. It follows that f is holomorphic on all of $\mathbb{C}$. Moreover, as a period parallelogram is compact, f is bounded on P. By periodicity, f is bounded everywhere and hence, by Liouville's Theorem (1.0.6), f must be constant. □

This motivates our next definition:

Definition 2.3.8 (Order of an elliptic function)**.** The order of an elliptic function f is the number of poles of f in any period parallelogram, counted with multiplicity.

Proposition 2.3.9. *For a non-constant elliptic function f, the sum of its zeros is congruent modulo the lattice to the sum of its poles within a period parallelogram, with all points lying in an irreducible set and counted with multiplicity.*

Proof. Let f be a non-constant elliptic function and let $U = \{a_1, \dots, a_k\}$ and $V = \{b_1, \dots, b_k\}$ denote the irreducible sets of zeros and poles, respectively, within a period parallelogram P, spanned by $\{\omega_1, \omega_2\}$. We aim to show that the sum of zeros of f differs from the sum of its poles by a period. By Proposition 2.3.4, there are only finitely many zeros and poles, and by Corollary 2.3.6, they occur in equal numbers. Then, as a consequence of Cauchy's residue theorem 1.0.3, we get

$$\sum_{i=1}^{k} a_i - \sum_{j=1}^{k} bj = \frac{1}{2\pi i} \int_{\partial P} z \, \frac{f'(z)}{f(z)} \, dz.$$

Shifting the second integral by ω_1 and the third one by ω_3, and using the periodicity of f and f', we obtain

$$\int_0^{\omega_1} z\frac{f'(z)}{f(z)} \, dz + \int_{\omega_1+\omega_2}^{\omega_2} z\frac{f'(z)}{f(z)} \, dz = \int_0^{\omega_1} (z - (z+\omega_2))\frac{f'(z)}{f(z)} \, dz = -\omega_2 \int_0^{\omega_1} \frac{f'(z)}{f(z)} \, dz$$
$$\int_{\omega_1}^{\omega_1+\omega_2} z\frac{f'(z)}{f(z)} \, dz + \int_{\omega_2}^{0} z\frac{f'(z)}{f(z)} \, dz = \int_{\omega_2}^{0} (z - (z+\omega_1))\frac{f'(z)}{f(z)} \, dz = \omega_1 \int_{\omega_2}^{0} \frac{f'(z)}{f(z)} \, dz,$$

which yields

$$\sum_{i=1}^{k} a_i - \sum_{j=1}^{k} bj = \frac{1}{2\pi i}\Big(\omega_1 \int_0^{\omega_2} \frac{f'(z)}{f(z)} \, dz - \omega_2 \int_0^{\omega_1} \frac{f'(z)}{f(z)} \, dz\Big).$$

Using $f(\omega_2) = f(0)$ and choosing a suitable branch of the complex logarithm, we get

$$\int_0^{\omega_2} \frac{f'(z)}{f(z)} \, dz = (\ln(f(\omega_2)) - \ln(f(0)) = \ln\Big(\frac{f(\omega_2)}{f(0)}\Big) = \ln(1) = 2m\pi i,$$

for some $m \in \mathbb{Z}$. Similarly,

$$-\int_0^{\omega_1} \frac{f'(z)}{f(z)}\, dz = 2n\pi i,$$

for some $n \in \mathbb{Z}$. This implies

$$\sum_{i=1}^{k} a_i - \sum_{j=1}^{k} bj = m\omega_1 + n\omega_2,$$

which completes the proof. □

Proposition 2.3.10. *The order of a non-constant elliptic function is at least* 2*.*

Proof. Let f be a non-constant elliptic function. By Proposition 2.3.7, f must at least have one pole in some period parallelogram P, so its order is at least 1. However, an elliptic function of order 1 has exactly one simple pole in a period parallelogram. In this case, the sum of the residues of f equals the residue at this single pole and therefore cannot vanish, contradicting Proposition 2.3.5. Thus, f must have order at least 2. □

Next, we introduce Eisenstein series, a family of lattice-based functions that encode essential information about the lattice and underlie the construction of the Weierstrass $\wp$-function, making them central to the study of elliptic functions.

Definition 2.3.11 (Eisenstein series)**.** Let L be a lattice in $\mathbb{C}$ and $k > 2$ an integer. The Eisenstein series of weight k for L is defined as

$$G_k(L) \coloneqq \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^k}.$$

Note that this series is well-defined by the next proposition.
Moreover, for all odd weights k, the Eisenstein series vanishes, as the terms $\frac{1}{w^k}$ and $\frac{1}{(-w)^k}$ cancel out in the sum by symmetry. Consequently, the only interesting Eisenstein series are those of even weight.

Considering lattices of the form $L = [1, \tau]$, where τ lies in the *upper half plane* $\mathbb{H} \coloneqq \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$, we can view $G_k(L)$ as a function of τ:

$$G_k(\tau) \coloneqq G_k([1, \tau]) = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m + n\tau)^k}.$$

Since $G_k(\tau)$ arises from a lattice function, it satisfies the transformation properties

$$G_k(\tau + 1) = G_k(\tau) \qquad \text{and} \qquad G_k\left(-\frac{1}{\tau}\right) = \tau^k G_k(\tau) \tag{2.2}$$

for all $\tau \in \mathbb{H}$.

Proposition 2.3.12. *For any lattice $L \subseteq \mathbb{C}$, the series $G_k(L)$ converges absolutely for all integers $k > 2$.*

Proof. Let δ be the minimum distance between two lattice points. Consider an annulus A of inner radius r and width $\frac{\delta}{2}$. Then any two distinct lattice points in A must be separated by an arc of length at least $\frac{\delta}{2}$. So A contains at most $\frac{8\pi r}{\delta}$ lattice points. Therefore, since the number of points $(n, m) \in \mathbb{Z}\backslash\{(0,0)\}$ with $N \leq |m + n\tau| < N + 1$ correspond to lattice points $m + n\tau \in \mathbb{Z} + \mathbb{Z}\tau$ in the annulus of radii N and $N + 1$, the number of lattice points in this annulus is bounded by cN, where $c \leq \frac{2}{\delta} \cdot \frac{8\pi r}{\delta} = \frac{16\pi}{\delta^2}$. The assumption $k > 2$ allows us to estimate

$$\sum_{\substack{\omega \in L \\ |\omega|>1}} \frac{1}{\omega^k} \;\leq\; \sum_{n=1}^{\infty} \frac{cn}{n^k} \;=\; c \sum_{n=1}^{\infty} \frac{1}{n^{k-1}} \;<\; \infty.$$

Since the finite sum $\sum_{\omega \in L, 0<|\omega|<1} \frac{1}{|\omega|^k}$ is clearly bounded, we get

$$\sum_{\omega \in L\backslash\{0\}} \frac{1}{|\omega|^k} \;=\; \sum_{\substack{\omega \in L \\ 0<|\omega|<1}} \frac{1}{|\omega|^k} + \sum_{\substack{\omega \in L \\ |\omega|\geq 1}} \frac{1}{|\omega|^k} \;<\; \infty,$$

as claimed. □

For the next proposition, let $q = e^{2\pi i\tau}$ with $\tau = x + iy \in \mathbb{H}$. It will be useful later on to express the Eisenstein series as sums of powers of q, which will converge as $|q| = e^{-2\pi y} < 1$. We will need the following two functions:

- The sum of positive divisors function of a positive integer n for a real or complex number l defined by
$$\sigma_l(n) = \sum_{d|n} d^l,$$
- The Riemann ζ-function defined as
$$\zeta(s) = \sum_{m=1}^{\infty} m^{-s}$$
for complex numbers s with $\mathrm{Re}(s) > 1$ and its analytic continuation elsewhere.

Proposition 2.3.13. *For all integers $k \geq 2$ and $\tau \in \mathbb{H}$ we have*

$$\begin{aligned} G_{2k}(\tau) &= 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{m=1}^{\infty} \sigma_{2k-1}(m) q^m \\ &= 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{r=1}^{\infty} \frac{r^{2k-1} q^r}{1 - q^r} \end{aligned}$$

Proof. With $q = e^{2\pi i\tau}$ and using Euler's identity $e^{i\pi} = -1$ we have

$$\begin{aligned}\pi\,\frac{\cos(\pi\tau)}{\sin(\pi\tau)} &= \pi i\,\frac{e^{i\pi\tau}+e^{-i\pi\tau}}{e^{i\pi\tau}-e^{-i\pi\tau}} = \pi i\,\frac{q^{\frac{1}{2}}+q^{-\frac{1}{2}}}{q^{\frac{1}{2}}+q^{-\frac{1}{2}}} = \pi i\,\frac{q^{-\frac{1}{2}}}{q^{-\frac{1}{2}}}\cdot\frac{q+1}{q-1}\\ &= \frac{\pi iq+\pi i}{q-1} = \frac{\pi iq-\pi i+2\pi i}{q-1} = \frac{\pi i(q-1)+2\pi i}{q-1}\\ &= \pi i+\frac{2\pi i}{q-1} = \pi i-\frac{2\pi i}{1-q} = \pi i-2\pi i\sum_{r=0}^{\infty}q^r,\end{aligned}$$

where in the last equality we used the geometric series.
The function $\sin(\pi\tau)$ has the following product expansion (for a proof see [6])

$$\sin(\pi\tau) = \pi\tau\prod_{m=1}^{\infty}\left(1-\frac{\tau}{m}\right)\left(1+\frac{\tau}{m}\right),$$

and taking its logarithmic derivative $(\log(\sin(\pi\tau)))'$ yields

$$\pi\,\frac{\cos(\pi\tau)}{\sin(\pi\tau)} = \frac{1}{\tau}+\sum_{m=1}^{\infty}\left(\frac{1}{\tau-m}+\frac{1}{\tau+m}\right) = \frac{1}{\tau}+\sum_{m=-\infty}^{\infty}\frac{1}{\tau+m}-\frac{1}{\tau} = \sum_{m=-\infty}^{\infty}\frac{1}{\tau+m}.$$

Combining these results, we obtain

$$\pi i-2\pi i\sum_{r=0}^{\infty}q^r = \sum_{m=-\infty}^{\infty}\frac{1}{\tau+m}.$$

Now we differentiate both sides of the equation $2k-1$ times. As interchanging the order of differentiation and summation over an infinite series is only possible if the derivatives of the summands uniformly converge to 0 and the original sum converges, we need to show this for both series. The geometric series is convergent as $|q|<1$ and the convergence of the series on the right hand side of the equation is given by

$$\sum_{m=1}^{\infty}\left|\frac{1}{\tau-m}+\frac{1}{\tau+m}\right| = \sum_{m=1}^{\infty}\left|\frac{2\tau}{\tau^2-m^2}\right| < \sum_{m=1}^{\infty}\frac{2|\tau|}{|-m^2|} = 2|\tau|\sum_{m=1}^{\infty}\frac{1}{m^2} < \infty,$$

as $|\tau| = x^2+y^2 > 0$, as absolute convergence implies convergence. For the uniform convergence we use that a series of a sequence of functions $(f_n)_{n=1}^{\infty}$ converges uniformly to a function f, if the sequence of its partial sums converges uniformly to f. Since $\mathbb{C}$ is a complete metric space, the claim follows by the Cauchy criterion for series (1.0.4).

Thus, we can interchange the order of differentiation and summation, and compute

$$\begin{aligned}\frac{\mathrm{d}^{2k-1}}{\mathrm{d}\tau^{2k-1}}\left(\pi i - 2\pi i\sum_{r=0}^{\infty} q^r\right) &= \frac{\mathrm{d}^{2k-2}}{\mathrm{d}\tau^{2k-2}}\left(-2\pi i\sum_{r=0}^{\infty}\frac{\mathrm{d}}{\mathrm{d}\tau}q^r\right)\\ &= \frac{\mathrm{d}^{2k-2}}{\mathrm{d}\tau^{2k-2}}\left(-2\pi i\sum_{r=1}^{\infty}(2\pi i r)q^r\right)\\ &\vdots\\ &= -(2\pi i)^{2k}\sum_{r=1}^{\infty} r^{2k-1}q^r,\end{aligned}$$

and

$$\begin{aligned}\frac{\mathrm{d}^{2k-1}}{\mathrm{d}\tau^{2k-1}}\left(\sum_{m=-\infty}^{\infty}\frac{1}{\tau+m}\right) &= \frac{\mathrm{d}^{2k-2}}{\mathrm{d}\tau^{2k-2}}\left(\sum_{m=-\infty}^{\infty}\frac{\mathrm{d}}{\mathrm{d}\tau}\frac{1}{\tau+m}\right)\\ &= \frac{\mathrm{d}^{2k-2}}{\mathrm{d}\tau^{2k-2}}\left(\sum_{m=-\infty}^{\infty}(-1)\frac{1}{(\tau+m)^2}\right)\\ &\vdots\\ &= (-1)^{2k-1}(2k-1)!\sum_{m=-\infty}^{\infty}\frac{1}{(\tau+m)^{2k}}.\end{aligned}$$

Hence,

$$-(2\pi i)^{2k}\sum_{r=1}^{\infty} r^{2k-1}q^r = (-1)^{2k-1}(2k-1)!\sum_{m=-\infty}^{\infty}\frac{1}{(\tau+m)^{2k}}.$$

Now consider the Eisenstein series $G_{2k}(\tau)$. Since $2k$ is even, the terms for (m,n) and $(-m.,-n)$ are equal, so we only need to sum over $n=0, m>0$ and $n>0, m\in\mathbb{Z}$ and double it. Therefore, we have

$$\begin{aligned}G_{2k}(\tau) &= \sum_{\substack{m,n\in\mathbb{Z}\\(m,n)\neq(0,0)}}\frac{1}{(m+n\tau)^{2k}}\\ &= 2\left(\sum_{\substack{n=0\\m>0}}\frac{1}{(m+n\tau)^{2k}} + \sum_{\substack{n>0\\m\in\mathbb{Z}}}\frac{1}{(m+n\tau)^{2k}}\right)\\ &= 2\sum_{m=1}^{\infty}\frac{1}{m^{2k}} + 2\sum_{n=1}^{\infty}\sum_{m=-\infty}^{\infty}\frac{1}{(m+n\tau)^{2k}}\\ &= 2\zeta(2k) - 2\sum_{n=1}^{\infty}(2\pi i)^{2k}\sum_{r=1}^{\infty}\frac{r^{2k-1}}{(-1)^{2k-1}(2k-1)!}q^{nr}\\ &= 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sum_{r=1}^{\infty} r^{2k-1}q^{nr},\end{aligned}$$

where in the fourth step we used the Riemann ζ-function as $\mathrm{Re}(2k) > 1$. Setting $m = nr$, the sum over r can be regarded as the sum over the positive divisors of m

$$\sum_{n=1}^{\infty}\sum_{r=1}^{\infty} r^{2k-1}q^{nr} = \sum_{m=1}^{\infty}\sum_{\substack{n=1\\ m=nr}}^{\infty} r^{2k-1}q^{m} = \sum_{m=1}^{\infty}\sum_{\frac{m}{r}=n,n\in\mathbb{N}}^{\infty} r^{2k-1}q^{m}$$
$$= \sum_{m=1}^{\infty}\sum_{r|m}^{\infty} r^{2k-1}q^{m} = \sum_{m=1}^{\infty}\sigma_{2k-1}(m)q^{m},$$

which proves the first formula. The geometric series

$$\sum_{n=1}^{\infty} q^{nr} = \frac{q^r}{1-q^r}$$

yields the second expression. □

2.3.2 The Weierstrass $\wp$-function

We now define one of the most important non-constant elliptic functions: the Weierstrass $\wp$-function. This function allows us to embed the complex torus into the projective plane, realizing it as an elliptic curve. Moreover, this fundamental example of elliptic function will serve to describe every other non-constant elliptic function in a later chapter.

Definition 2.3.14 (Weierstrass $\wp$-function)**.** For a lattice L in $\mathbb{C}$ and $z \in \mathbb{C}\backslash L$, the Weierstrass $\wp$-function is defined as

$$\wp(z;L) \coloneqq \frac{1}{z^2} + \sum_{\omega\in L\backslash\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right).$$

In the following, whenever the lattice L is fixed or clear from the context, we will simply write $\wp(z)$ instead of $\wp(z;L)$.

By definition, the Weierstrass $\wp$-function has a double pole at each lattice point, including $z = 0$. We will show that these are its only poles and that $\wp(z)$ is holomorphic on $\mathbb{C}\backslash L$.

Proposition 2.3.15. *The Weierstrass $\wp$-function is well-defined and holomorphic on $\mathbb{C}\backslash L$.*

Proof. To prove well-definedness, we show that the series

$$\sum_{\omega\in L\backslash\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

is convergent. For each $n \in \mathbb{N}$, define the function

$$f_n(z) = \frac{1}{z^2} + \sum_{\substack{\omega\in L\\ 0<|w|<n}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right).$$

Each function $f_n(z)$ is clearly holomorphic for all $z \in \mathbb{C}\backslash L$, since we can differentiate the finite sum term by term. We will show that the sequence of functions $(f_n)_{n\in\mathbb{N}}$ converges uniformly to $\wp$ on all compact subsets S of $\mathbb{C}$ disjoint from the lattice L. This will allow us to apply Theorem 1.0.5 to conclude that $\wp$ is holomorphic on $\mathbb{C}\backslash L$.
Let $S \subseteq \mathbb{C}$ be a compact set disjoint from L. Then S is bounded, so we can fix $r \in \mathbb{R}_{>0}$ such that $|z| \leq r$ for all $z \in S$. For all but finitely many $\omega \in L$, we have $|\omega| > 2r$. By the triangle inequality, $|\omega - z| + |z| \geq |\omega|$, and thus we get the following inequalities:

$$|\omega - z| \geq |\omega| - |z| \geq \frac{1}{2}|\omega|$$
$$|2\omega - z| \leq |2\omega| + |-z| \leq \frac{5}{2}|\omega|.$$

Hence,

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| = \left|\frac{z(2\omega - z)}{\omega^2(z-\omega)^2}\right| \leq \frac{r\frac{5}{2}|\omega|}{|\omega|^2(\frac{1}{2}|\omega|)^2} = \frac{10r}{|\omega|^3},$$

for all $z \in S$. Since the series $\sum_{\omega\in L\backslash\{0\}} \frac{c(z)}{|\omega|^3}$ is convergent by Proposition 2.3.12, it follows that $\sum_{\omega\in L\backslash\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$ converges absolutely for all $z \in S$, and hence $\wp$ is well-defined. Moreover, the sequence $(f_n)_{n\in\mathbb{N}}$ converges uniformly to $\wp$ on S, since for every $\epsilon > 0$ there exists $N \in \mathbb{N}$ such that for all $n \geq N$ we have $|\wp(z) - f_n(z)| < \epsilon$ for all $z \in S$. Then Theorem 1.0.5 implies that $\wp(z)$ is holomorphic on the open set $\mathbb{C}\backslash L$. □

Proposition 2.3.16. *For any lattice $L \subseteq \mathbb{C}$, the Weierstrass $\wp$-function and its derivative*

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

satisfy the following:

(i) $\wp(z)$ is an even meromorphic function, whose poles consist of double poles at each $z \in L$,

(ii) $\wp'(z)$ is an odd meromorphic function, whose poles consist of triple poles at each $z \in L$.

Proof. First, note that the series defining $\wp$ is uniformly convergent on $\mathbb{C}\backslash L$ by the proof of the previous proposition, so we may differentiate term by term to compute $\wp'$.
Since $\{-\omega \mid \omega \in L\} = L$ and the defining series of $\wp$ converges absolutely, we may rearrange terms without affecting the limit, hence $\wp(z) = \wp(-z)$. It is clear from the definition that $\wp(z)$ has a double pole at each lattice point, so (i) follows from Proposition 2.3.15. Part (ii) then follows from the fact that $\wp'(z)$ is meromorphic on $\mathbb{C}\backslash L$, as $\wp(z)$ is meromorphic and the expression for $\wp'(z)$ involves only termwise differentiation. □

Corollary 2.3.17. *For any lattice $L \subseteq \mathbb{C}$, $\wp(z)$ is an elliptic function of order 2 for L and $\wp'(z)$ is an elliptic function of order 3 for L.*

Proof. Recall that the order of an elliptic function is the number of poles in any period parallelogram, counted by multiplicity. The function $\wp(z)$ has two poles in every fundamental domain, while $\wp'(z)$ has three. By definition, $\wp'(z)$ is periodic with respect to L, so it remains to show the same for $\wp(z)$.
Since $\wp'(z)$ is periodic, we have $\wp'(z+\omega) = \wp'(z)$ for all $\omega \in L$. Integrating with respect to z yields $\wp(z) = \wp(z+\omega) + c(\omega)$, where $c(\omega) \in \mathbb{C}$ is a constant independent of z. Evaluating at $z = -\frac{1}{2}\omega$ (which does not lie in L) gives

$$\wp\left(-\frac{\omega}{2}\right) = \wp\left(-\frac{\omega}{2}+\omega\right) + c(\omega) = \wp\left(\frac{\omega}{2}\right) + c(\omega).$$

Since $\wp$ is an even function, we get $c(\omega) = 0$ and thus $\wp(z) = \wp(z+\omega)$ for $\omega \in L$, proving that $\wp$ is periodic. The corollary then follows from Proposition 2.3.16. □

The Weierstrass $\wp$-function is one of the simplest non-constant elliptic functions, having minimal order 2 (Proposition 2.3.10) and being constructed in a natural, explicit way from the lattice L. Moreover, from Section 2.3.1, it follows that the Weierstrass $\wp$-function and its derivative $\wp'$ descend to well-defined elliptic functions over the complex torus $\mathbb{C}/L$, making them a natural starting point for the study of elliptic functions. For now, we will use $\wp$ and $\wp'$ to construct an explicit isomorphism between $\mathbb{C}/L$ and an the set of points of an elliptic curve over $\mathbb{C}$.

The study of elliptic functions goes back to the German mathematician Gauß, who discovered them as solutions to elliptic integrals $\int \sqrt{f(z)}\ dz$, where $f(z)$ is a cubic or quartic polynomial. His work was later taken on by Legendre, Abel and Jacobi.
Our next goal is to show that the Weierstrass $\wp(z)$-function satisfies a differential equation of the form $\wp'(z)^2 = f(\wp(z))$, where $f(x)$ is a cubic polynomial with coefficients in $\mathbb{C}$. To derive this differential equation, we first compute the Laurent series expansion of $\wp(z)$ around $z = 0$.

Proposition 2.3.18. *Let L be a lattice in $\mathbb{C}$. The Laurent series expansion of $\wp(z)$ around $z = 0$ is given by*

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

where $G_{2n+2}(L)$ is the Eisenstein series of weight $2n+2$ for L.

Proof. Consider the geometric series

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n,$$

which converges absolutely for $|x| < 1$. By taking the derivative on both sides, while noting that termwise differentiation is allowed inside the open disk of convergence, we find

$$\frac{1}{(1-x)^2} = \sum_{n=1}^{\infty} n x^{n-1} = \sum_{n=0}^{\infty} (n+1) x^n.$$

Fix the lattice L and choose a radius $r > 0$ smaller than the length of the shortest non-zero vector in L (which exists since L is discrete). Then for any $\omega \in L\backslash\{0\}$ and z with $|z| < r$, we have $|\frac{z}{\omega}| < 1$, so we may set $x = \frac{z}{\omega}$ and obtain

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

Summing over all $\omega \in L\backslash\{0\}$ gives a double series. For $|z| < r'$ with any $0 < r' < r$, this series is absolutely convergent: indeed for fixed n, the outer sum $\sum_{\omega\neq 0}|\omega|^{-(n+2)}$ converges (because $n+2 \geq 3$ and the lattice sum $\sum_{\omega\neq 0}|\omega|^{-k}$ converges for $k > 2$ by Proposition 2.3.12), and for $|z| \leq r'$ the factor $(n+1)z^n$ makes the inner sum in n converges as well. By absolute convergence we may interchange the order of summation, thus for $|z| < r$

$$\begin{aligned}\wp(z) &= \frac{1}{z^2} + \sum_{\omega\in L\backslash\{0\}}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right) = \frac{1}{z^2} + \sum_{\omega\in L\backslash\{0\}}\sum_{n=1}^{\infty}\frac{(n+1)z^n}{\omega^{n+2}} \\ &= \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)\left(\sum_{\omega\in L\backslash\{0\}}\frac{1}{\omega^{n+2}}\right)z^n.\end{aligned}$$

Setting $G_{n+2}(L) = \sum_{\omega\in L\backslash\{0\}}\omega^{-(n+2)}$, and noting that for odd k the terms ω^{-k} and $(-\omega)^{-k}$ in the sum cancel by symmetry we obtain

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

□

We now deduce the fundamental algebraic relation satisfied by the Weierstrass $\wp$-function and its derivative. This differential equation provides the link between a lattice $L \subseteq \mathbb{C}$ and the corresponding elliptic curve, with coefficients determined by the lattice via Eisenstein series.

Theorem 2.3.19. *Let L be a lattice in $\mathbb{C}$. Then $\wp(z)$ satisfies the equation*

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

where $g_2(L) = 60G_4(L)$ and $g_3(L) = 140G_6(L)$.

Proof. We use the previous proposition to write out the first few terms of $\wp$ and $\wp'$ around 0:

$$\begin{aligned}\wp(z) &= \frac{1}{z^2} + 3G_4(L)z^2 + 5G_6(L)z^4 + \cdots \\ \wp'(z) &= -\frac{2}{z^3} + 6G_4(L)z + 20G_6(L)z^6 + \cdots \\ \wp(z)^3 &= \frac{1}{z^6} + \frac{9G_4(L)}{z^2} + 15G_6(L) + \cdots \\ \wp'(z)^2 &= \frac{4}{z^6} + \frac{24G_4(L)}{z^2} - 80G_6(L) + \cdots.\end{aligned}$$

Now consider the function

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

Forming a linear combination of powers of $\wp$ and $\wp'$, we can compute the Laurent series expansion of $f(z)$ around $z = 0$ and see that $f(0) = 0$, since the non-positive powers of z all cancel. Also, since $\wp$ and $\wp'$ have poles only at points of L, f is holomorphic on the fundamental parallelogram P_0. By periodicity of f, since $\wp$ and $\wp'$ are, f is holomorphic on the entire complex plane. Note that all values of $f(z)$ lie in the closure of a period parallelogram, which is a compact set, so f is bounded. It then follows from Liouville's Theorem (1.0.6), that f is constant, hence identically 0 and the theorem is proven. □

With $x = \wp(z)$ and $y = \wp'(z)$, the differential equation corresponds to the elliptic curve

$$E_L : y^2 = 4x^3 - g_2(L)x - g_3(L).$$

This curve can easily be written in Weierstrass form by setting $g_2(L) = -4A$ and $g_3(L) = -4B$. Thus, every lattice L determines an elliptic curve over $\mathbb{C}$, provided that the corresponding projective curve

$$f(x, y) = y^2 - g(x) = y^2 - 4x^3 + g_2(L)x + g_3(L)$$

is non-singular. Singular points (x_0, y_0) are the points on the curve where all partial derivatives vanish simultaneously, i.e. $f(x_0, y_0) = \frac{\delta f}{\delta x}(x_0, y_0) = \frac{\delta f}{\delta y}(x_0, y_0) = 0$. Solving this system, the third equation yields $y_0 = 0$, and the second gives $x_0^2 = \frac{g_2(L)}{12}$, which inserted in the first gieves $x_0 = -\frac{3g_3(L)}{2g_2(L)}$. Reinserting this value into the second then leads to $g_2(L)^3 - 27g_3(L)^2 = 0$. Hence, as long as the *discriminant of the lattice* L,

$$\Delta(L) \coloneqq g_2(L)^3 - 27g_3(L)^2,$$

is non-zero, the above equation defines an elliptic curve over $\mathbb{C}$.

We will show next that the discriminant is indeed non-zero for every lattice L.

Lemma 2.3.20. *Let L be a lattice in $\mathbb{C}$ and let $z, \omega \in \mathbb{C}\backslash L$. Then $\wp(z) = \wp(\omega)$ if and only if $z \equiv \pm\omega \bmod L$.*

Proof. The direction "⇐" follows from (2.1) and the fact that $\wp$ is an even function.
For the other direction, suppose $\wp(z) = \wp(\omega)$ for some $z, \omega \in \mathbb{C}\backslash L$. Consider the elliptic function $f(z) = \wp(z) - \wp(\omega)$, whose only pole lying in some period parallelogram P is at 0. Since it is a double pole, the number of zeros of f in P, counted with multiplicity, is equal to 2, by Theorem 2.3.6. Now there are two cases:
If $\omega \not\equiv -\omega \bmod L$, then ω and $-\omega$ are two distinct points in P, both zeros of f. Since the total number of zeros is 2, these are all zeros, each of multiplicity 1. Hence, $\wp'(z) \neq 0$.
If $\omega \equiv -\omega \bmod L$, then $2\omega \in L$ by the definition of congruence. Since $\wp'(z)$ is an odd function, we have $\wp'(\omega) = \wp'(\omega - 2\omega) = \wp'(-\omega) = -\wp(\omega)$, which forces $\wp'(\omega) = 0$. Hence ω gives rise to a zero of f in P. Since the total number of zeros in P is 2, this zero must have multiplicity 2 and these are all zeros of f in P. □

Lemma 2.3.21. *Let $L \subseteq \mathbb{C}$ be a lattice and let $z \in \mathbb{C}\backslash L$. Then $\wp'(z) = 0$ if and only if $2z \in L$.*

Proof. Suppose $2z \in L$ for some $z \notin L$. Then $\wp'(z) = \wp'(z-2z) = \wp'(-z) = -\wp'(z) = 0$, since $\wp'$ is periodic with respect to L and an odd function. Conversely, let $L = [\omega_1, \omega_2]$, and suppose $2z \in L$ with $z \notin L$. Then the only points z in a period parallelogram P satisfying $\wp'(z) = 0$ are $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$ and $\frac{\omega_1+\omega_2}{2}$. These points are all distinct by Lemma 2.3.20, since they are distinct modulo L. Finally, since $\wp'$ is an elliptic function of order 3, it has exactly three zeros (counted with multiplicity) in P, namely the ones listed above. □

The points $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$ and $\frac{\omega_1+\omega_2}{2}$ are called the *half-periods* of L. They correspond precisely to the non-zero points of order 2 on $\mathbb{C}/L$, i.e. the non-zero solutions of $2z \equiv 0 \bmod L$.

2.3.3 Lattices define elliptic curves

With the Weierstrass $\wp$-function and its key properties in hand, we now construct an elliptic curve from any lattice in $\mathbb{C}$ and explicitly identify its points with those of the corresponding complex torus, making the analytic-to-algebraic correspondence concrete.

Theorem 2.3.22. *For any lattice $L \subseteq \mathbb{C}$, we have $\Delta(L) \neq 0$.*

Proof. Let $L = [\omega_1, \omega_2]$ and set $r_1 \coloneqq \frac{\omega_1}{2}, r_2 \coloneqq \frac{\omega_2}{2}$ and $r_3 \coloneqq \frac{\omega_1+\omega_2}{2}$ to be the half-periods of L. By the previous lemma, $\wp'(r_i) = 0$, and from the differential equation we obtain

$$0 = \wp'(r_i)^2 = 4\wp(r_i)^3 - g_2(L)\wp(r_i) - g_3(L),$$

so the values $\wp(r_i)$, $i = 1, 2, 3$, are roots of the polynomial $4x^3 - g_2(L)x - g_3(L)$. Dividing the equation by the leading coefficient of the polynomial gives an equivalent equation with a monic polynomial $g(x) = x^3 - \frac{g_2(L)}{4}x - \frac{g_3(L)}{4}$, whose roots we denote by $e_i = \wp(r_i)$, $i = 1, 2, 3$. We now relate the discriminant of the polynomial g to that of the lattice L. By Theorem 1.0.11 (ii), the discriminant of g is $\Delta(g) = (e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2$. Using Vieta's formulas listed in Theorem 1.0.11 (i), we find

$$\begin{aligned} e_1 + e_2 + e_3 &= 0, \\ e_1e_2 + e_1e_3 + e_2e_3 &= -\frac{g_2(L)}{4}, \\ e_1e_2e_3 &= \frac{g_3(L)}{4}. \end{aligned}$$

The first relation gives $e_3 = -e_1 - e_2$ and inserting it into the other two yields

$$\begin{aligned} \frac{g_2(L)}{4} &= -(e_1e_2 + e_1(-e_1 - e_2) + e_2(-e_1 - e_2)) = e_1^2 + e_1e_2 + e_2^2, \\ \frac{g_3(L)}{4} &= e_1e_2(-e_1 - e_2) = -e_1^2e_2 - e_1e_2^2. \end{aligned}$$

Thus, using the definition of the discriminant of L, we compute

$$\begin{aligned}
\Delta(L) &= \frac{1}{16}(g_2(L)^3 - 27g_3(L)^2) \\
&= 4\left(\frac{g_2(L)}{4}\right)^3 - 27\left(\frac{g_3(L)}{4}\right)^2 \\
&= 4(e_1^2 + e_1e_2 + e_2^2)^3 - 27(-e_1^2e_2 - e_1e_2^2)^2 \\
&= 4e_1^6 + 12e_1^5e_2 - 3e_1^4e_2^2 - 26e_1^3e_2^3 - 3e_1^2e_2^4 + 12e_1e_2^5 + 4e_2^6 \\
&= (2e_1^3 + 3e_1^2e_2 - 3e_1e_2^2 - 2e_2^3)^2 \\
&= ((e_1 - e_2)(2e_1 + e_2)(e_1 + 2e_2))^2 \\
&= (e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2.
\end{aligned}$$

Since the roots $e_i = \wp(r_i)$ are all distinct for $i = 1, 2, 3$ by Lemma 2.3.20, we conclude that $\Delta(L) \neq 0$, as desired. □

Note that this proof explains the appearance of the factor -16 in the definition of the discriminant of an elliptic curve mentioned in Section 2.1. Moreover, this definition coincides with that of the discriminant of a lattice by using the identities $g_2(L) = -4A$ and $g_3(L) = -4B$.

Having established the non-vanishing of the lattice discriminant, the cubic equation associated with the Weierstrass $\wp$-function defines a non-singular elliptic curve. This ensures that the construction of the elliptic curve directly from the lattice in $\mathbb{C}$ is well-defined and leads to the following result:

Corollary 2.3.23. *For every lattice L in $\mathbb{C}$ there is an elliptic curve E over $\mathbb{C}$ such that $E \cong E_L$.*

The construction carried out in this section not only establishes the previous corollary, but also provides a natural map from the complex torus defined by the lattice L and the set of points of the corresponding elliptic curve E_L over $\mathbb{C}$:

$$\Phi : \mathbb{C}/L \to E_L(\mathbb{C}),$$

where each class $z + L$ is sent to $(\wp(z), \wp'(z))$ for $\in \mathbb{C}\backslash L$. The map Φ embeds the torus into $\mathbb{C}^2$ as an algebraic curve satisfying the Weierstrass equation $y^2 = x^3 + g_2(L)x + g_3(L)$ with $\Delta(L) \neq 0$. The lattice points themselves are excluded to ensure that $\wp$ and $\wp'$ are defined; they correspond to the point at infinity on the elliptic curve, completing the curve in the projective setting. A more detailed discussion will follow in the next section.

2.4 The isomorphism from a complex torus to the associated elliptic curve

Building on the construction of the map Φ in the previous section, we now show rigorously that Φ defines a group isomorphism between the complex torus associated with a lattice in $\mathbb{C}$ and the set of points of the corresponding elliptic curve over $\mathbb{C}$. This isomorphism identifies the additive structure of the torus with the group law on the curve, providing a concrete link between the analytic and algebraic description of elliptic curves.

To achieve this, we will explore the group structure of elliptic curves in more detail, in particular their property of being commutative groups under component-wise addition. Elliptic curves are symmetric about the x-axis, so for a point P, we take $-P$ to be its opposite point. Algebraically speaking, for an elliptic curve defined by $E_L : y^2 = x^3 + Ax + B$ over $\mathbb{C}$, the opposite point to a point $P = (x, y)$ is the point $-P = (x, -y)$ with the same x-coordinate but negated y-coordinate.
For two points $P, Q \in E_L(\mathbb{C})$, the addition $P + Q$ is defined geometrically by drawing the line that intersects P and Q, which generally will intersect the curve at a third point R, and then define $P + Q = -R$, the opposite point to R. Thus, by definition, any three points $P, Q, R \in E_L(\mathbb{C})$ lying on the same line satisfy $P + Q + R = \infty$. This definition of addition covers all cases except for a few special situations involving the point at infinity, which are treated separately as follows:

- *Identity*: If one of the points is ∞, say $Q = \infty$, then we define $P + \infty = P = \infty + P$, making ∞ the identity element of the group.
- *Opposites*: If two points are opposites of each other, say $Q = -P$, then the line through them is vertical. In this case we define the third intersection point as $R = \infty$, so that $P + (-P) = \infty$.
- *Doubling*: If the two points coincide, say $P = Q$, then we use the tangent to the curve at P as our line.
  - In the generic case, the tangent intersects the curve in another point R, and we define $P + P = 2P = -R$.
  - If the tangent does not intersect the curve at another point, we set $R = \infty$, which gives $P + P = 2P = \infty$.
- *Inflection*: If P is an inflection point, i.e. a point where the concavity of the curve changes, then the tangent has triple intersection with the curve at P. In this case we obtain $P + P + P = 3P = \infty$.

Moreover, a *point of order k* on the elliptic curve is a point P satisfying $kP = \infty$. From the doubling case we see that points of order 2 on the elliptic curve are precisely those which are their own opposites, i.e. those with $P = -P$, namely points of the form $(x, 0)$ where the y-coordinate vanishes. (In contrast, for a general point $P = (x, y)$ with $y \neq 0$, the opposite point is $-P = (x, -y)$, which is distinct from P.)

We are now prepared to state the theorem.

Theorem 2.4.1. *Let L be a lattice in $\mathbb{C}$ and let $E_L : y^2 = x^3 + Ax + B$ be the corresponding elliptic curve over $\mathbb{C}$. Then the map*

$$\Phi : \mathbb{C}/L \longrightarrow E_L(\mathbb{C}) : z + L \mapsto \begin{cases} (\wp(z), \wp'(z)), & \text{if } z \in \mathbb{C}\backslash L \\ 0, & \text{if } z \in L. \end{cases}$$

is a group isomorphism.

Proof. Well-definedness: If $z' \equiv z \bmod L$, then $z' = z + \lambda$ with $\lambda \in L$. Since $\wp$ and $\wp'$ are periodic, $\wp(z') = \wp(z)$ and $\wp'(z') = \wp'(z)$ and hence $\Phi(z' + L) = \Phi(z + L)$.
Identity and inverses: $0 \in L$ implies $\Phi(0 + L) = 0$ and for all $z \notin L$ we have

$$\Phi(-z + L) = (\wp(-z), \wp'(-z)) = (\wp(z), -\wp'(z)) = -\Phi(z + L),$$

as $\wp$ is even and $\wp'$ is odd and on an elliptic curve $-(x, y) = (x, -y)$.
Before turning to the other properties of a group isomorphism, a short consideration. Let $L = [\omega_1, \omega_2]$ and consider the three half-periods $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$ and $\frac{\omega_1+\omega_2}{2}$, which represent exactly the non-zero points of order 2 in $\mathbb{C}/L$, i.e. those satisfying $2z = 0$ in $\mathbb{C}/L$, or equivalently, $2z \in L$ with $z \notin L$. By Lemma 2.3.21, $\wp'$ vanishes at these three points, hence Φ maps points of order 2 in $\mathbb{C}/L$ to points of order 2 in $E_L(\mathbb{C})$, since points of order 2 on an elliptic curve are precisely those with y-coordinate equal to 0. Moreover, by the proof of Theorem 2.3.22, the images of the half-periods under $\wp$ are all distinct and correspond to the three roots of $4\wp(z)^3 - g_2(L)\wp(z) - g_3(L)$, so it follows that the map Φ is injective on points of order 2.
Surjectivity: let $(x_0, y_0) \in E_L(\mathbb{C})$ and we show that there exists $z_0 \in \mathbb{C}/L$ with $\Phi(z_0) = (x_0, y_0)$. Since $\wp(z)$ is an elliptic function for L of order 2 by Corollary 2.3.17, the function $f(z) = \wp(z) - x_0$ is also an elliptic function for L of order 2. Hence, by Corollary 2.3.6, f has two zeros in any fundamental parallelogram P, counted with multiplicity. These cannot occur at 0 as f has a pole at 0. So let $z_0 \in P$ with $z_0 \neq 0$ be one such zero. Then $\wp(z_0) = x_0$. Since $(x_0, y_0) \in E_L(\mathbb{C})$, it follows that the differential equation satisfied by $\wp$ from Theorem 2.3.19 implies $\wp'(z_0)^2 = 4\wp(z_0)^3 - g_2(L)\wp(z_0) - g_3(L) = y_0^2$, so $\wp'(z_0) = \pm y_0$. Therefore, $\Phi(z_0 + L) = (x_0, \wp'(z_0)) = (x_0, \pm y_0)$. If $\wp'(z_0) = y_0$ we are done. If $\wp'(z_0) = -y_0$, replace z_0 by $-z_0$; since $\wp(-z_0) = \wp(z_0) = x_0$ and $\wp'(-z_0) = -\wp'(z_0) = y_0$, we obtain $\Phi(-z_0 + L) = (x_0, y_0)$. Thus, in any case, there exists $z_0 \in \mathbb{C}\backslash L$ such that $\Phi(z_0) = (x_0, y_0)$, as desired.
Injectivity: let $z_1, z_2 \in P$ and suppose that $\Phi(z_1 + L) = \Phi(z_2 + L)$. We show that $z_1 = z_2$ in $\mathbb{C}/L$. If $2z_1 \in L$, then z_1 is a point of order 2 in $\mathbb{C}/L$, and by the consideration above, this implies $z_1 \equiv z_2 \bmod L$. Otherwise, if $2z_1 \notin L$, then $\wp'(z_1) \neq 0$ by Lemma 2.3.21. As argued in the surjectivity proof, the function $f(z) = \wp(z) - \wp(z_1)$ has exactly two zeros in P; let these be a_1 and a_2. Then $\wp(a_i) = \wp(z_1)$ for $i = 1, 2$, and $a_1 = z_1$ by construction of f and $a_2 = -z_1$ by the evenness of $\wp$. Now, since $\wp(z_1) = \wp(z_2)$ by assumption, it follows that either $z_2 \equiv z_1 \bmod L$ or $z_2 \equiv -z_1 \bmod L$. But also $\wp'(z_1) = \wp'(z_2)$ by assumption, and by the oddness of $\wp'$ we have $\wp'(-z_1) = -\wp'(z_1) \neq \wp'(z_1)$ and $\wp'(z_1) \neq 0$. Hence the second possibility is excluded, and we conclude $z_2 \equiv z_1 \bmod L$.

Homomorphism: let $z_1, z_2 \in \mathbb{C}/L$ and we show $\Phi(z_1+z_2+L) = \Phi(z_1+L)+\Phi(z_2+L)$. By Theorem 2.3.3, we may assume $z_1, z_2 \in P$. Also, if z_1 or z_2 is in L, the claim is immediate from the definition of Φ, and if $z_1 + z_2 \in L$, then $z_1 \equiv -z_2 \bmod L$, which forces $z_1 \equiv z_2 \bmod L$ by the injectivity argument. So in addition we may assume $z_1, z_2, z_1 + z_2 \notin L$.
Let $P_1 = \Phi(z_1)$ and $P_2 = \Phi(z_2)$, which are affine points in $E_L(\mathbb{C})$, and since z_1 and z_2 are not opposites of each other, P_1 and P_2 are neither, so that P_1 and P_2 have different x-coordinates, hence the line ℓ through them is not vertical. Let $y = mx + b$ be the equation describing the line ℓ and let P_3 be the third intersection point of ℓ with $E_L(\mathbb{C})$. Since P_1 and P_2 are not opposites of each other, P_3 cannot be the point at infinity and hence $P_1 + P_2 + P_3 = 0$ by the addition law on $E_L(\mathbb{C})$.
Now consider the function $\ell(z) = -\wp'(z) + m\wp(z) + b$, which vanishes exactly when $(\wp(z), \wp'(z))$ lies on the line ℓ. By construction, $\ell(z)$ is an elliptic function for L, which is of order 3 as $\wp'(z)$ is of order 3 by Corollary 2.3.17, hence it has exactly 3 zeros (counted with multiplicity, in P by Corollary 2.3.6. Two of them are z_1 and z_2, as $P_1 = \Phi(z_1)$ and $P_2 = \Phi(z_2)$ lie on the line by assumption. Let the third one be $z_3 \in P$. The point $\Phi(z_3)$ lies both on the line ℓ and on the elliptic curve $E_L(\mathbb{C})$ and hence must lie in $\{P_1, P_2, P_3\}$. As we have a bijection between $\{z_1, z_2, z_3\}$ and $\{\Phi(z_1), \Phi(z_2), \Phi(z_3)\} = \{P_1, P_2, P_3\}$ and $P_1 = \Phi(z_1)$ and $P_2 = \Phi(z_2)$ by assumption, the point z_3 is mapped to P_3. Indeed, it clearly holds if P_3 is distinct from P_1 and P_2, otherwise, if P_3 is coincides with P_1 or P_2, say P_1, then $\ell(z)$ has a double zero at z_1 and we have $z_3 = z_1$ and finally, if $P_1 = P_2 = P_3$, then clearly $z_1 = z_2 = z_3$ holds. Thus, in every case we have $P_3 = \Phi(z_3)$. Hence, as $P_1 + P_2 + P_3 = 0$, it suffices to show $z_1 + z_2 + z_3 \in L$, since this implies $z_1 + z_2 \equiv -z_3 \bmod L$ giving

$$\Phi(z_1 + L) + \Phi(z_2 + L) = P_1 + P_2 = -P_3 = -\Phi(z_3 + L) = \Phi(-z_3 + L) = \Phi(z_1 + z_2 + L).$$

Assume that the boundary C of P does not contain any zeros of $\ell(z)$; otherwise use another period parallelogram and replace z_1, z_2, z_3 by congruent points (Theorem 2.3.3). Moreover, assume the boundary to be oriented counterclockwise. Then the generalized Cauchy's argument principle 1.0.7 for $g(z) = z$ and $f(z) = \ell(z)$ gives

$$\frac{1}{2\pi i}\int_C z\frac{\ell'(z)}{\ell(z)}\,dz = \sum_{\omega\in P}\omega\ \mathrm{ord}_\omega(\ell) = z_1 + z_2 + z_3 - 3\cdot 0 = z_1 + z_2 + z_3.$$

Now we evaluate the integral. Define $f(z) = \frac{\ell'(z)}{\ell(z)}$, which is an elliptic function for L since $\ell(z)$ is, therefore also its derivative $\ell'(z)$, and thus their quotient because the set of elliptic functions for L forms a field. By writing $P = P_0 + h$ for some $h \in \mathbb{C}$ and P_0

being the fundamental parallelogram, we have

$$\begin{aligned}\int_C zf(z)dz &= \int_h^{h+\omega_1} zf(z)dz + \int_{h+\omega_1}^{h+\omega_1+\omega_2} zf(z)dz + \int_{h+\omega_1+\omega_2}^{h+\omega_2} zf(z)dz + \int_{h+\omega_2}^{h} zf(z)dz \\ &= \int_h^{h+\omega_1} uf(u)du + \int_h^{h+\omega_2} (u+\omega_1)f(u)du \\ &\quad - \int_h^{h+\omega_1} (u+\omega_2)f(u)du - \int_h^{h+\omega_2} uf(u)du \\ &= \omega_1 \int_h^{h+\omega_2} f(u)du - \omega_2 \int_h^{h+\omega_1} f(u)du,\end{aligned}$$

where we used the shifts $u = z - \omega_1$ and $u = z - \omega_2$ for the second and third integrals and then the periodicity of f with respect to L.
A naive attempt to compute the integral $\int f(u)du$ using $\int \frac{\ell'(u)}{\ell(u)}du = \log(\ell(u))$ fails, since $\ell(u)$ is multivalued and its logarithm is not single-valued. Instead, we interpret it in terms of the *winding number*: for a closed (not necessarily simple) curve C and a point $z_0 \notin C$, the integral $\frac{1}{2\pi i}\int_C \frac{dz}{z-z_0}$ is always an integer and counts the number of times the curve C "winds around" the point z_0.
In our case, the function $\ell(h+t\omega_2)$ parametrizes a closed curve C_1 from $\ell(h)$ to $\ell(h+\omega_2) = \ell(h)$ as t ranges in $[0,1]$. By construction, this curve circles exactly one zero of $\ell(z)$ in the fundamental parallelogram P (counted with multiplicity). Therefore, the winding number around 0 is a non-zero integer. Hence,

$$\frac{1}{2\pi i}\int_h^{h+\omega_2} f(u)du = \frac{1}{2\pi i}\int_0^1 \frac{\ell'(h+t\omega_2)}{\ell(h+t\omega_2)}\omega_2 dt = \frac{1}{2\pi i}\int_{C_1} \frac{dz}{z-0} = c_1 \in \mathbb{Z}\backslash\{0\}.$$

Similarly, the function $\ell(h+t\omega_1)$ parametrizes a closed curve C_2 from $\ell(h)$ to $\ell(h+\omega_1) = \ell(h)$, as t ranges from 0 to 1, giving

$$\frac{1}{2\pi i}\int_h^{h+\omega_1} f(u)du = \int_{C_2} \frac{dz}{z-0} = c_2 \in \mathbb{Z}\backslash\{0\}.$$

Combining these results, we have

$$\int_C zf(z)dz = \omega_1 \int_h^{h+\omega_2} f(u)du - \omega_2 \int_h^{h+\omega_1} f(u)du = \omega_1 c_1 - \omega_2 c_2 \in L.$$

Comparing this with the expression obtained from the Generalized argument principle, we conclude $z_1 + z_2 + z_3 = c_1\omega_1 - c_2\omega_2 \in L$, as desired. □

While this gives a precise identification of a torus with an elliptic curve, it does not yet yield a one-to-one correspondence between lattices and elliptic curves: distinct lattices can lead to isomorphic curves. We will return to this point in the next section, when we consider the converse direction from elliptic curves to lattices.

2.5 From elliptic curves to lattices

We now turn to the converse direction of the correspondence between lattices and elliptic curves: starting from an elliptic curve over $\mathbb{C}$, we aim to reconstruct a lattice that generates it. To do so, we rely on the j-invariant and the j-function, which provide a precise way to classify elliptic curves and relate them to homothety classes of lattices. This establishes a bijective correspondence at the level of objects - elliptic curves and lattices - thereby completing the full two-way correspondence that underlies the analytic and algebraic perspectives.

2.5.1 The j-invariant

We now focus on the j-invariant, the key quantity that captures the essential properties of an elliptic curve. It assigns to each curve a complex number uniquely determining its isomorphism class, allowing us to compare curves and connect them explicitly to lattices.

Definition 2.5.1 (j-invariant of an elliptic curve)**.** Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{C}$. Its j-invariant is defined by

$$j(E) = j(A, B) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

This expression is always defined by Theorem 2.3.22, since the discriminant of a lattice agrees with that of the associated elliptic curve, as mentioned in Section 2.3.3.

Definition 2.5.2 (j-invariant of a lattice)**.** For a lattice L in $\mathbb{C}$, the j-invariant $j(L)$ is defined to be the complex number

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

where $g_2(L)$ and $g_3(L)$ denote the Eisenstein series of weight 4 and 6 for L.

Again, this definition is well-defined as $\Delta(L) \neq 0$ for any lattice L by Theorem 2.3.22. Also, the reason for the factor 1728 will become clear later (Chapter 4).

Since the elliptic curve $E_L : y^2 = 4x^3 - g_2(L)x - g_3(L)$ is isomorphic to the elliptic curve $y^2 = x^3 + Ax + B$ with $g_2(L) = -4A$ and $g_3(L) = -4B$, we get

$$j(L) = 1728\frac{g_2(L)^3}{g_2(L)^3 - 27g_3(L)^2} = 1728\frac{(-4A)^3}{(-4A)^3 - 27(-4B)^2} = 1728\frac{4A^3}{4A^3 + 27B^2} = j(E_L),$$

so the j-invariant of the lattice L agrees with the j-invariant of the corresponding elliptic curve E_L.

Definition 2.5.3 (Homothety)**.** Two lattices L and L' are called homothetic, if $L' = \lambda L$ for some $\lambda \in \mathbb{C}\backslash\{0\}$.

Lemma 2.5.4. *Let $L \subseteq \mathbb{C}$ be a lattice, and let $\wp(z)$ have the Laurent expansion*

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

as in Proposition 2.3.18. Then, for each $n \geq 1$, the coefficient $(2n+1)G_{2n+2}(L)$ of z^{2n} is a polynomial with rational coefficients in $g_2(L)$ and $g_3(L)$, independent of L.

Proof. Set $a_n \coloneqq (2n+1)G_{2n+2}(L)$ so that we can write $\wp(z) = z^{-2} + \sum_{n=1}^{\infty} a_n z^n$. Differentiating twice gives

$$\wp''(z) = 6z^{-4} + \sum_{n=1}^{\infty} 2n(2n-1) a_n z^{2n-2},$$

and squaring $\wp(z)$ yields

$$\wp(z)^2 = z^{-4} + \sum_{n=1}^{\infty} 2a_n z^{2n-2} + \sum_{n=3}^{\infty} \sum_{k=1}^{n-2} a_k a_{n-k-1} z^{2n-2}.$$

Recall from Theorem 2.3.19, that $\wp$ satisfies the differential equation

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

which upon differentiating twice gives

$$\wp''(z) = 6\wp(z)^2 - \frac{1}{2} g_2(L).$$

By comparing the coefficients of z^{2n-2} for $n \geq 3$ we get

$$2n(2n-1)a_n = 6\left(2a_n + \sum_{k=1}^{n-2} a_k a_{n-k-1}\right),$$

and therefore

$$a_n = \frac{6}{2n(2n-1) - 12} \sum_{k=1}^{n-2} a_k a_{n-k-1}.$$

for $n \geq 3$. Thus, each a_n can be computed recursively from $a_1, \ldots, a_{n-2}$ for $n \geq 3$. Since $a_1 = \frac{g_2(L)}{20}$ and $a_2 = \frac{g_3(L)}{28}$, all coefficients are polynomials in $g_2(L)$ and $g_3(L)$ with rational coefficients, as claimed. □

Theorem 2.5.5. *Let L and L' be lattices in $\mathbb{C}$. Then L and L' are homothetic if and only if $j(L) = j(L')$.*

Proof. Suppose first that the lattices L and L' are homothetic. Then there exists $\lambda \in \mathbb{C}\backslash\{0\}$ such that $L' = \lambda L$. By definition of the Eisenstein series, we have

$$g_2(L') = 60 \sum_{\omega \in L'\backslash\{0\}} \frac{1}{\omega^4} \;=\; 60 \sum_{\omega \in L\backslash\{0\}} \frac{1}{(\lambda\omega)^4} \;=\; \lambda^{-4} g_2(L), \tag{2.3}$$

and similarly, $g_3(L') = \lambda^{-6} g_3(L)$. Therefore, the j-invariant satisfies

$$j(L') = 1728 \frac{(\lambda^{-4} g_2(L))^3}{(\lambda^{-4} g_2(L))^3 - 27(\lambda^{-6} g_3(L))^2} = 1728 \frac{g_2(L)^3}{g_2(L)^3 - 27 g_3(L)^2} = j(L).$$

Conversely, let L and L' be lattices such that $j(L) = j(L')$. Let $E_L : y^2 = x^3 + Ax + B$ and $E_{L'} : y^2 = x^3 + A'x + B'$ be the corresponding elliptic curves, with $g_2(L) = -4A, g_3(L) = -4B$ and $g_2(L') = -4A', g_3(L') = -4B'$. By the theory of elliptic curves over $\mathbb{C}$, there exists $\mu \in \mathbb{C} \backslash \{0\}$ such that $A' = \mu^4 A$ and $B' = \mu^6 B$ (see [14, Thm. 13.13]). Setting $\lambda = \frac{1}{\mu}$ gives $g_2(L') = \lambda^{-4} g_2(L) = g_2(\lambda L)$ and $g_3(L') = \lambda^{-6} g_3(L) = g_3(\lambda L)$. By the previous lemma, the coefficients of the Laurent expansion of $\wp(z; L)$ are polynomials in $g_2(L)$ and $g_3(L)$ with rational coefficients, which uniquely determine $\wp(z; L)$. Since $g_2(L') = g_2(\lambda L)$ and $g_3(L') = g_3(\lambda L)$ by (2.3), it follows $(2n+1)G_{2n+2}(L') = (2n+1)G_{2n+2}(\lambda L)$, which implies that $\wp(z; L)$ and $\wp(z; L')$ have the same Laurent expansion at 0. By analytic continuation, $\wp(z; L') = \wp(z; \lambda L)$ everywhere, and therefore $L' = \lambda L$, as desired. □

Corollary 2.5.6. *Two lattices L and L' are homothetic if and only if the corresponding elliptic curves E_L and $E_{L'}$ are isomorphic over $\mathbb{C}$.*

Combining Theorem 2.5.5 and Corollary 2.5.6, we see that elliptic curves over $\mathbb{C}$ are classified up to isomorphism by their j-invariant.
Moreover, these results show that the map from homothety classes of lattices in $\mathbb{C}$ to isomorphism classes of elliptic curves over $\mathbb{C}$ is injective. To establish a full correspondence, we still need surjectivity.

For our current purpose, the next theorem would suffice for the case of elliptic curves over $\mathbb{C}$. However, we state it in a more general form for future reference.
Accordingly, we assume that K is a field of characteristic $\mathrm{char}(K) \neq 2, 3$, so that every elliptic curve can be described by a short Weierstrass equation $y^2 = x^3 + Ax + B$. This assumption ensures that the curve is non-singular; for more details, see Section 2.1.

Theorem 2.5.7. *Let K be a field with $\mathrm{char}(K) \neq 2, 3$. For every $j_0 \in K$ there is an elliptic curve E over K such that $j(E) = j_0$.*

Proof. Let E be an elliptic curve over K. As the j-invariant of an elliptic curve E is defined by $j(E) = j(A, B) = 1728 \frac{4A^3}{4A^3 + 27B^2}$, there are two special cases worth noticing: if $A = 0$ then $j(E) = 0$ and if $B = 0$ then $j(E) = 1728$. Since the discriminant of E never vanishes by Theorem 2.3.22, A and B can not be 0 at the same time. Thus we must treat these to cases separately: if $j_0 = 0$ or $j_0 = 1728$, we may take E to be $x^3 + 1$ or $x^3 + x$, respectively. Otherwise, let E be the curve defined by $y^2 = x^3 + Ax + B$, where

$$A = 3j_0(1728 - j_0) \quad \text{and} \quad B = 2j_0(1728 - j_0)^2.$$

We claim that $j(A, B) = j_0$. Indeed,

$$\begin{aligned} j(A,B) &= 1728\frac{4A^3}{4A^3+27B^2} \\ &= 1728\frac{4\cdot 3^3 j_0^3(1728-j_0)^3}{4\cdot 3^3 j_0^3(1728-j_0)^3 + 27\cdot 2^2 j_0^2(1728-j_0)^4} \\ &= 1728\frac{j_0}{j_0+1728-j_0} \\ &= j_0, \end{aligned}$$

which completes the proof. □

With $K = \mathbb{C}$, this theorem implies that the j-invariant defines a surjective map between $\mathbb{C}$ and the set of isomorphism classes of elliptic curves over $\mathbb{C}$.

2.5.2 The j-function

To extend the correspondence to lattices, we introduce the j-function, which assigns to each homothety class of lattices a complex number. Expressing the j-invariant analytically in terms of a lattice parameter leads to its definition as a function on the upper half-plane.

Recall that every lattice $L = [\omega_1, \omega_2]$ is homothetic to a lattice of the form $L' = [1, \tau]$, with $\tau = \frac{\omega_1}{\omega_2} \in \mathbb{H}$. This allows us to define the j-invariant as a function on $\mathbb{H}$.

Definition 2.5.8 (j-function)**.** For $\tau \in \mathbb{H}$, the j-function is defined by $j(\tau) = j([1, \tau])$. Similarly, we define $g_2(\tau) = g_2([1, \tau])$, $g_3(\tau) = g_3([1, \tau])$ and $\Delta(\tau) = \Delta([1, \tau])$.

It follows that

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

and

$$g_2(\tau) = 60 \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(m+n\tau)^4}, \qquad g_3(\tau) = 140 \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(m+n\tau)^6},$$

which converge absolutely by Proposition 2.3.12.

Theorem 2.5.9. *The j-function is holomorphic on $\mathbb{H}$ and satisfies the relations $j(-\frac{1}{\tau}) = j(\tau)$ and $j(\tau+1) = j(\tau)$.*

Proof. Note that $j(-\frac{1}{\tau})$ and $j(\tau+1)$ are well-defined, since $-\frac{1}{\tau}$ and $\tau+1$ lie in $\mathbb{H}$. Moreover, the lattices $[1, \tau]$ and $[1, -\frac{1}{\tau}]$ are homothetic, while the lattices $[1, \tau]$ and $[1, \tau+1]$ are equal, hence $j(-\frac{1}{\tau}) = j(\tau)$ and $j(\tau+1) = j(\tau)$ by Theorem 2.5.5.
To show that the j-function is holomorphic on $\mathbb{H}$, it therefore suffices to show that $g_2(\tau)$

and $g_3(\tau)$ are holomorphic on $\mathbb{H}$. We begin with $g_2(\tau)$. By Proposition 2.3.12, the series defining $g_2(\tau)$ converges absolutely. It remains to show, however, that this convergence is uniform on compact subsets of $\mathbb{H}$. Let $D \subseteq \mathbb{H}$ be compact and consider the function

$$f : D \times S^1 \longrightarrow \mathbb{R} : (\tau, e^{it}) \longmapsto |\cos(t) + \tau \sin(t)|.$$

Then f is continuous and non-zero on the compact set $D \times S^1$, Hence it is bounded below by some constant c_D and $|m+n\tau| \geq c_D\sqrt{m^2+n^2}$ holds for all pairs $(m,n) \in \mathbb{Z}^2\backslash\{(0,0)\}$. But the series

$$\sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} (m^2+n^2)^{-\gamma}$$

converges for $\gamma > 1$. The proof for $g_3(\tau)$ is similar. It follows that $g_2(\tau)$, $g_3(\tau)$, and thus $j(\tau)$ are holomorphic on $\mathbb{H}$, since $\Delta(\tau)$ never vanishes. □

To describe when two points $\tau, \tau' \in \mathbb{H}$ give the same lattice up to homothety, we consider the group

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

which acts on $\mathbb{H}$ via linear fractional transformations

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

for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.
The group $\mathrm{SL}_2(\mathbb{Z})$ is generated by the matrices $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, so the j-function satisfies $j(\gamma\tau) = j(\tau)$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ by Theorem 2.5.9. We say in this case that j is $\mathrm{SL}_2(\mathbb{Z})$-*invariant*. In fact, more is true.

For practical reasons, we set $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

Lemma 2.5.10. *Let $\tau, \tau' \in \mathbb{H}$. Then $j(\tau) = j(\tau')$ if and only if $\tau' = \gamma\tau$ for some $\gamma \in \Gamma$.*

Proof. Suppose $\tau' = \gamma\tau$ for some $\gamma \in \Gamma$ and $\tau, \tau' \in \mathbb{H}$. By Theorem 2.5.9, we have $j(S\tau) = j(-\frac{1}{\tau}) = j(\tau)$ and $j(T\tau) = j(\tau+1) = j(\tau)$ and so $j(\tau) = j(\tau')$, since S and T generate Γ.
Conversely, suppose $j(\tau) = j(\tau')$ for some $\tau, \tau' \in \mathbb{H}$. The lattices $[1,\tau]$ and $[1,\tau']$ are homothetic by Theorem 2.5.5, so there exists $\lambda \in \mathbb{C}\backslash\{0\}$ such that $[1,\tau'] = \lambda[1,\tau]$. Therefore, there are $a,b,c,d \in \mathbb{Z}$ such that

$$\begin{aligned} \tau' &= a\lambda\tau + b\lambda \\ 1 &= c\lambda\tau + d\lambda \end{aligned}$$

Rewriting the second equation gives $\lambda = \frac{1}{c\tau+d}$ and substituting this into the first yields

$$\tau' = \frac{a\tau+b}{c\tau+d} = \gamma\tau, \qquad \text{where } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}^{2\times 2}.$$

Using Theorem 2.5.5, we could also write $[1, \tau] = \lambda^{-1}[1, \tau']$, which similarly gives $\tau = \gamma'\tau'$ for some $\gamma' \in \mathbb{Z}^{2\times 2}$. Combining these relations implies $\tau' = \gamma\gamma'\tau'$, so that $\det(\gamma) = \pm 1$. Since both τ and τ' lie in $\mathbb{H}$, we must have $\det(\gamma) = 1$, and therefore $\gamma \in \Gamma$. □

Two points $\tau, \tau' \in \mathbb{H}$ with the property $\tau' = \gamma\tau$ for some $\gamma \in \Gamma$ are said to be Γ-*equivalent*. This defines an equivalence relation on $\mathbb{H}$, and he equivalence class of τ is called the Γ-*orbit of* τ.

The previous lemma shows that $j(\tau) = j(\tau')$ if and only if τ and τ' are Γ-equivalent. In other words, j takes the same value on each Γ-orbit. Thus the j-function is a *complete invariant* for the action of Γ on $\mathbb{H}$, i.e. two points have the same j-value if and only if they belong to the same Γ-orbit.
Therefore, when studying the j-function, it suffices to study its behaviour on Γ-equivalence classes, that is, on the quotient $\mathbb{H}/\Gamma$. This action does not distinguish between matrices that differ by a sign, so taking the quotient by $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm \mathrm{I}_2\}$ yields the same result. Despite this fact, we will stick with $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

Now we want to find a fundamental domain for $\mathbb{H}/\Gamma$, i.e. a set of unique representatives in $\mathbb{H}$ for each Γ-equivalence class. There are many ways of constructing one, but a common choice is the region

$$\mathcal{F} = \Big\{\tau \in \mathbb{H} \mid |\tau| \geq 1,\ \mathrm{Re}(\tau) \in [-\tfrac{1}{2}, \tfrac{1}{2}),\ \text{such that } |\tau| > 1 \text{ if } \mathrm{Re}(\tau) > 0\Big\},$$

bounded by the vertical lines $\mathrm{Re}(\tau) = \frac{1}{2}$ and $\mathrm{Re}(\tau) = -\frac{1}{2}$ and the circle $|\tau| = 1$.

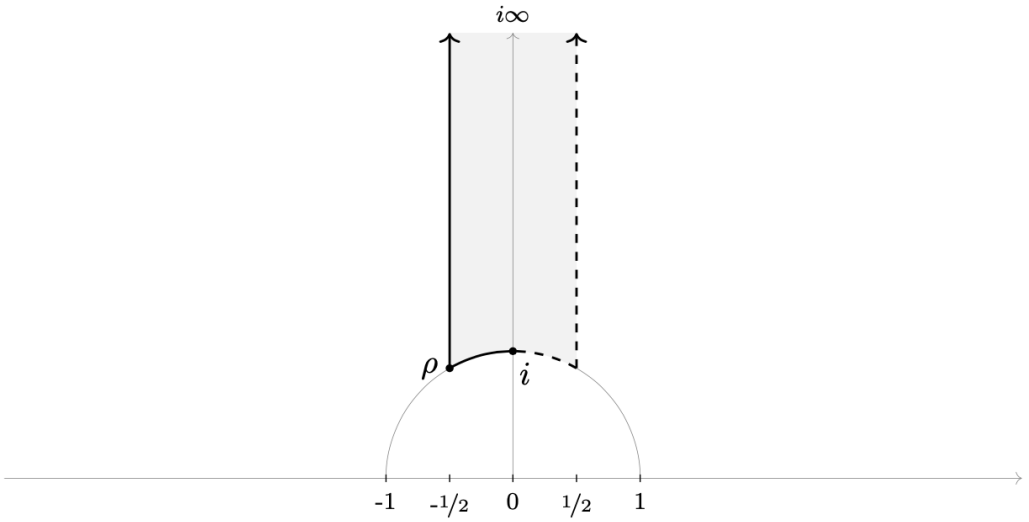

Figure 2.2: Fundamental domain $\mathcal{F}$ for $\mathbb{H}/\Gamma$ with $i = e^{\frac{\pi i}{2}}$ and $\rho = e^{\frac{2\pi i}{3}}$.
Reproduced from [14, Lec. 15]. Changes: none.

Lemma 2.5.11. *The set $\mathcal{F}$ is a fundamental domain for $\mathbb{H}/\Gamma$.*

Proof. We show that for any $\tau \in \mathbb{H}$ there is a unique $\tau' \in \mathcal{F}$ such that $\tau' = \gamma\tau$ for some $\gamma \in \Gamma$. We start with existence. Let $\tau \in \mathbb{H}$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$. We have

$$\mathrm{Im}(\gamma\tau) = \mathrm{Im}\left(\frac{a\tau+b}{c\tau+d}\right) = \frac{\mathrm{Im}((a\tau+b)(c\bar{\tau}+d))}{|c\tau+d|^2} = \frac{(ad-bc)\mathrm{Im}(\tau)}{|c\tau+d|^2} = \frac{\mathrm{Im}(\tau)}{|c\tau+d|^2} > 0, \tag{2.4}$$

so $\gamma\tau \in \mathbb{H}$. Since $(c,d) \mapsto |c\tau+d|^2$ is a positive definite quadratic form, it has minimum value for integers c, d which are relatively prime. By Bézout's Theorem, there are integers a, b, such that $ad - bc = 1$. So we can find a matrix $\gamma_0 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, such that $\mathrm{Im}(\gamma\tau) \leq \mathrm{Im}(\gamma_0\tau)$ for all $\gamma \in \Gamma$. Set $\gamma = T^k\gamma_0$, where $k \in \mathbb{N}$ is chosen such that $\mathrm{Re}(\gamma\tau) \in [-\frac{1}{2}, \frac{1}{2}]$, and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ is one of the generators of Γ. We claim that $\tau' = \gamma\tau \in \mathcal{F}$. If this was not the case, we would have $|\tau'| < 1$ and therefore $\mathrm{Im}(S\tau') = \mathrm{Im}(\tau')|\tau'|^{-2} > \mathrm{Im}(\tau')$, contradicting the maximality of $\mathrm{Im}(\gamma_0\tau)$, where $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ is the other generator of Γ. Hence, $|\tau'| \geq 1$ and together with $|\mathrm{Re}(\tau')| \leq \frac{1}{2}$ we obtain $\tau' \in \mathcal{F}$, proving existence.
Now we show uniqueness. We show that no two points in the interior of $\mathcal{F}$ share the same Γ-orbit. Let $\tau_1, \tau_2 \in \mathcal{F}$ with $\tau_2 = \gamma\tau_1$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, and assume $\mathrm{Im}(\tau_1) \leq \mathrm{Im}(\tau_2)$. By (2.4) we get

$$\mathrm{Im}(\tau_2) = \mathrm{Im}(\gamma\tau_1) = \mathrm{Im}(\tau_1)|c\tau_1+d|^{-2} \geq \mathrm{Im}(\tau_1), \tag{2.5}$$

so $|c\tau_1+d|^2 \leq 1$, thus using that $\mathrm{Re}(\tau_1) \in [-\frac{1}{2}, \frac{1}{2}]$ since $\tau_1 \in \mathcal{F}$, we get

$$1 \geq |c\tau_1+d|^2 = (c\tau_1+d)(c\bar{\tau_1}+d) = c^2|\tau_1|^2 + 2cd\mathrm{Re}(\tau_1) + d^2 \geq c^2|\tau_1|^2 + d^2 - |cd| \geq 1,$$

where the last inequality follows from $|\tau_1| \geq 1$, again since $\tau_1 \in \mathcal{F}$, and the fact that c and d cannot both be zero since $\det(\gamma) = 1$. Thus $|c\tau_1+d| = 1$, which implies $\mathrm{Im}(\tau_1) = \mathrm{Im}(\tau_2)$ by (2.5). Also we get $|c|, |d| \leq 1$ and, by replacing γ by $-\gamma$ if necessary (as discussed earlier), we may assume $c \geq 0$. This leaves us with 3 cases:

Case 1: $c = 0, d = \pm 1$: by the constraint $ad - bc = 1$, we get $a = d$ and so $\tau_2 = \gamma\tau_1 = \tau_1 \pm b$. By comparing real parts on both sides and using that $-\frac{1}{2} \leq \mathrm{Re}(\tau_1)$, $\mathrm{Re}(\tau_2) \leq \frac{1}{2}$, we see that there are only 3 possibilities for b, i.e. $b = 0, -1, 1$.
If $b = 0$, then $\tau_1 = \tau_2$ since both real and imaginary parts coincide.
If $b = 1$ resp. $b = -1$, then $\tau_2 = \tau_1 + 1$ and $\mathrm{Re}(\tau_1) = \frac{1}{2}$ resp. $\tau_2 = \tau_1 - 1$ and $\mathrm{Re}(\tau_1) = -\frac{1}{2}$, so τ_1 and τ_2 lie on the boundary lines of $\mathcal{F}$ and thus not in the interior.

Case 2: $c = \pm 1, d = 0$: the constraint forces $b = -1$ and by above we get $|\tau_1| = 1$, so τ_1 lies on the unit circle. Thus $\tau_2 = a - \frac{1}{\tau_1}$ and again by comparing real parts we get $a = 0, -1, 1$ as possibilities. If $a = 0$, then $\tau_1 = \tau_2 = i$. If $a = 1$ resp. $a = -1$, then $\tau_1 = \tau_2 = \rho = e^{\frac{2\pi i}{3}}$ resp. $\tau_1 = \tau_2 = e^{\frac{\pi i}{3}}$, which lie on the boundary of $\mathcal{F}$.

Case 3: $c = d = \pm 1$: Since $|c\tau_1| \leq 1$, we see that $\tau_1 = \rho$, as for any other $\tau \in \mathcal{F}$, we have $|\pm\tau \pm 1| > 1$. By the constraint $ad - bc = 1$, it follows that $a - b = 1$, so $b = -1 + a$. For $a = 0$ we get $\tau_1 = \tau_2 = \rho$ and for $a = 1$ we get $\tau_2 = \tau_1 + 1 = e^{\frac{\pi i}{3}}$, so all choices lie on the boundary again.
We conclude that in no case do τ_1 and τ_2 belong to the interior of $\mathcal{F}$, unless $\gamma = I_2$ and $\tau_1 = \tau_2$, which concludes the proof. □

Theorem 2.5.12. *The restriction of the j-function $j|_{\mathcal{F}} : \mathcal{F} \longrightarrow \mathbb{C}$ to the fundamental domain $\mathcal{F}$ is bijective.*

Proof. Since injectivity follows from Lemma 2.5.10 and Lemma 2.5.11, it remains to show surjectivity. For this aim we compute the limits of $g_2(\tau)$ and $g_3(\tau)$ as $\mathrm{Im}(\tau) \to \infty$. Following the approach used in the proof of Proposition 2.3.13, we write

$$g_2(\tau) = 60 \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(m+n\tau)^4} = 60 \left(2\sum_{m=1}^{\infty} \frac{1}{m^4} + \sum_{\substack{m,n\in\mathbb{Z} \\ n\neq 0}} \frac{1}{(m+n\tau)^4} \right).$$

The second sum vanishes for $\mathrm{Im}(\tau) \to \infty$, leading to

$$\lim_{\mathrm{Im}(\tau)\to\infty} g_2(\tau) = 120 \sum_{m=1}^{\infty} \frac{1}{m^4} = 120\zeta(4) = 120\frac{\pi^4}{90} = \frac{4\pi^4}{3},$$

where $\zeta(s)$ denotes the Riemann ζ-function. Similarly, we obtain

$$\lim_{\mathrm{Im}(\tau)\to\infty} g_3(\tau) = 280 \sum_{m=1}^{\infty} \frac{1}{m^6} = 280\zeta(6) = 280\frac{\pi^6}{945} = \frac{8\pi^6}{3}.$$

This implies

$$\lim_{\mathrm{Im}(\tau)\to\infty} \Delta(\tau) = \left(\frac{4\pi^4}{3}\right)^3 - 27\left(\frac{8\pi^6}{3}\right)^2 = 0$$

Thus the quantity $j(\tau) = 1728\frac{g_2(\tau)^3}{\Delta(\tau)}$ is unbounded when $\mathrm{Im}(\tau) \to \infty$.
Furthermore, since the j-function is non-constant and holomorphic on $\mathbb{H}$ by Theorem 2.5.9, its image $j(\mathbb{H})$ is an open subset of $\mathbb{C}$. We now claim that $j(\mathbb{H})$ is also closed in $\mathbb{C}$. Let $j(\tau_1), j(\tau_2), \ldots$ be a convergent sequence in $j(\mathbb{H})$ converging to some $\omega \in \mathbb{C}$. We need to show that $j(\tau) = w$, for some $\tau \in \mathbb{H}$. By Lemma 2.5.10 we know that $j(\tau) = j(\tau')$ if and only if τ' is Γ-equivalent to τ. Thus, since the j-function is Γ-invariant (Theorem 2.5.9), we may replace each τ_n by a Γ-equivalent point in the fundamental domain $\mathcal{F}$. Hence, without loss of generality, we may assume $\tau_n \in \mathcal{F}$ for all $n \geq 1$. Now, if the sequence $\mathrm{Im}(\tau_1), \mathrm{Im}(\tau_2), \ldots$ were unbounded, then by the above mentioned limit

$$\lim_{\mathrm{Im}(\tau)\to\infty} j(\tau) = \infty,$$

the sequence $j(\tau_1), j(\tau_2), \ldots$ would have a subsequence convergent to ∞, contradicting the fact $j(\tau_n) \to \omega \in \mathbb{C}$ for $n \to \infty$. Hence the sequence of the imaginary parts is bounded, say by B. Consequently, all the τ_n lie in a compact subset of $\mathcal{F}$, namely

$$\Omega = \left\{ \tau \in \mathbb{H} \;\middle|\; \mathrm{Re}(\tau) \in \left[-\frac{1}{2}, \frac{1}{2}\right],\ \mathrm{Im}(\tau) \in \left[\frac{1}{2}, B\right] \right\} \subseteq \mathcal{F}.$$

By compactness, there is a subsequence of the τ_n, which converges to some $\tau \in \Omega$. Since the j-function is holomorphic (Theorem 2.5.9) and hence continuous, we get $j(\tau) = \omega$.

It follows that the set $j(\mathbb{H})$ contains all its limit points and is therefore closed as claimed. As the set $j(\mathbb{H})$ is both open and closed, and $\mathbb{C}$ is connected, we get $j(\mathbb{H}) = \mathbb{C}$. Finally, since every point of $\mathbb{H}$ is Γ-equivalent to an point of $\mathcal{F}$ (Lemma 2.5.11) and the j-function is constant on Γ-orbits (Lemma 2.5.10), it follows that $j(\mathcal{F}) = \mathbb{C}$. □

This proof explains the coefficients 60 and 140 in the definitions of $g_2(L)$ and $g_3(L)$, indeed they are the smallest pair of integers, such that the above limit is 0.

2.5.3 Elliptic curves arise from lattices

With the j-invariant and j-function in place, we can now complete the correspondence between lattices and elliptic curves by showing that every elliptic curve over $\mathbb{C}$ arises from a lattice. This establishes the full two-way link between the analytic and algebraic perspectives.

The surjectivity of the j-function restricted to the fundamental domain from the previous theorem now allows us to deduce the following result:

Corollary 2.5.13. *Let $g_2, g_3 \in \mathbb{C}$ with $g_2^3 - 27g_3^2 \neq 0$. Then there exists a lattice $L \subseteq \mathbb{C}$ such that $g_2(L) = g_2$ and $g_3(L) = g_3$.*

Proof. Since the j-function is surjective, and $g_2^3 - 27g_3^2 \neq 0$ by assumption, there is some $\tau \in \mathbb{H}$ such that

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

As in the proof of Theorem 2.5.5, there is a complex number λ, such that $g_2 = \lambda^{-4}g_2(L)$ and $g_3 = \lambda^{-6}g_3(L)$. It follows that $L = \lambda[1, \tau]$ is the desired lattice. □

This shows that the j-invariant induces a surjective map from the set of homothety classes of lattices in $\mathbb{C}$ to $\mathbb{C}$. Together with the surjectivity of the j-invariant on elliptic curves over $\mathbb{C}$ (Theorem 2.5.7), the composition yields a surjective map from the set of homothety classes of lattices in $\mathbb{C}$ to the set of isomorphism classes of elliptic curves over $\mathbb{C}$. The injectivity of this map was established earlier, hence we obtain the following fundamental result.

Note that this also provides an alternative proof of Corollary 2.3.23, which established the existence of an elliptic curve E_L over $\mathbb{C}$ associated to every lattice $L \subseteq \mathbb{C}$. While Corollary 2.3.23 was deduced via the explicit construction of E_L using Weierstrass functions, the present approach derives it as a consequence of the surjectivity of the j-invariant.

Corollary 2.5.14. *For every elliptic curve E over $\mathbb{C}$ there is a lattice L in $\mathbb{C}$ such that $E \cong E_L$. Moreover, there is a one-to-one correspondence between the set of homothety classes of lattices in $\mathbb{C}$ and the set of isomorphism classes of elliptic curves over $\mathbb{C}$.*

An important and classical result in elliptic curve theory, the Uniformization Theorem, is a direct consequence of the first part of this corollary together with Theorem 2.4.1.

3 Complex multiplication and the ideal class group correspondence

Complex multiplication of elliptic curves over $\mathbb{C}$ sits at the intersection of arithmetic and geometry, connecting the structure of imaginary quadratic orders with the lattices underlying elliptic curves. In this chapter, we aim to make this connection precise by establishing a correspondence between the ideal class group of an order $\mathcal{O}$ and the lattices in $\mathbb{C}$ associated with elliptic curves having complex multiplication by $\mathcal{O}$.
To achieve this, we proceed step by step. We begin with homomorphisms of complex tori and isogenies of elliptic curves, laying the geometric and group-theoretic groundwork. This naturally leads us to the study of endomorphisms of elliptic curves, and from there to the algebraic framework of orders in imaginary quadratic number fields. With this foundation, we define complex multiplication, highlighting curves whose endomorphism rings are larger than usual. We then examine the lattices corresponding to a given endomorphism ring, introducing proper and fractional ideals to capture their structure. Finally, we bring these threads together in the study of the ideal class group and its action on lattices, culminating in a complete classification of elliptic curves with complex multiplication and a clear demonstration of the deep link between arithmetic and geometry.

This chapter follows the structure of [3, §10 C] and has been expanded with additional explanations and proofs following [14, Lec. 16], as well as some results from [3, §7 A].

3.1 Homomorphisms of complex tori and isogenies of elliptic curves

We begin by considering holomorphic maps between complex tori. These maps capture the algebraic structure of the tori and, when passed to the associated elliptic curves, correspond precisely to isogenies. This perspective sets the stage for understanding how lattice structures control the relationships between elliptic curves.

Every $\alpha \in \mathbb{C}$ determines a holomorphic map $z \mapsto \alpha z$, which is an endomorphism of $\mathbb{C}$ when considered as an additive group. So whenever we have two lattices L_1 and L_2 in $\mathbb{C}$, the inclusion $\alpha L_1 \subseteq L_2$ induces a group homomorphism

$$\varphi_\alpha : \mathbb{C}/L_1 \to \mathbb{C}/L_2 : z + L_1 \mapsto \alpha z + L_2,$$

which is also a holomorphic map of complex manifolds. In fact, every holomorphic map that fixes zero arises this way. The well-definedness is ensured by the condition $\alpha L_1 \subseteq L_2$ as $z \equiv \omega \bmod L_1$ implies $\alpha z \equiv \alpha\omega \bmod L_2$ for all $z, \omega \in \mathbb{C}$. Thus the following diagram

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\pi_1} & \mathbb{C}/L_1 \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \varphi_\alpha} \\ \mathbb{C} & \xrightarrow{\pi_2} & \mathbb{C}/L_2 \end{array}$$

commutes, where $\pi_1 : \mathbb{C} \to \mathbb{C}/L_1$ and $\pi_2 : \mathbb{C} \to \mathbb{C}/L_2$ denote the quotient maps.

Conversely, for every holomorphic map $\varphi : \mathbb{C}/L_1 \to \mathbb{C}/L_2$ with $\varphi(0) = 0$ there is a unique $\alpha \in \mathbb{C}$ with $\varphi = \varphi_\alpha$. Thus we have the following isomorphism of additive groups:

$$\begin{aligned} \{\alpha \in \mathbb{C} \mid \alpha L_1 \subseteq L_2\} &\to \{\text{homomorphmisms } \varphi : \mathbb{C}/L_1 \to \mathbb{C}/L_2\} \\ \alpha &\mapsto \varphi_\alpha. \end{aligned}$$

If $L_1 = L_2$, then the sets are isomorphic as commutative rings.
Indeed, the set on the left-hand side contains 0, is closed under addition, and thus forms an additive subgroup of $\mathbb{C}$. When $L_1 = L_2$, it is also closed under multiplication, making it a subring of $\mathbb{C}$. Similarly, the set on the right-hand side is an additive group under pointwise addition. In the case $L_1 = L_2$, we obtain that $\mathrm{Hom}(\mathbb{C}/L_1, \mathbb{C}/L_1)$ is the endomorphism ring $\mathrm{End}(\mathbb{C}/L_1)$, with multiplication given by composition.

Thus we can identify $\mathrm{Hom}(\mathbb{C}/L_1, \mathbb{C}/L_2)$ with $\{\alpha \in \mathbb{C} \mid \alpha L_1 \subseteq L_2\}$ and α with φ_α. For better readability, will therefore write α for the complex number satisfying $\alpha L_1 \subseteq L_2$ as well as for a homomorphism $\mathbb{C}/L_1 \to \mathbb{C}/L_2$.

As next step we want to identify $\{\alpha \in \mathbb{C} \mid \alpha L_1 \subseteq L_2\}$ with $\mathrm{Hom}(E_{L_1}, E_{L_2})$, for which we will now study $\mathrm{Hom}(\mathbb{C}/L_1, \mathbb{C}/L_2)$ and $\mathrm{Hom}(E_{L_1}, E_{L_2})$ a little more.

To study maps between elliptic curves, we first recall that a rational function is a function which can be expressed as a rational fraction, i.e., an algebraic fraction where both the numerator and denominator are polynomials. The coefficients of these polynomials may be taken from any field K, they are not restricted to be rational numbers. The set of rational functions over a field K forms the field of fractions of the ring of polynomial functions over K.

Also recall that the set of elliptic functions for a fixed lattice L forms a field, denoted $\mathbb{C}(L)$. As mentioned in Section 2.3.2, the Weierstrass $\wp$-function provides a natural starting point for describing all elliptic functions. Indeed, every elliptic function can be expressed as a rational function of $\wp$ and its derivative, and the subfield of even elliptic functions $\mathbb{C}(L)^{\text{even}} \subseteq \mathbb{C}(L)$ is generated by $\wp$ alone, meaning that every even elliptic function is a rational function in $\wp$.

Theorem 3.1.1. *Let L be a lattice in $\mathbb{C}$. Then we have*

(i) $\mathbb{C}(L) = \mathbb{C}(\wp, \wp')$,

(ii) $\mathbb{C}(L)^{even} = \mathbb{C}(\wp)$.

Proof. Let $f \in \mathbb{C}(L)$. Writing f as a sum of an even and an odd function

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

we see that it suffices to prove the theorem separately for even and odd elliptic functions. Now, let $g \in \mathbb{C}(L)$. Since $\wp'(z)$ is an odd elliptic function with simple zeros and no poles aside from those of order 3 at lattice points by Proposition 2.3.16 and Corollary 2.3.17, the quotient $\frac{g(z)}{\wp'(z)}$ is even and elliptic. Hence, every odd elliptic function can be written as a product of an even and an odd elliptic function:

$$g(z) = \frac{g(z)}{\wp'(z)}\wp'(z).$$

Thus, it suffices to consider even elliptic functions, and statement (i) follows from (ii). So let $f \in \mathbb{C}(L)^{\text{even}}$, and note that any zero or pole at the origin has even order.
Indeed, if the order at 0 is k, then near 0 we can write

$$f(z) = a_k z^k + a_{k+1} z^{k+1} + \dots$$

with $a_k \neq 0$. Since f is even, we have $f(z) = f(-z)$, which implies

$$a_k z^k + a_{k+1} z^{k+1} \dots = f(z) = f(-z) = (-1)^k (a_k z^k - a_{k+1} z^{k+1} + \dots).$$

Therefore $(-1)^k a_k = a_k$, so k must be even.
Now, since elliptic functions are doubly periodic, the same local behaviour occurs at every lattice point $\omega \in L$. Therefore, the order of any zero or pole of f at any lattice point is even. Hence, there exists an integer m such that the product $f\wp(z)^m$ has no zeros or poles at any lattice points. By replacing f with $f\wp(z)^m$, we may therefore assume that f has no zeros or poles on the lattice L. Our goal is to construct a function using $\wp$ that has the same zeros and poles (with the same multiplicities) as f.
Consider the function $f_c(z) = \wp(z) - c$ for some $c \in \mathbb{C}$, which, like $\wp(z)$, has double poles at each lattice point. Note that the zeros of f_c are the preimages of c under $\wp$ and since $\wp$ is even, $f_c(z_0) = 0$ implies $f_c(-z_0) = 0$ as well. Thus, f_c has either one double zero or two simple zeros on $\mathbb{C}/L$, depending on whether $z_0 \equiv -z_0 \bmod L$ holds, that is whether z_0 is a half-period. It follows that f_c has a double zero if and only if $c = e_1, e_2$ or e_3, where $e_1 = \wp(\frac{\omega_1}{2}), e_2 = \wp(\frac{\omega_2}{2})$ and $e_3 = \wp(\frac{\omega_1+\omega_2}{2})$ are the values of $\wp$ at the half-periods of L. For all other $c \in \mathbb{C}$, the function f_c has two distinct simple zeros.
We now study the zeros and poles of f in more detail. Since f is even, its zeros come in pairs $\{a, -a\}$, unless $a \equiv -a \bmod L$, in which case a is a half-period and, by our earlier observation, the corresponding order is even. Thus, if $a_1, -a_1, \dots, a_m, -a_m$, counted with multiplicity, denote all the zeros of f, then the function

$$(\wp(z) - \wp(a_1)) \cdot \dots \cdot (\wp(z) - \wp(a_m))$$

has the same zeros as f. Similarly, if $b_1, -b_1, \dots, b_m, -b_m$, again counted with multiplicity, describe all the poles of f, then

$$\frac{1}{(\wp(z) - \wp(b_1)) \cdot \dots \cdot (\wp(z) - \wp(b_m))}$$

has the same poles as f. Hence, the function

$$g(z) = \frac{(\wp(z) - \wp(a_1)) \cdot \ldots \cdot (\wp(z) - \wp(a_m))}{(\wp(z) - \wp(b_1)) \cdot \ldots \cdot (\wp(z) - \wp(b_m))}$$

has exactly the same zeros and poles as f. Since f and g are elliptic functions and share the same zeros and poles, the quotient $\frac{f}{g}$ is an elliptic function without any zeros or poles and thus holomorphic and doubly periodic on $\mathbb{C}$. Hence it is also bounded and therefore constant by Liouville's Theorem 1.0.6. It follows that $f = Cg$ for some constant $C \in \mathbb{C}$ and since $g \in \mathbb{C}(\wp)$, we conclude $f \in \mathbb{C}(\wp)$ as desired. □

For future use, we state the following refinement of part (ii) of the previous theorem:

Proposition 3.1.2. *Let $L \subseteq \mathbb{C}$ be a lattice. Every even elliptic function for L that is holomorphic on $\mathbb{C}\backslash L$ is a polynomial in $\wp$.*

Proof. Let f be an even elliptic function for L that is holomorphic on $\mathbb{C}/L$. We claim that there is a polynomial $A(x) \in \mathbb{C}[x]$ such that

$$g(z) \coloneqq f(z) - A(\wp(z))$$

is holomorphic at the origin. Assume that it is not possible.
Therefore, among all such polynomials, choose $A(x)$ such that $g(z)$ has a pole of minimal order at the origin. Since f and $\wp$ are even, the difference $g(z)$ is also even, so the pole at $z = 0$ must be of even order. That is,

$$g(z) = \frac{a}{z^{2M}} + \text{higher order terms},$$

with $a \neq 0$ and $M > 0$. Now, using the Laurent expansion of $\wp(z)$ near the origin given in Proposition 2.3.18, we obtain

$$\wp(z)^M = \frac{1}{z^{2M}} + \text{higher order terms}.$$

Hence,

$$g(z) - a\wp(z)^M = f(z) - \left(A(\wp(z)) + a\wp(z)^M\right)$$

has a pole of order strictly less than $2M$ at $z = 0$. This contradicts the minimality of the pole order for the original choice of $A(x)$. Therefore, such a polynomial $A(x)$ must exist, for which $f(z) - A(\wp(z))$ is holomorphic at $z = 0$.
Since f is elliptic, the difference $f(z) - A(\wp(z))$ is elliptic as well and hence it is holomorphic at all points of the lattice L by periodicity. By assumption, f is holomorphic on $\mathbb{C}\setminus L$, so $f(z) - A(\wp(z))$ is holomorphic on all of $\mathbb{C}$. It follows that $|f(z) - A(\wp(z))|$ is continuous and hence bounded on the compact region $P = \{\lambda_1\omega_1 + \lambda_2\omega_2 \mid 0 \leq \lambda_1, \lambda_2 \leq 1\}$, say by $Q > 0$. Then, given any $z \in \mathbb{C}$, we can find $z' \in P$ such that $z \equiv z' \bmod L$ by Theorem 2.3.3. It follows that $|g(z)| = |g(z')| \leq Q$, since $g(z)$ is L-periodic. Thus $f(z)$ is bounded. By Liouville's theorem 1.0.6, it follows that $g(z)$ is constant. Thus $f(z)$ differs from $A(\wp(z))$ by a constant, so in particular, $f(z)$ is a polynomial in $\wp(z)$. □

Theorem 3.1.3. *Let L_1, L_2 be lattices in $\mathbb{C}$ and E_1, E_2 the corresponding elliptic curves. Moreover set $\wp_i(z) = \wp(z; L_i)$ and let $\Phi_i : \mathbb{C}/L_i \to E_i(\mathbb{C})$ be the isomorphism between complex tori and elliptic curves over $\mathbb{C}$ for $i = 1, 2$, as in Theorem 2.4.1. Then for any $\alpha \in \mathbb{C}$ the following are equivalent:*

(i) $\alpha L_1 \subseteq L_2$,

(ii) $\wp_2(\alpha z)$ *is a rational function in* $\wp_1(z)$, *i.e.* $\wp_2(\alpha z) = \frac{u(\wp_1(z))}{v(\wp_1(z))}$ *for some polynomials* $u, v \in \mathbb{C}[x]$ *with* $v \neq 0$,

(iii) There is a unique homomorphism $\phi_\alpha : E_1 \to E_2$ such that the following diagram commutes:

$$\begin{array}{ccccc} \mathbb{C} & \longrightarrow & \mathbb{C}/L_1 & \xrightarrow{\Phi_1} & E_1(\mathbb{C}) \\ \downarrow{\scriptstyle \alpha} & & & & \downarrow{\scriptstyle \phi_\alpha} \\ \mathbb{C} & \longrightarrow & \mathbb{C}/L_2 & \xrightarrow{\Phi_2} & E_2(\mathbb{C}). \end{array}$$

Proof. Since the statements clearly hold for $\alpha = 0$, we assume $\alpha \neq 0$.
"$(i) \Rightarrow (ii)$": Let $\omega \in L_1$. Then $\wp_2(\alpha(z+\omega)) = \wp_2(\alpha z + \alpha\omega) = \wp_2(\alpha z)$ since $\alpha\omega \in L_2$ and $\wp_2$ is periodic with respect to L_2. So $\wp(\alpha z)$ is periodic with respect to L_1 and being meromorphic, it is an elliptic function for L_1. Moreover, it is even by Proposition 2.3.16, and therefore a rational function in $\wp_1$ by Theorem 3.1.1 (ii).
"$(ii) \Rightarrow (iii)$": Let $\wp_2(\alpha z) = \frac{u(\wp_1(z))}{v(\wp_1(z))}$ for some polynomials $u, v \in \mathbb{C}[x]$ with $v \neq 0$. To prove existence, let $s \coloneqq (u'v - v'u)$ and let $t \coloneqq \alpha v^2$, where u' and v' denote the derivatives of u and v and define the function

$$\phi_\alpha(x, y) \coloneqq \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right),$$

which is well-defined as $v, t \neq 0$. By the chain rule we compute

$$\begin{aligned} \wp_2'(\alpha z) &= \frac{1}{\alpha}(\wp_2(\alpha z))' = \frac{1}{\alpha}\left(\frac{u(\wp_1(z))}{v(\wp_1(z))}\right)' \\ &= \frac{1}{\alpha}\frac{u'(\wp_1(z))v(\wp_1(z)) - u'(\wp_1(z))v(\wp_1(z))'}{v(\wp_1(z))^2} = \frac{s(\wp_1(z))}{t(\wp_1(z))}\wp_1'(z), \end{aligned}$$

and thus

$$\phi_\alpha(\Phi_1(z)) = \phi_\alpha(\wp_1(z), \wp_1'(z)) = \left(\frac{u(\wp_1(z))}{v(\wp_1(z))}, \frac{s(\wp_1(z))}{t(\wp_1(z))}\wp_1'(z)\right) = (\wp_2(\alpha z), \wp_2'(\alpha z)) = \Phi_2(\alpha z),$$

so the above diagram commutes.
To show uniqueness, we assume that ϕ is another group homomorphism satisfying $\phi(\Phi_1(z)) = \Phi_2(\alpha z)$. Then we have

$$(\phi - \phi_\alpha)(\Phi_1(z)) = \phi(\Phi_1(z)) - \phi_\alpha(\Phi_1(z)) = \Phi_2(\alpha z) - \Phi_2(\alpha z) = 0,$$

and therefore $\phi = \phi_\alpha$.
"$(iii) \Rightarrow (i)$": For all $\omega \in L_1$ we have $\Phi_2(\alpha\omega) = \phi_\alpha(\Phi_1(\omega)) = \Phi(0) = 0$, thus $\alpha\omega \in L_2$ and $\alpha L_1 \subseteq L_2$ as desired. □

Since the polynomials u and v are non-constant, as $\wp_2(z)$ is not, the map $\phi_\alpha : E_1 \to E_2$ is a non-constant morphism and hence surjective, as a morphism of projective curves is either constant or surjective. This establishes that ϕ_α is an isogeny, a concept introduced in Section 2.1. Moreover, the fact that u and v can be chosen to be relatively prime, while s and t already are, implies that the polynomials u, v, s and t are uniquely determined up to a non-zero scalar in $\mathbb{C}$. Thus the expression

$$\phi_\alpha(x, y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$$

is often referred to as the *standard form* of the isogeny $\phi_\alpha : E_1 \to E_2$ and one can show that every isogeny of elliptic curves is of this form (see [14, Lemma 4.26]).

For later use, we define the *degree of an isogeny* ϕ by $\deg(\phi) \coloneqq \max(\{\deg(u), \deg(v)\})$, which is well-defined by above. Moreover, we say that an isogeny is *separable*, if the derivative $\frac{u(x)}{v(x)}$ is non-zero, otherwise we call ϕ_α *inseparable*.
As noted above, the polynomials u, v, s and t are uniquely determined up to a non-zero scalar in $\mathbb{C}$, so the degree and separability of ϕ_α are intrinsic properties and do not depend on the choice of its representation as a rational map.

3.2 Endomorphism rings of elliptic curves

The results of the previous section also provide structural insight into homomorphisms of elliptic curves. Specializing to the case where the domain and codomain coincide, we obtain the corresponding description of endomorphisms, which will lead naturally to the study of orders in imaginary quadratic number fields.

Corollary 3.2.1. *Let L_1, L_2 be lattices in $\mathbb{C}$. For every $\phi \in \mathrm{Hom}(E_1, E_2)$, there is a unique $\alpha = \alpha_\phi \in \mathbb{C}$ satisfying $(i) - (iii)$ from Theorem 3.1.3. The map $\phi \mapsto \alpha_\phi$ defines the group isomorphism between $\mathrm{Hom}(E_1, E_2)$ and $\{\alpha \in \mathbb{C} \mid \alpha L_1 \subseteq L_2\}$ with inverse map $\alpha \mapsto \phi_\alpha$.*

Proof. Let the maps Φ_1 and Φ_2 be as in the previous theorem. Then for every $\phi \in \mathrm{Hom}(E_1, E_2)$, the composition $\Phi_2^{-1} \circ \phi \circ \Phi_1$ is an element of $\mathrm{Hom}(\mathbb{C}/L_1, \mathbb{C}/L_2)$ and is therefore induced by the multiplication-by-α map $\alpha \mapsto \alpha z$ for a unique $\alpha = \alpha_\phi$ with $\alpha L_1 \subseteq L_2$ by the observations at the beginning of this chapter. The maps $\alpha \mapsto \phi_\alpha$ and $\phi \mapsto \alpha_\phi$ are thus inverse bijections.
It is easy to show that the map $\Psi : \mathrm{Hom}(E_1, E_2) \to \{\alpha \in \mathbb{C} \mid \alpha L_1 \subseteq L_2\} : \phi \mapsto \alpha_\phi$ fulfills $\Psi(\phi_1 + \phi_2) = \Psi(\phi_1) + \Psi(\phi_2)$ for some $\phi_1, \phi_2 \in \mathrm{Hom}(E_1, E_2)$ and $\Psi(0) = 0$, so that Ψ is a group homomorphism, thus an isomorphism and the statement is proven. □

Thus we have described the following isomorphisms

$$\{\alpha \in \mathbb{C} \mid \alpha L_1 \subseteq L_2\} \cong \mathrm{Hom}(\mathbb{C}/L_1, \mathbb{C}/L_2) \cong \mathrm{Hom}(E_{L_1}, E_{L_2}).$$

We will now consider the special case $L = L_1 = L_2$ and set $E_L = E$, obtaining
$\{\alpha \in \mathbb{C} \mid \alpha L \subseteq L\} \cong \mathrm{Hom}(E_L, E_L) = \mathrm{End}(E_L)$ the *endomorphism ring* of E_L with multiplication defined by composition.

Corollary 3.2.2. *Let $L \subseteq \mathbb{C}$ be a lattice and set $E = E_L$. The map $\phi \mapsto \alpha_\phi$ defines the ring isomorphism between* $\mathrm{End}(E)$ *and* $\{\alpha \in \mathbb{C} \mid \alpha L \subseteq L\}$ *with inverse map $\alpha \mapsto \phi_\alpha$.*

Proof. Let $\Psi : \mathrm{End}(E) \to \{\alpha \in \mathbb{C} \mid \alpha L \subseteq L\}$ be the group homomorphism as in the proof of the previous corollary. It is straightforward to check that $\Psi(\phi_1\phi_2) = \Psi(\phi_1)\psi(\phi_2)$ for all $\phi_1, \phi_2 \in \mathrm{End}(E)$, so Ψ is a ring homomorphism, and thus a ring isomorphism since it is a bijection. □

The ring $\mathrm{End}(E)$ is not necessarily commutative, however its center always contains the multiplication-by-n maps, denoted by $[n]$, for all $n \in \mathbb{Z}$. These endomorphisms form a subring of $\mathrm{End}(E)$ isomorphic to $\mathbb{Z}$, so we have $\mathbb{Z} \subseteq \mathrm{End}(E)$. This inclusion is not always an equality, as we will see in the next sections.

3.3 Orders in quadratic number fields

Our discussion shows that endomorphism rings always contain the integer multiplications, but in certain cases they can be strictly larger. To describe these richer structures, we first recall some background on quadratic number fields and their orders, which provide the natural setting for such enlarged endomorphism rings. This material also lays the groundwork for a detailed classification of orders in a later chapter.

Every quadratic number field K can be written as $K = \mathbb{Q}(\sqrt{d})$ for a uniquely determined squarefree integer $d \in \mathbb{Z}\backslash\{0, 1\}$. Every such K has an integral basis $\{1, \omega_K\}$, with ω_K given by

$$\omega_K = \begin{cases} \sqrt{d} & \text{if } d \not\equiv 1 \bmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

As the integral basis is a set of elements in K that generates the ring of integers $\mathcal{O}_K$ as a $\mathbb{Z}$-module, $\mathcal{O}_K$ can be written as $\mathcal{O}_K = [1, \omega_K] = \mathbb{Z} + \mathbb{Z}\omega_K$.
The discriminant d_K of K is then defined in terms of this integral basis by

$$d_K = \begin{cases} 4d & \text{if } d \not\equiv 1 \bmod 4 \\ d & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

For more details see [8, Thm. 3.3].

This integer d_K is sometimes also called a *fundamental discriminant*, i.e. an integer D such that either $D \equiv 1 \bmod 4$ is squarefree, or $D = 4d$ with $d \equiv 2, 3 \bmod 4$ with d squarefree. The term „fundamental discriminant“ suggests the existence of non-fundamental ones, and together, they provide a natural description of what we mean by a discriminant in general. We call an integer D a *discriminant*, if $D \equiv 0, 1 \bmod 4$ is a non-square.
The non-fundamental discriminants are also related to quadratic number fields in a similar way as the fundamental ones: they correspond to discriminants of orders in quadratic number fields. This leads us to the next definition:

Definition 3.3.1 (Order in a quadratic number field)**.** An order $\mathcal{O}$ in a quadratic number field K is a subset $\mathcal{O} \subseteq K$, which satisfies the following properties:

(i) $\mathcal{O}$ is a subring of K containing 1,

(ii) $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module,

(iii) $\mathcal{O}$ contains a $\mathbb{Q}$-basis of K.

Remark 3.3.2. *Some facts about orders in a quadratic number field K:*

1. *Any order $\mathcal{O}$ is torsion-free, since K is torsion-free. Conditions (ii) and (iii) then imply that $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank 2.*

2. *The ring of integers $\mathcal{O}_K$ is always an order of K. Moreover, conditions (i) and (ii) imply that for any order $\mathcal{O}$ we have $\mathcal{O} \subseteq \mathcal{O}_K$, so $\mathcal{O}_K$ is the* maximal order *of K.*

3. *Since both $\mathcal{O}$ and $\mathcal{O}_K$ are free $\mathbb{Z}$-modules of rank 2 by 1. and $\mathcal{O} \subseteq \mathcal{O}_K$ by 2., the index $f = [\mathcal{O}_K : \mathcal{O}]$ is finite and is called the* conductor *of $\mathcal{O}$.*

4. *Writing $\mathcal{O}_K = [1, \omega_K]$ as seen above, every order $\mathcal{O}$ can be described as*

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = [1, f\omega_K].$$

In particular, this shows that every order can be expressed in the form $\mathcal{O} = [1, \omega]$, for some element $\omega \in K$ (see [3, Lemma 7.2] for a proof).

From part *4.* of the above remark, it follows that an order $\mathcal{O}$ admits an integral basis of K, so we can define the discriminant of $\mathcal{O}$ in the same way as for $\mathcal{O}_K$ - as the square of the determinant of a 2×2-matrix whose rows are the elements of the integral basis, evaluated under the two automorphisms of the field K. Similar to the case of $\mathcal{O}_K$, it can be shown that the discriminant of $\mathcal{O}$ is independent of the chosen basis. When using the basis $[1, f\omega_K]$, the discriminant of $\mathcal{O}$ is given by $D = f^2 d_K$, where d_K is the fundamental discriminant of K, i.e. the discriminant of the maximal order $\mathcal{O}_K$.
Since the square of any integer is congruent to either 0 or 1 modulo 4, we have $f^2 \equiv 0, 1 \mod 4$. Moreover, as $d_K \equiv 0, 1 \mod 4$, it follows that every discriminant of the form $D = f^2 d_K$ satisfies $D \equiv 0, 1 \mod 4$, making it consistent with our general definition of a discriminant. More generally, it turns our that any non-square integer $D \equiv 0, 1 \mod 4$ is in fact the discriminant of some order in a quadratic field.

We summarize the preceding remark and discussion in the following theorem:

Theorem 3.3.3. *Let $\mathcal{O}$ be an order in a quadratic number field K with fundamental discriminant d_K. Then the discriminant of $\mathcal{O}$ is given by $D = f^2 d_K$, where $f \geq 1$ is an integer. Conversely, if $D \equiv 0, 1 \mod 4$ is non-square, then there exists a unique fundamental discriminant d_K and a unique integer $f \geq 1$, such that $D = f^2 d_K$. Moreover, there exists a unique order $\mathcal{O} \subseteq \mathbb{Q}(\sqrt{d_K})$ with discriminant D.*

3.4 Complex multiplication

Having analysed the endomorphisms of elliptic curves and introduced the framework of orders in imaginary quadratic number fields, we now bring these perspectives together. We focus on the special case where the endomorphism ring extends beyond $\mathbb{Z}$, which leads naturally to the notion of complex multiplication.

Theorem 3.4.1. *Let E be an elliptic curve over $\mathbb{C}$. Then $\mathrm{End}(E)$ is isomorphic to either $\mathbb{Z}$ or an order in an imaginary quadratic number field.*

Proof. Let L be the lattice corresponding to the elliptic curve E (Corollary 2.5.14). Since $\mathrm{End}(E) \cong \{\alpha \in \mathbb{C} \mid \alpha L \subseteq L\}$ is commutative, it is not isomorphic to an order in a quaternion algebra. Since any lattice is homothetic to one of the form $L = [1, \tau]$, it suffices to consider this case. Note that $\alpha[1, \tau] \subseteq [1, \tau]$ is equivalent to $\alpha \cdot 1 \in [1, \tau]$ and $\alpha \cdot \tau \in [1, \tau]$, so there exist integers m, n, p, q such that $\alpha = m + n\tau$ and $\alpha\tau = p + q\tau$, i.e.

$$n\tau^2 + \tau(m - q) - p = 0.$$

Unless τ is quadratic irrational, one has $n = 0$, so $\alpha \in \mathbb{Z}$ and $\mathrm{End}(E) \cong \mathbb{Z}$.
If τ is quadratic irrational, it satisfies a minimal polynomial of the form $x^2 + b'x + c'$ over $\mathbb{Q}$. By multiplying the polynomial with the least common multiple of the denominators of its coefficients, say $a \in \mathbb{Z}$, it follows that τ satisfies a polynomial of the form $ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}$ and $\gcd(a, b, c) = 1$. Then, from

$$\alpha\tau = m\tau + n\tau^2 = m\tau + n\frac{-b\tau - c}{a} = m + \frac{-bn}{a}$$

we see that $\alpha \cdot \tau \in [1, \tau]$ if and only if $a \mid n$. In this case, $\mathrm{End}(E) \cong \mathbb{Z} + \mathbb{Z}a\tau$. Since $a\tau$ is algebraic over $\mathbb{Q}(\tau)$, it follows that $\mathrm{End}(E)$ is isomorphic to an order in an imaginary quadratic number field. □

We want to focus on the case where $\mathrm{End}(E)$ is isomorphic to an order $\mathcal{O}$ in an imaginary quadratic number field.

Definition 3.4.2 (Complex multiplication)**.** Let E be an elliptic curve over $\mathbb{C}$. If $\mathrm{End}(E) \cong \mathcal{O}$ for some order $\mathcal{O}$ in an imaginary quadratic number field, then we say that E has complex multiplication by $\mathcal{O}$.

3.5 The ideal class group and correspondence with lattices

Building on the introduction of complex multiplication, we now turn our attention to the lattices that realize these enlarged endomorphism rings. In particular, we aim to classify lattices up to homothety for which the corresponding elliptic curve has endomorphism ring isomorphic to a given order $\mathcal{O}$. This perspective naturally brings us to the notion of $\mathcal{O}$-ideals and, ultimately, to the ideal class group, which organizes these lattices into equivalence classes.

Having seen that complex multiplication arises precisely when an elliptic curve has a larger endomorphism ring isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field, we now seek to determine for which lattices $L \subseteq \mathbb{C}$ this occurs.
Since any order $\mathcal{O}$ can itself be written as $[1, \omega]$ for an element $\omega \in K$ as stated in Remark 3.3.2, it can be viewed as a lattice in K and therefore in $\mathbb{C}$. Thus a natural candidate is $L = \mathcal{O}$. Moreover, as the set $\{\alpha \in \mathbb{C} \mid \alpha L \subseteq L\}$ remains unchanged when replacing L with any homotetic lattice L', we are naturally led to study lattices up to homothety.

Theorem 3.5.1. *Let $L \subseteq \mathbb{C}$ be a lattice, E_L the corresponding elliptic curve and let $\mathcal{O}$ be an order in an imaginary quadratic number field K. If $\mathrm{End}(E_L) \cong \mathcal{O}$, then L is homothetic to a sublattice of $\mathcal{O}$.*

Proof. We may assume that $L = [1, \tau]$ and $\mathcal{O} = [1, \omega]$ for some $\tau \in \mathbb{H}$ and $\omega \in K$. Since $\mathrm{End}(E_L) \cong \mathcal{O}$, we have $\alpha \cdot \tau \in [1, \tau]$ for all $\alpha \in \mathcal{O}$. In particular, for $\alpha = a + b\omega$ with $a, b \in \mathbb{Z}$ and $a = 0$ this gives $b\omega \cdot \tau \in [1, \tau]$ for all $b \in \mathbb{Z}$. Hence $\omega\tau \in [1, \tau]$, which implies $\omega \in L$. Thus we can write $\omega = m + n\tau$ for some $m, n \in \mathbb{Z}$ with $n \neq 0$. Then $nL = [n, n\tau] = [n, \omega - m] \subseteq [1, \omega] = \mathcal{O}$, so L is homothetic to a sublattice of $\mathcal{O}$. □

We now reveal that the result admits a stronger form.

Definition 3.5.2 ($\mathcal{O}$-ideal)**.** Let $\mathcal{O}$ be an order in an imaginary quadratic number field. An $\mathcal{O}$-ideal is an additive subgroup of $\mathcal{O}$ closed under multiplication by $\mathcal{O}$.

This definition generalizes the classical notion of an ideal in K: by allowing the additive subgroup to be in K rather than being strictly contained in $\mathcal{O}$, it permits the existence of elements outside of $\mathcal{O}$ while still maintaining closure under multiplication by $\mathcal{O}$.

Since sublattices of $\mathcal{O}$ are additive subgroups closed under multiplication by $\mathcal{O}$, they are nothing other than $\mathcal{O}$-ideals. Therefore, under the assumption $\mathrm{End}(E_L) \cong \mathcal{O}$, the previous theorem implies that L is homothetic to an $\mathcal{O}$-ideal, i.e. there is some $\lambda \in K \backslash \{0\}$ such that λL is an $\mathcal{O}$-ideal. As for every $\alpha \in \mathcal{O}$ we have $\alpha L \subseteq L$ by assumption, it follows that L is closed under multiplication by $\mathcal{O}$ and so L is an $\mathcal{O}$-ideal.

However, the converse implication does not hold in general: if L is an $\mathcal{O}$-ideal, it does not necessarily follow that $\mathrm{End}(E) \cong \mathcal{O}$. To see this, let L be an arbitrary $\mathcal{O}$-ideal and name the set

$$\mathcal{O}(L) \coloneqq \{\alpha \in \mathbb{C} \mid \alpha L \subseteq L\},$$

which is an order in K. It is clear that $\mathcal{O} \subseteq \mathcal{O}(L)$ always holds, since L is closed under multiplication by $\mathcal{O}$ by assumption. However, equality may fail. As counterexample consider $K = \mathbb{Q}[\sqrt{-3}], \mathcal{O} = \mathbb{Z}[\sqrt{-3}], L = (2, 1 + \sqrt{-3})$, here $\mathcal{O}(L)$ strictly contains $\mathcal{O}$.
This fact motivates the following definition:

Definition 3.5.3 (Proper ideal, fractional ideal)**.** Let $\mathcal{O}$ be an order in an imaginary quadratic number field K and L be an $\mathcal{O}$-ideal. We say that L is a proper $\mathcal{O}$-ideal if $\mathcal{O}(L) = \mathcal{O}$. For every $\alpha \in K \backslash \{0\}$ and every $\mathcal{O}$-ideal $\mathfrak{a}$, the $\mathcal{O}$-module $\mathfrak{b} = \alpha\mathfrak{a} = \{\alpha a \mid a \in \mathfrak{a}\}$ is called a fractional $\mathcal{O}$-ideal.

It follows from the definition that a fractional $\mathcal{O}$-ideal is an additive subgroup of an imaginary quadratic number field, which is closed under the multiplication by elements of $\mathcal{O}$. Thus fractional $\mathcal{O}$-ideals are more general structures than $\mathcal{O}$-ideals, as they may contain elements that do not belong to the order $\mathcal{O}$ itself.

Now, if L is homothetic to a proper $\mathcal{O}$-ideal, i.e. $L = \lambda\mathfrak{a}$ with $\mathfrak{a}$ proper and $\lambda \in K\backslash\{0\}$, we have

$$\mathrm{End}(E_L) \cong \mathcal{O}(L) = \mathcal{O}(\lambda\mathfrak{a}) = \mathcal{O}(\mathfrak{a}) = \mathcal{O},$$

so the converse indeed holds. The isomorphism $\mathrm{End}(E_L) \cong \mathcal{O}(L)$ is given by Corollary 3.2.2.

Moreover, note that every $\mathcal{O}$-ideal is homothetic to a proper $\mathcal{O}$-ideal. Indeed, for any $\mathcal{O}$-ideal L, the set $\mathcal{O}(L)$ contains $\mathcal{O}$, as seen before. By multiplying L with a suitable non-zero element of K, one can always obtain a lattice with endomorphism ring equal to $\mathcal{O}$. That is, there exists $\lambda \in K\backslash\{0\}$, such that λL is a proper $\mathcal{O}$-ideal. Thus, every $\mathcal{O}$-ideal is homothetic to a proper one. This and the fact that the concept of homothety can also be applied to lattices in $\mathbb{C}$ and $\mathcal{O}$-ideals, as every $\mathcal{O}$-ideal is a lattice in $\mathbb{C}$, completes the picture:

Corollary 3.5.4. *Let $L \subseteq \mathbb{C}$ be a lattice, E_L the corresponding elliptic curve and let $\mathcal{O}$ be an order in an imaginary quadratic number field. Then $\mathrm{End}(E_L) \cong \mathcal{O}$ if and only if L is homothetic to a proper $\mathcal{O}$-ideal.*

Remark 3.5.5. *For future theory we recall some facts about fractional $\mathcal{O}$-ideals:*

(i) Setting $\alpha = 1$, we see that every $\mathcal{O}$-ideal is a fractional $\mathcal{O}$-ideal. Fractional ideals that are contained in $\mathcal{O}$ are precisely the (integral) $\mathcal{O}$-ideals. Moreover, the order $\mathcal{O}$ itself is an $\mathcal{O}$-ideal by previous considerations and hence also a fractional $\mathcal{O}$-ideal.

(ii) Every proper $\mathcal{O}$-ideal is a fractional $\mathcal{O}$-ideal. Indeed, if $L \subseteq K$ is an $\mathcal{O}$-ideal with $\mathcal{O}(L) = \mathcal{O}$, then there exists $\alpha \in K^\times$ such that $L = \alpha\mathfrak{a}$, where $\mathfrak{a} \coloneqq \alpha^{-1}L$ is an $\mathcal{O}$-ideal.

(iii) A fractional $\mathcal{O}$-ideal $\mathfrak{a}$ is called invertible*, if there exists another fractional $\mathcal{O}$-ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \mathcal{O}$. We denote the* inverse *$\mathfrak{b}$ by $\mathfrak{a}^{-1}$. A fractional $\mathcal{O}$-ideal is proper if and only if it is invertible (see [3, Prop. 7.4] for a proof).*

(iv) The (absolute) norm *of a non-zero $\mathcal{O}$-ideal $\mathfrak{a}$ is defined by*

$$\mathrm{N}\mathfrak{a} = [\mathcal{O} : \mathfrak{a}] = |\mathcal{O}/\mathfrak{a}| \in \mathbb{Z}_{>0}.$$

For a fractional $\mathcal{O}$-ideal $\mathfrak{a} = [\alpha, \beta]$ we have $\mathfrak{a}\overline{\mathfrak{a}} = (\mathrm{N}\mathfrak{a})$, where $\overline{\mathfrak{a}} = [\overline{\alpha}, \overline{\beta}]$ and $(\mathrm{N}\mathfrak{a})$ denotes the principal $\mathcal{O}$-ideal generated by the integer $\mathrm{N}\mathfrak{a}$. In particular, the inverse of $\mathfrak{a}$ is given by the fractional $\mathcal{O}$-ideal $\mathfrak{a}^{-1} = \frac{1}{\mathrm{N}\mathfrak{a}}\overline{\mathfrak{a}}$. For a proof see [14, Thm. 17.10].

Remark 3.5.6. *For later purposes, note that with Definition 3.5.3, Lemma 3.4.1 implies that if τ is a root of a polynomial of the form $ax^2 + bx + c$ of minimal degree with integer coefficients and $\gcd(a, b, c) = 1$ in $K = \mathbb{Q}(\tau)$, then $[1, \tau]$ is a proper $\mathcal{O}$-ideal with $\mathcal{O} = [1, a\tau]$. Indeed, using the notation as in the proof, $\alpha\tau \in [1, \tau]$ if and only if $a \mid n$ with $\alpha = m + n\tau$ implies $\{\alpha \in K \mid \alpha[1, \tau] \subseteq [1, \tau]\} = [1, a\tau] = \mathcal{O}$, then the claim follows from the definition of proper $\mathcal{O}$-ideal.*

Remark 3.5.7. *As we are interested in lattices up to homothety, we regard two $\mathcal{O}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$ to be equivalent, if they are homothetic as lattices, i.e. if $\alpha\mathfrak{a} = \beta\mathfrak{b}$ for some non-zero $\alpha, \beta \in \mathcal{O}$. So for homothetic lattices $L' = \lambda L$ that are $\mathcal{O}$-ideals, we can write $\lambda = \frac{\alpha}{\beta}$ for some $\alpha, \beta \in \mathcal{O}$. It is easy to see that ideal multiplication respects this equivalence.*

This brings us to the definition of the ideal class group, which consists of equivalence classes of proper $\mathcal{O}$-ideals under multiplication. By Remark 3.5.5 (*iii*), proper $\mathcal{O}$-ideals are exactly the invertible fractional ideals, and multiplication of fractional ideals is commutative since multiplication in K is commutative. Thus, proper ideals form an abelian group, and principal ideals, i.e. those of the form $\alpha\mathcal{O}$ for some $\alpha \in K\backslash\{0\}$, form a subgroup. Taking equivalence classes modulo principal ideals then yields a well-defined quotient.

Definition 3.5.8 (Ideal class group)**.** Let $\mathcal{O}$ be an order in an imaginary quadratic number field. We denote by $I(\mathcal{O})$ the abelian group of proper $\mathcal{O}$-ideals under ideal multiplication and by $P(\mathcal{O})$ its subset of principal $\mathcal{O}$-ideals. Then the quotient

$$C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$$

is called the ideal class group of $\mathcal{O}$. Its cardinality is known as the class number $h(\mathcal{O})$.

This brings us to the final result of this chapter, which establishes the one-to-one correspondence we aimed to prove.

Corollary 3.5.9. *Let $\mathcal{O}$ be an order in an imaginary quadratic number field. There is a one-to-one correspondence between elements of the ideal class group $C(\mathcal{O})$ and the homothety classes of lattices $L \subseteq \mathbb{C}$ with $End(E_L) \cong \mathcal{O}$. In particular, the number of homothety classes is equal to the class number $h(\mathcal{O})$.*

Note that the second statement relies on the finiteness of the ideal class group. The Class number theorem states that the ideal class group of a maximal order $\mathcal{O}_K$ in an imaginary quadratic number field K is finite. We will not prove this here, but refer the reader to standard references such as [8, Thm. 9.7]. Moreover, for a general order $\mathcal{O} \subseteq \mathcal{O}_K$, its class number $h(\mathcal{O})$ is an integer multiple of $h(\mathcal{O}_K)$, which is a general result that we will state in Chapter 5 to classify orders with specific class numbers. In particular, this ensures that $h(\mathcal{O})$ is finite.

4 Modular functions

Modular functions lie at the crossroads of analysis, geometry and arithmetic. They arise as special meromorphic functions on the upper half-plane that respect the action of congruence subgroups and encode deep symmetries of elliptic curves. Our goal in this chapter is to develop their analytic and algebraic theory, focusing on the connections between the classical j-function and modular functions for congruence subgroups.
We proceed in five steps. We begin with congruence subgroups, which provide the natural setting in which modular functions are defined. As a starting point, we consider modular functions for $\mathrm{SL}_2(\mathbb{Z})$, focusing on the fundamental role of the modular j-function. Building on this foundation, we extend our attention to more general subgroups, where new functions arise and interact with j through the modular polynomial. This leads us to a structural analysis of the corresponding fields of modular functions, clarifying degrees of extensions and explicit generators. Finally, we adopt an arithmetic perspective, showing how modular functions can be described over $\mathbb{Q}$. This viewpoint will be crucial later, where modular functions connect analytic constructions with arithmetic applications.

The exposition in this chapter follows [3, §11 B-C], supplemented with additional explanations and proofs from [14, Lec. 18, 19] and [3, §12 A].

4.1 Congruence subgroups

To understand functions that reflect the symmetries of elliptic curves, we focus on those invariant under certain subgroups of $\mathrm{SL}_2(\mathbb{Z})$, called congruence subgroups. These invariances lead naturally to modular functions, which encode both the analytic and arithmetic structure of the curves and set the stage for the constructions that follow.

Recall from Chapter 2 that $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ acts on the upper half plane $\mathbb{H}$ via fractional linear transformations

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

and that the points of the quotient $\mathbb{H}/\Gamma$ (the Γ-orbits of $\mathbb{H}$) can be identified with the points of the fundamental domain $\mathcal{F}$ by Theorem 2.5.11. Since $\mathcal{F}$ is unbounded along the positive imaginary x-axis, it is not compact in $\mathbb{H}$, and hence neither is $\mathbb{H}/\Gamma$.
To compactify this space, we add an extra point, called the *point at infinity* ∞. More generally, it is natural to include not just ∞ but all points Γ-equivalent to it, i.e. all points in its Γ-orbit, in order to ensure that the extended upper half plane is compatible

with the action of Γ. Indeed, for $\tau \in \mathbb{H}$, we have

$$\lim_{\mathrm{Im}(\tau)\to\infty} \frac{a\tau + b}{c\tau + d} = \frac{a}{c} \in \mathbb{Q},$$

so it makes sense to include all rational numbers together with ∞. This leads to the *extended upper half plane*

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

By extending the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ to $\mathbb{P}^1(\mathbb{Q})$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (x : y) = (ax + by : cx + dy),$$

we obtain an action of $\mathrm{SL}_2(\mathbb{Z})$ on the extended upper half plane $\mathbb{H}^*$. Here $(x : y)$ denotes a point in $\mathbb{P}^1(\mathbb{Q})$ in homogeneous coordinates, and the points in $\mathbb{H}^* \backslash \mathbb{H} = \mathbb{P}^1(\mathbb{Q})$ are called *cusps*. Every cusp is equivalent under the action of Γ. Indeed, let $(x : y)$ be any cusp. Since we are using homogeneous coordinates, we may assume $x, y \in \mathbb{Z}$ and $\gcd(x, y) = 1$. By Bézout's Theorem, there are $a, b \in \mathbb{Z}$, such that $ax + by = 1$. Then

$$\gamma = \begin{pmatrix} a & b \\ -y & x \end{pmatrix} \in \Gamma \quad \text{with} \quad \gamma(x : y) = (1 : 0).$$

Thus every cusp is Γ-equivalent to ∞.

This allows us to extend the fundamental domain $\mathcal{F}$ of $\mathbb{H}$ to a fundamental domain $\mathcal{F}^*$ of $\mathbb{H}^*$ by including a single cusp, namely ∞. In this way, $\mathcal{F}^*$ becomes a compact subset of $\mathbb{H}^*$, and consequently, the quotient $\mathbb{H}^*/\Gamma$ is also compact.
To study finer arithmetic and geometric properties of these quotients, we consider certain subgroups of $\Gamma = \mathrm{SL}_2(\mathbb{Z})$:

Definition 4.1.1 (Congruence subgroup)**.** For any $N \in \mathbb{N}$, the principal congruence subgroup of level N in $\mathrm{SL}_2(\mathbb{Z})$ is

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

A subgroup of $\mathrm{SL}_2(\mathbb{Z})$ is called a congruence subgroup if it contains $\Gamma(N)$ for some N; the smallest such N is called its level.

It follows from the definition that every congruence subgroup of level N is a congruence subgroup, but not every congruence subgroup is necessarily associated with a specific level N.

Remark 4.1.2. *Every congruence subgroup is a subgroup of* $\mathrm{SL}_2(\mathbb{Z})$ *of finite index. The converse does not necessarily hold. A proof can be found in [12].*

One of the most important families of congruence subgroups of level N is the following:

$$\Gamma_0(N) \coloneqq \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \bmod N \right\}.$$

Note that $\Gamma(N) \subseteq \Gamma_0(N) \subseteq \Gamma = \mathrm{SL}_2(\mathbb{Z})$, so that in the special case $N = 1$, we have $\Gamma(1) = \Gamma_0(1) = \Gamma$. From now on, however, we will use Γ to denote a generic congruence subgroup, not necessarily all of $\mathrm{SL}_2(\mathbb{Z})$.

Remark 4.1.3. *Quotients of $\mathbb{H}$ or $\mathbb{H}^*$ by a congruence subgroup are called* modular curves*. In particular, the following are examples of modular curves:*

$$Y(N) \coloneqq \mathbb{H}/\Gamma(N), \qquad Y_0(N) \coloneqq \mathbb{H}/\Gamma_0(N)$$

and similarly,

$$X(N) \coloneqq \mathbb{H}^*/\Gamma(N), \qquad X_0(N) \coloneqq \mathbb{H}^*/\Gamma_0(N).$$

Using the same arguments as before for $X(1)$, one can show that $X(N)$ and $X_0(N)$ are compact Riemann surfaces. However, the proof requires a slight modification, since a fundamental domain may contain several cusps, not just the one at ∞.
From a more conceptual perspective, these modular curves also arise as moduli spaces: for instance, $X(1)$ classifies elliptic curves up to isomorphism, while $X_0(N)$ classifies elliptic curves together with a cyclic subgroup of order N. Since we do not need this moduli interpretation later, we will not develop the theory further.

Instead, we consider functions that are invariant under a congruence subgroup. Their invariance under translations implies periodicity, which in turn ensures they admit q-expansions - an essential tool for defining modular functions.

Definition 4.1.4 (Γ-invariant)**.** Let Γ be a congruence subgroup. A function $f : \mathbb{H} \to \mathbb{C}$ is called Γ-invariant if $f(\gamma\tau) = f(\tau)$ for all $\tau \in \mathbb{H}$ and $\gamma \in \Gamma$.

This generalizes the notion of Γ-invariance introduced in Section 2.5.2, where $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

Let Γ' be a congruence subgroup of level N and suppose that f is meromorphic on $\mathbb{H}$. Moreover, assume that f is Γ'-invariant. Consider the element $U = \left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma'$ and note that $\tau + N = U\tau$. By Γ'-invariance of f, we have

$$f(\tau + N) = f(U\tau) = f(\tau),$$

so f is periodic with period N. In particular, $f(\tau + 1) = f(\tau)$, so f can be expressed as a function in $q = q(\tau) = e^{2\pi i\tau}$, defined for $0 < |q| < 1$. Thus, f admits a Fourier expansion of the form

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

called the *q-expansion* of f.
Because f has period N, we can also express f as a function in $q^{\frac{1}{N}}$, defined for $0 < |q^{\frac{1}{N}}| < 1$, yielding the expansion

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

Moreover, $f(\gamma\tau)$ also has period N, since $\gamma U \gamma^{-1} \in \Gamma'$ implies

$$f(\gamma(\tau + N)) = f(\gamma U \tau) = f(\gamma U \gamma^{-1} \gamma\tau) = f(\gamma\tau).$$

by Γ'-invariance.

Definition 4.1.5 (Meromorphic at the cusps)**.** Let $f : \mathbb{H} \to \mathbb{C}$ be a meromorphic function, which is Γ-invariant for some congruence subgroup Γ of level N. The function $f(\tau)$ is said to be meromorphic at the cusps, if for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the q-expansion of $f(\gamma\tau)$ has only finitely many nonzero coefficients a_n with $n < 0$. That is, it can be written in the form

$$f(\gamma\tau) = \sum_{n=-n_0}^{\infty} a_n q^{\frac{n}{N}},$$

with $a_{n_0} \neq 0$ for some $n_0 \in \mathbb{N}$.

Note that it follows from the definition that if $f(\tau)$ is meromorphic at the cusps then $f(\gamma\tau)$ is meromorphic at the cusps for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, as $\mathrm{SL}_2(\mathbb{Z})$ permutes the cusps and so the transformation $\gamma\tau$ simply takes one cusp to another.

Definition 4.1.6 (Modular function)**.** Let Γ be a congruence subgroup. A modular function for Γ is a Γ-invariant meromorphic function $f : \mathbb{H} \to \mathbb{C}$, which is meromorphic at the cusps.

Sums, products and quotients of modular functions for a congruence subgroup Γ are again modular functions for Γ. Since constant functions are also modular functions, the set of all modular functions for Γ forms a field, which we denote by $\mathbb{C}(\Gamma)$.
Moreover, if f is a modular function for a congruence subgroup Γ, then f is also modular for any smaller congruence subgroup $\Gamma' \subseteq \Gamma$. Indeed, invariance under Γ implies invariance under Γ', and the property of being meromorphic at the cusps does not dependent on the choice of subgroup. This gives the inclusion relation

$$\Gamma' \subseteq \Gamma \;\Rightarrow\; \mathbb{C}(\Gamma) \subseteq \mathbb{C}(\Gamma'). \tag{4.1}$$

4.2 Modular functions for $\Gamma(1)$: the j-function

We begin with the simplest congruence subgroup, $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$, and focus on the j-function as a concrete example of a modular function. Its invariance under the full modular group captures key symmetries and provides a foundation for studying modular functions for other subgroups.

Since $j(\tau+1) = j(\tau)$ by Theorem 2.5.9, the j-function admits a q-expansion, which we write as

$$j(\tau) = \sum_{n=-\infty}^{\infty} c_n q^n.$$

Our goal is to show that $j(\tau)$ is indeed a modular function for $\Gamma(1)$.

We have already shown in Theorem 2.5.9 that $j(\tau)$ is $\Gamma(1)$-invariant and holomorphic, and hence meromorphic on $\mathbb{H}$. To verify that $j(\tau)$ is a modular function for $\Gamma(1)$, it remains to check that it is meromorphic at the cusps. Since all cusps are $\Gamma(1)$-equivalent (see the previous section), it suffices to consider ∞, which can be done via the q-expansion. Expressing $j(\tau)$ in terms of $g_2(\tau)$ and $g_3(\tau)$ (or equivalently $\Delta(\tau)$ and $g_2(\tau)$), where these functions are constant multiples of the Eisenstein series $G_4(\tau)$ and $G_6(\tau)$ respectively, it suffices to compute the q-expansions of the Eisenstein series. By the transformation properties in (2.2), the functions $G_k(\tau)$ are periodic under $\tau \mapsto \tau+1$ and hence admit q-expansions.

Theorem 4.2.1. *Let $L = [1, \tau]$ with $\tau \in \mathbb{H}$, let $q = e^{2\pi i \tau}$ and let $\sigma_l(n)$ denote the sum of positive divisors function. Then we have*

$$g_2(\tau) = \frac{4\pi^4}{3}\left(1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right)$$
$$g_3(\tau) = \frac{8\pi^6}{27}\left(1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n\right).$$

Proof. As introduced in Section 2.5.2, the functions g_2 and g_3 are given in terms of Eisenstein series by $g_2(\tau) = 60G_4(\tau)$ and $g_3(\tau) = 140G_6(\tau)$. Using the special values of the Riemann ζ-function

$$\zeta(4) = \frac{\pi^4}{90} \quad \text{and} \quad \zeta(6) = \frac{\pi^6}{945},$$

and Proposition 2.3.13 with $k = 2$ and $k = 3$, we obtain

$$\begin{aligned} g_2(\tau) = 60G_4(\tau) &= 120\zeta(4) + 120\frac{(2\pi i)^4}{3!}\sum_{m=1}^{\infty}\sigma_3(m)q^m \\ &= \frac{4\pi^4}{3}\left(1 + 240\sum_{m=1}^{\infty}\sigma_3(m)q^m\right) \\ g_3(\tau) = 140G_6(\tau) &= 280\zeta(6) + 280\frac{(2\pi i)^6}{5!}\sum_{m=1}^{\infty}\sigma_5(m)q^m \\ &= \frac{8\pi^6}{27}\left(1 - 504\sum_{m=1}^{\infty}\sigma_5(m)q^m\right), \end{aligned}$$

as desired. □

Corollary 4.2.2. *Let $q = e^{2\pi i\tau}$. The q-expansion of the j-function is of the form*

$$j(\tau) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} a_n q^n,$$

where the coefficients a_n are integers.

Proof. With the help of the previous theorem, we first compute the expansion of the discriminant $\Delta(\tau)$, which by definition is given by $\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2$. For $g_2(\tau)^3$, the computation is straightforward since all coefficients are positive:

$$\begin{aligned} g_2(\tau)^3 &= \frac{64}{27}\pi^{12}(1 + 240q + 2160q^2 + \ldots)^3 \\ &= \frac{64}{27}\pi^{12}(1 + 720q + 179280q^2 + \ldots). \end{aligned}$$

For the second term, we use the binomial formula $(1 + x^2) = 1 + 2x + x^2$ with $x = -504q - 16632q^2 - \cdots$ and obtain

$$\begin{aligned} 27g_3(\tau)^2 &= \frac{64}{27}\pi^{12}(1 - 504q - 16632q^2 - \ldots)^2 \\ &= \frac{64}{27}\pi^{12}(1 + 2(-504q - 16632q^2 - \ldots) + (-504q - 16632q^2 - \ldots)^2) \\ &= \frac{64}{27}\pi^{12}(1 - 1008q + 220752q^2 + \ldots), \end{aligned}$$

where we note that only the coefficient of q is negative, since the square in the last term contributes only higher-order positive terms. Combining these computations yields

$$\begin{aligned} \Delta(\tau) &= g_2(\tau)^3 - 27g_3(\tau)^2 \\ &= \frac{64}{27}\pi^{12}((1 + 720q + 179280q^2 + \cdots) - (1 - 1008q + 220752q^2 + \cdots)) \\ &= \frac{64}{27}\pi^{12}(1728q - 41472q^2 - \cdots) \\ &= \frac{64}{27}\pi^{12}1728q(1 - 24q + 252q^2 + \cdots), \end{aligned}$$

where in the penultimate step we used that all coefficients are divisible by 1728. Indeed, all coefficients (except the leading one) of $g_2(\tau)^3$ and $27g_3(\tau)^2$ are divisible by 240^3 and $27 \cdot 504^2$, respectively, whose prime factorisations are $2^{12} \cdot 3^3 \cdot 5^3$ and $2^6 \cdot 3^7 \cdot 7^2$. Hence they share the factor $2^6 \cdot 3^3 = 1728$, which divides all coefficients of the difference $g_2(\tau)^3 - 27g_3(\tau)^2$.

Finally, using the definition of the j-function and the computed expansions of $g_2(\tau)^3$ and $\Delta(\tau)$, a simple polynomial division gives

$$\begin{aligned} j(\tau) &= 1728\frac{g_2(\tau)^3}{\Delta(\tau)} \\ &= 1728\frac{\frac{64}{27}\pi^{12}(1+720q+179280q^2+\cdots)}{\frac{64}{27}\pi^{12}1728q(1-24q+252q^2+\cdots)} \\ &= \frac{1}{q}+744+196884q+21493760q^2+\ldots \\ &= \frac{1}{q}+744+\sum_{n=1}^{\infty}a_nq^n, \end{aligned}$$

which is the desired q-expansion of the j-function. The integrality of the coefficients a_n is not immediate from this division, since dividing two series with integer coefficients need not produce integer coefficients in general. This will be addressed rigorously in Chapter 7. □

Observe that the factor 1728 is the smallest integer required to ensure that the coefficients of $j(\tau)$ are integers. Moreover, the prefactor $\frac{64}{27}\pi^{12}1728 = 4096 = (2\pi)^{12}$ in the expansion of $\Delta(\tau)$ will reappear in its product expansion in terms of the Dedekind η-function (see Chapter 7).

In particular, the corollary shows that $j(\tau)$ is a modular function for $\Gamma(1)$, since it has a simple pole at ∞ and so is meromorphic there.
Moreover, every modular function for $\Gamma(1)$ can be expressed in terms of the j-function, as we will see next.

Definition 4.2.3 (Holomorphic at ∞)**.** Let f be a modular function for a congruence subgroup of level N. We say that f is holomorphic at ∞ if its q-expansion involves only non-negative powers of $q^{\frac{1}{N}}$, i.e. it can be written in the form

$$f(\tau)=\sum_{n=0}^{\infty}a_nq^{\frac{n}{N}}.$$

Lemma 4.2.4. *The following statements hold:*

(i) A modular function for $\Gamma(1)$ that is holomorphic on $\mathbb{H}$ and at ∞ is constant.

(ii) A modular function for $\Gamma(1)$ that is holomorphic on $\mathbb{H}$ is a polynomial in $j(\tau)$.

Proof. "(i)": Let f be a modular function for $\Gamma(1)$ that is holomorphic on $\mathbb{H}$ and at ∞. Since f is holomorphic at ∞, we have that $f(\infty)=\lim_{\mathrm{Im}(\tau)\to\infty}f(\tau)$ exists by definition and is a complex number. Thus it makes sense to extend the domain of f from $\mathbb{H}$ to the compactified set $\mathbb{H}\cup\{\infty\}$ by setting $f(\infty)$ equal to this limit.
We now show that $f(\mathbb{H}\cup\{\infty\})$ is compact. To this end, let $f(\tau_1), f(\tau_2),\ldots$ be a sequence of points in the image of f. We have to find a subsequence, which converges to a

point $f(\tau_0)$ for some $\tau_0 \in \mathbb{H} \cup \{\infty\}$. Since f is $\Gamma(1)$-invariant, we can assume that the points τ_k, $k \geq 1$, lie in the fundamental domain $\mathcal{F} = \{\tau \in \mathbb{H} \mid |\tau| \geq 1,\ \mathrm{Re}(\tau) \in [-\frac{1}{2}, \frac{1}{2}),\ \text{such that } |\tau| > 1 \text{ if } \mathrm{Re}(\tau) > 0\}$ of $\mathbb{H}$. If the sequence of the imaginary parts $\mathrm{Im}(\tau_1), \mathrm{Im}(\tau_2), \ldots$ is unbounded, then $f(\tau_1), f(\tau_2), \ldots$ has a subsequence converging to $f(\infty)$, which exists by above. If the sequence of the imaginary parts is bounded, then the τ_k, $k \geq 1$, lie in a compact subset $\Omega \subseteq \mathbb{H}$ as in the proof of Lemma 2.5.11. It follows that we can find the desired converging subsequence. Thus $f(\mathbb{H} \cup \{\infty\})$ is compact.
Since f is holomorphic on $\mathbb{H}$ and at ∞, it is continuous on $\mathbb{H} \cup \{\infty\}$. Moreover, the absolute value function $|\cdot| : \mathbb{C} \to \mathbb{R}$ is continuous, hence $|f|$ is continuous on $\mathbb{H} \cup \{\infty\}$ as well. Since its image is compact, $|f|$ attains a maximum there, and the Maximum modulus principle 1.0.9 then implies that f is constant.
"(ii)": Let f be a modular function for $\Gamma(1)$ that is holomorphic on $\mathbb{H}$. Since f is meromorphic at the cusps by definition, its q-expansion only has finitely many terms with negative powers of q. Since by Corollary 4.2.2 the q-expansion of j starts with $\frac{1}{q}$, we can find a polynomial $A(x) \in \mathbb{C}[x]$, such that $f(\tau) - A(j(\tau))$ is holomorphic at ∞. As f is also holomorphic on $\mathbb{H}$, f is constant by (i). Thus $f(\tau)$ is a polynomial in $j(\tau)$. □

Proposition 4.2.5. *Every modular function for* $\Gamma(1)$ *is a rational function in* $j(\tau)$*, i.e.* $\mathbb{C}(\Gamma(1)) = \mathbb{C}(j)$.

Proof. Let f be a modular function for $\Gamma(1)$. We want to find a polynomial $B(x) \in \mathbb{C}[x]$, such that $B(j(\tau))f(\tau)$ is holomorphic on $\mathbb{H}$, which will imply that $f(\tau)$ is a rational function in $j(\tau)$ by the previous lemma. Since f has a meromorphic q-expansion, f only has finitely many poles in the fundamental domain $\mathcal{F}$ and since f is $\Gamma(1)$-invariant, Lemma 2.5.11 implies that every pole of f is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to one in $\mathcal{F}$. Therefore, it suffices to eliminate the poles in $\mathcal{F}$: if f has a pole of order m at $\tau_0 \in \mathcal{F}$, then $(j(\tau) - j(\tau_0))^m f(\tau)$ is holomorphic at τ_0. By repeating this process for each pole in $\mathcal{F}$, we construct a polynomial $B(x)$ such that $B(j(\tau))$ has no poles in $\mathcal{F}$ is holomorphic on $\mathbb{H}$. It follows that $f(\tau)$ is a rational function in $j(\tau)$. □

Proposition 4.2.6. *Let* Γ *be a congruence subgroup. The field* $\mathbb{C}(\Gamma)$ *of modular functions for* Γ *is a finite extension of* $\mathbb{C}(j)$ *of degree at most* $[\Gamma(1) : \Gamma]$.

Proof. Let $n = [\Gamma(1) : \Gamma]$ and let γ_1 be the identity in $\Gamma(1)$. Moreover, let $\Gamma \subseteq \Gamma(1)$ be a subgroup and $\{\gamma_1, \ldots, \gamma_n\} \subseteq \Gamma(1)$ a set of right coset representatives for Γ, i.e. we have $\Gamma(1) = \Gamma\gamma_1 \biguplus \ldots \biguplus \Gamma\gamma_n$. Now let $f \in \mathbb{C}(\Gamma)$, and for $i \in I \coloneqq \{1, \ldots, n\}$ define $f_i(\tau) = f(\gamma_i\tau)$. Since f is Γ-invariant, we have $f(\gamma_i\tau) = f(\gamma_i'\tau)$ for any $\gamma_i' \in \Gamma\gamma_i$. Moreover, for any $\gamma \in \Gamma(1)$, multiplication on the right by γ permutes the cosets $\{\Gamma\gamma_i\}_{i\in I}$, so that as sets $\{f(\gamma_i\gamma\tau)\}_{i\in I} = \{f(\gamma_i\tau)\}_{i\in I}$. Since f is meromorphic at the cusps and $\Gamma(1)$-invariant, each f_i inherits these properties. Consequently, any symmetric polynomial in the f_i's is meromorphic at the cusps and $\Gamma(1)$-invariant, and is therefore an element of $\mathbb{C}(j)$ by Proposition 4.2.5. Now consider the monic polynomial

$$P(Y) = \prod_{i\in I}(Y - f_i),$$

which has degree n and coefficients in $\mathbb{C}(j)$, since the coefficients are symmetric polynomials in the f_i. Note that $f = f_1$ is a root of P, as γ_1 is the identity. It follows that every $f \in \mathbb{C}(j)$ is a root of a monic polynomial in $\mathbb{C}(j)[Y]$ of degree n. Hence, $\mathbb{C}(\Gamma)/\mathbb{C}(j)$ is an algebraic extension. Since we are in characteristic zero, it is also separable.
We claim that that $\mathbb{C}(\Gamma)$ is finitely generated over $\mathbb{C}(j)$. Suppose the contrary. Then there exist elements $g_1, \dots g_{n+1} \in \mathbb{C}(\Gamma)$ such that

$$\mathbb{C}(j) \subsetneq \mathbb{C}(j)(g_1) \subsetneq \mathbb{C}(j)(g_1, g_2) \subsetneq \dots \subsetneq \mathbb{C}(j)(g_1, \cdots g_{n+1}).$$

But then $\mathbb{C}(j)(g_1, \dots g_{n+1})$ is a finite separable extension if $\mathbb{C}(j)$ of degree at least $n+1$, and by the Primitive element theorem (1.0.10) it must be a simple extension, i.e. generated by a single element $g \in \mathbb{C}(\Gamma)$ of degree at least $n+1$. This is a contradiction, so we conclude that $[\mathbb{C}(\Gamma) : \mathbb{C}(j)] \leq n$. A symmetric argument, considering the construction of f_i and the monic polynomial $P(Y)$, shows that $[\mathbb{C}(\Gamma) : \mathbb{C}(j)] \geq n$. Therefore, equality holds, which concludes the proof. □

Generally, the equality $[\mathbb{C}(\Gamma) : \mathbb{C}(j)] = [\Gamma(1) : \Gamma]$ holds if $-I \in \Gamma$, which we will prove for the congruence subgroup $\Gamma_0(N)$ in the next section.

4.3 Modular functions for $\Gamma_0(N)$

Having seen that the j-function is central to our study of modular functions for $\Gamma(1)$, we now build on this foundation to consider modular functions for the congruence subgroup $\Gamma_0(N)$. Similar ideas will allow us to explore a richer structure of modular relationships.

Theorem 4.3.1. *The function $j_N(\tau) \coloneqq j(N\tau)$ is a modular function for $\Gamma_0(N)$.*

Proof. As $j(\tau)$ is a modular function for $\Gamma(1)$ by the previous section, it is also a modular function for any congruence subgroup, in particular for $\Gamma_0(N)$ by (4.1). Hence, $j_N(\tau)$ is meromorphic on $\mathbb{H}$ and meromorphic at the cusps. It remains to show that $j_N(\tau)$ is $\Gamma_0(N)$-invariant. Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$. Then $c \equiv 0 \bmod N$ and

$$j_N(\gamma\tau) = j(N\gamma\tau) = j\left(\frac{N(a\tau+b)}{c\tau+d}\right) = j\left(\frac{aN\tau+b\tau}{\frac{c}{N}N\tau+d}\right) = j(\gamma' N\tau) = j(N\tau) = j_N(\tau),$$

since the j-function is $\mathrm{SL}_2(\mathbb{Z})$-invariant, where $\gamma' = \left(\begin{smallmatrix} a & bN \\ \frac{c}{N} & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ because $\frac{c}{N}$ is an integer and $\det(\gamma') = \det(\gamma) = 1$. Thus, $j_N(\tau)$ is indeed $\Gamma_0(N)$-invariant. □

Theorem 4.3.2. *The field of modular functions for $\Gamma_0(N)$ is an extension of $\mathbb{C}(j)$ of degree $[\Gamma(1) : \Gamma_0(N)]$ generated by $j_N(\tau)$.*

Proof. Let $n = [\Gamma(1) : \Gamma_0(N)]$. By the previous theorem, we have $j_N \in \mathbb{C}(\Gamma_0(N))$, so $\mathbb{C}(j_N) \subseteq \mathbb{C}(\Gamma_0(N))$. Since $\mathbb{C}(\Gamma_0(N))$ is a finite extension of $\mathbb{C}(j)$ of degree at most n by Proposition 4.2.6, the degree formula gives

$$[\mathbb{C}(\Gamma_0(N)) : \mathbb{C}(j)] = [\mathbb{C}(\Gamma_0(N)) : \mathbb{C}(j_N)] \cdot [\mathbb{C}(j_N) : \mathbb{C}(j)],$$

so it suffices to show that the minimal polynomial of j_N over $\mathbb{C}(j)$ has degree at least n. As in the previous proof, let $\{\gamma_1, \ldots, \gamma_n\} \subseteq \Gamma(1)$ be a set of right coset representatives for $\Gamma_0(N)$ and let $P \in \mathbb{C}(j)[Y]$ be the minimal polynomial of $j_N(\tau)$ over $\mathbb{C}(j)$. Then we have $P(j(\tau), j_N(\tau)) = 0$. Replacing τ by $\gamma_i\tau$ for each $i = 1, \ldots, n$, we get

$$0 = P(j(\gamma_i\tau), j_N(\gamma_i\tau)) = P(j(\tau), j_N(\gamma_i\tau)),$$

since j is $\Gamma(1)$-invariant by Theorem 2.5.9. Hence each function $j_N(\gamma_i\tau)$ is a root of P. To prove that $\deg(P) \geq n$, we show that the functions $j_N(\gamma_i\tau)$, $i = 1, \ldots, n$, are distinct. Suppose they are not. Then there exist $0 \leq i, k \leq n$ with $i \neq k$ and $\tau \in \mathbb{H}$ such that $j_N(\gamma_i\tau) = j_N(\gamma_k\tau)$. Consider the fundamental domain $\mathcal{F}$ for $\mathbb{H}/\Gamma(1)$ from Theorem 2.5.11, and pick $\alpha, \beta \in \Gamma(1)$ such that $\alpha N\gamma_i\tau, \beta N\gamma_k\tau \in \mathcal{F}$. Since j is injective on $\mathcal{F}$ by Theorem 2.5.12, we have

$$j(\alpha N\gamma_i\tau) = j(\beta N\gamma_k\tau) \quad \iff \quad \alpha N\gamma_i\tau = \pm\beta N\gamma_k\tau \quad \iff \quad \alpha N\gamma_i = \pm\beta N\gamma_k.$$

Here N is viewed as the matrix $\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)$, since $N\tau = \frac{N\tau+0}{0\tau+1}$. Now let $\gamma = \alpha^{-1}\beta = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then the above equivalence gives

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

so that

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

Since $\gamma_i\gamma_k^{-1} \in \mathrm{SL}_2(\mathbb{Z})$ as it is a group, we have $\frac{b}{N} \in \mathbb{Z}$ and $cN \equiv 0 \bmod N$, hence $\gamma_i\gamma_k^{-1} \in \Gamma_0(N)$. It follows that $\gamma_i \in \Gamma_0(N)\gamma_k$ and so γ_i and γ_k lie in the same right coset of $\Gamma_0(N)$, contradicting the choice of distinct coset representatives. Therefore, the functions $j_N(\gamma_i\tau)$ are all distinct, and the minimal polynomial of j_N over $\mathbb{C}(j)$ has degree n. This completes the proof. □

Note that this theorem implies that the field of modular functions for $\Gamma_0(N)$ is equal to $\mathbb{C}(j(\tau), j_N(\tau))$, since $\mathbb{C}(j(\tau))(j_N(\tau)) = \mathbb{C}(j(\tau), j_N(\tau))$. Therefore, every modular function for $\Gamma_0(N)$ is a rational function in $j(\tau)$ and $j(N\tau)$.

4.4 The modular polynomial

With the structure of modular functions for $\Gamma_0(N)$ in hand, we now turn to the modular polynomial. This polynomial encodes the algebraic relations between the values of the j-function at related points and provides a key tool for understanding the arithmetic properties of modular functions, including the integrality of its coefficients.

Definition 4.4.1 (Modular polynomial)**.** The minimal polynomial of j_N over $\mathbb{C}(j)$ is called the modular polynomial and is denoted by Φ_N.

By the proof of the previous theorem, we can write the modular polynomial Φ_N as

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

where $\{\gamma_1, \ldots, \gamma_n\} \subseteq \Gamma(1)$ is a set of right coset representatives for $\Gamma_0(N)$ with $n = [\Gamma(1) : \Gamma_0(N)]$. Its coefficients are symmetric polynomials in the values $j_N(\gamma_i\tau)$ and hence $\Gamma(1)$-invariant, as in the proof of Proposition 4.2.6. Since these coefficients are also holomorphic on $\mathbb{H}$, as $j(\tau)$ is, Lemma 4.2.4 implies that they are polynomials in $j(\tau)$. Therefore, we have $\Phi_N \in \mathbb{C}(j)[Y]$.

By introducing a new variable X in place of $j(\tau)$, we may view $\Phi_N(j(\tau), j(N\tau))$ as a polynomial $\Phi_N(X, Y) \in \mathbb{C}[X, Y]$. Our next goal is to show that the coefficients of $\Phi_N(X, Y)$ are actually integers. To this end, we first fix a set of right coset of right representatives for $\Gamma_0(N)$ in $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$.

In the next lemma and in the subsequent proofs, we restrict ourselves to prime N, as this case is sufficient for proving the First main theorem of complex multiplication and covers the most practical applications (such as the SEA algorithm). The proof for composite N is essentially the same, but explicitly determining a set of right coset representatives γ_i and computing the q-expansions of the functions $j_N(\gamma_i\tau)$ is slightly more complicated.

Lemma 4.4.2. *Let N be prime. The right cosets of $\Gamma_0(N)$ in $\Gamma(1)$ are of the form*

$$\{\Gamma_0(N)\} \cup \left\{\Gamma_0(N) S T^k \mid 0 \leq k < N\right\},$$

where $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ are the generators of $\Gamma(1)$.

Proof. We first show that these cosets cover $\Gamma(1)$. Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$. If $c \equiv 0 \bmod N$, then $\gamma \in \Gamma_0(N)$ and so it lies in the first coset. Otherwise choose $k \in [0, N-1]$, such that $kc \equiv d \bmod N$, which is possible since c is nonzero modulo N. Moreover, let $\gamma_0 = \left(\begin{smallmatrix} ka-b & a \\ kc-d & c \end{smallmatrix}\right) \in \Gamma_0(N)$, then

$$\gamma_0 S T^k = \begin{pmatrix} ka - b & a \\ kc - d & c \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \gamma,$$

which lies in $\Gamma_0(N) S T^k$, the second coset.
It remains to show that the cosets are distinct. Suppose they are not. Then there exist $\gamma_1, \gamma_2 \in \Gamma_0(N)$ such that one of the following cases occurs:
Case 1: $\gamma_1 = \gamma_2 S T^k$ for some $0 \leq k < N$. Let $\gamma_2 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$. Then

$$\gamma_1 = \gamma_2 S T^k = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix} = \begin{pmatrix} b & bk - a \\ d & dk - c \end{pmatrix}.$$

Since $\gamma_1 \in \Gamma_0(N)$, we must have $d \equiv 0 \bmod N$. But $\gamma_2 \in \Gamma_0(N)$ implies $c \equiv 0 \bmod N$, so $\det(\gamma_2) = ad - bc \equiv 0 \bmod N$, contradicting $\gamma_2 \in \Gamma_0(N)$.

Case 2: $\gamma_1 ST^j = \gamma_2 ST^k$ with $0 \leq j < k < N$. Let $m = k - j$. Then

$$\gamma_1 = \gamma_2 ST^m S^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & m \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} a - bm & b \\ c - dm & d \end{pmatrix}.$$

Again, since $\gamma_1 \in \Gamma_0(N)$, we have $c - dm \equiv 0 \bmod N$. But $\gamma_2 \in \Gamma_0(N)$ implies $c \equiv 0 \bmod N$ and since $m \not\equiv 0 \bmod N$, this implies $d \equiv 0 \bmod N$. Therefore, $\det(\gamma_2) = ad - bc \equiv 0 \bmod N$, which contradicts $\gamma_2 \in \Gamma_0(N)$.
Thus, in both cases, we reach a contradiction, showing that the cosets are indeed distinct. □

Lemma 4.4.3 (Hasse q-expansion principle)**.** *Let f be a modular function for $\Gamma(1)$ that is holomorphic on $\mathbb{H}$ and whose q-expansion has coefficients lying in an additive subgroup A of $\mathbb{C}$. Then f is a polynomial in $j(\tau)$ with coefficients in A.*

Proof. Since we know that $f(\tau) = P(j(\tau))$ for some $P \in \mathbb{C}[X]$ by Lemma 4.2.4, we just need to show that $P \in A[X]$. We prove the claim by induction on $d = \deg(P)$.
The statement is clear for $d = 0$, so we may assume $d > 0$ and that the claim holds for polynomials of degree $d - 1$. Let $P \in \mathbb{C}[X]$ have degree $d = \deg(P)$. Since the q-expansion of $j(\tau)$ begins with q^{-1} by Corollary 4.2.2, the q-expansion of $f = P \circ j$ has the form

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

with $a_n \in A$ and $a_{-d} \neq 0$. Set $P_1(X) = P(X) - a_{-d}X^d$ and $f_1(\tau) = P_1(j(\tau)) = f(\tau) - a_{-d}j(\tau)^d$. By induction hypothesis, $P_1(X)$ has coefficients in A, and hence also the q-expansion of $f_1(X)$ does. Therefore, also $P(X) = P_1(X) + a_{-d}X^d$ has coefficients in A, which concludes the proof. □

For the last proof in this section, recall that for $N \geq 1$, the cyclotomic field $\mathbb{Q}(\zeta_N)$ is the field extension of $\mathbb{Q}$ obtained by adjoining a primitive N-th root of unity $\zeta_N = e^{\frac{2\pi i}{N}}$. Since the roots of the minimal polynomial of ζ_N, the N-th cyclotomic polynomial, are precisely the distinct powers of ζ_N, $\mathbb{Q}(\zeta_N)$ is its splitting field over $\mathbb{Q}$. Moreover, as $\mathbb{Q}$ has characteristic zero, the minimal polynomial is separable, so the extension $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ is Galois. The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ is naturally isomorphic to the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^*$ with an element $r \in (\mathbb{Z}/N\mathbb{Z})^*$ corresponding to the automorphism σ_r defined by $\sigma_r(\zeta_N) = \zeta_N^r$.

Theorem 4.4.4. *Let N be a positive integer. Then $\Phi_N \in \mathbb{Z}[X, Y]$.*

Proof. We prove the theorem for prime N, see the comment above.
Let $\gamma_k = ST^k$. Using Lemma 4.4.2 we have

$$\Phi_N(Y) = (Y - j_N(\tau)) \prod_{k=0}^{N-1} (Y - j_N(\gamma_k \tau)).$$

Now let $f(\tau)$ be a coefficient of $\Phi_N(Y)$. Then $f(\tau)$ is a holomorphic function on $\mathbb{H}$ since $j(\tau)$ is. Moreover, $f(\tau)$ is $\Gamma(1)$-invariant as in the proof of Proposition 4.2.6, since it is a symmetric polynomial in $j_N(\tau)$ and the functions $j_N(\gamma_k\tau)$, which correspond to a complete set of right coset representatives for $\Gamma_0(N)$. Finally, $f(\tau)$ is meromorphic at the cusps since $j_N(\tau)$ and the functions $j_N(\gamma_k\tau)$ are, giving that $f(\tau)$ is a modular function for $\Gamma(1)$. Thus $f(\tau)$ is a polynomial in $j(\tau)$ by Lemma 4.2.4.
We now show that the q-expansion of $f(\tau)$ has integer coefficients; it then will follow that $f(\tau)$ is an integer polynomial in $j(\tau)$ by Lemma 4.4.3 and therefore $\Phi_N \in \mathbb{Z}[X,Y]$. As first step, we show that the q-expansion of $f(\tau)$ has rational coefficients. Using $q = q(\tau) = e^{2\pi i\tau}$, Corollary 4.2.2 gives

$$j_N(\tau) = \frac{1}{q^N} + 744 + \sum_{n=1}^{\infty} a_n q^{nN},$$

with coefficients $a_n \in \mathbb{Z}$ (the integrality of these coefficients will be justified in Chapter 7.). This shows $j_N \in \mathbb{Z}((q))$. Moreover, we have

$$\begin{aligned} j_N(\gamma_k\tau) = j(N\gamma_k\tau) &= j\left(\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} ST^k\tau\right) = j\left(S\begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix}\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}\tau\right) \\ &= j\left(\begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix}\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}\tau\right) = j\left(\begin{pmatrix} 1 & k \\ 0 & N \end{pmatrix}\tau\right) = j\left(\frac{\tau+k}{N}\right), \end{aligned}$$

since $\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)S = S\left(\begin{smallmatrix} 1 & 0 \\ 0 & N \end{smallmatrix}\right)$ and $j(\tau)$ is $\Gamma(1)$-invariant. Now let $\zeta_N = e^{\frac{2\pi i}{N}}$. Then

$$q\left(\frac{\tau+k}{N}\right) = e^{2\pi i\frac{\tau+k}{N}} = e^{2\pi i\frac{\tau}{N}}e^{2\pi i\frac{k}{N}} = q^{\frac{1}{N}}\zeta_N^k.$$

and using the above q-expansion we obtain

$$j_N(\gamma_k\tau) = j\left(\frac{\tau+k}{N}\right) = \frac{\zeta_N^{-k}}{q^{\frac{1}{N}}} + \sum_{n=0}^{\infty} a_n\zeta_N^{kn}q^{\frac{n}{N}}.$$

Hence $j_N(\gamma_k\tau)$ lies in the field of formal Laurent series $\mathbb{Q}(\zeta_N)((q^{\frac{1}{N}}))$, i.e. the field of formal Laurent series in powers of $q^{\frac{1}{N}}$ and coefficients in the cyclotomic field $\mathbb{Q}(\zeta_N)$.
We claim that $f(\tau)$ is contained in the smaller field $\mathbb{Q}((q^{\frac{1}{N}}))$, which we show using Galois theory. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, acting on the coefficients of the Laurent series by $\zeta_N \mapsto \zeta_N^r$ for some $r \in (\mathbb{Z}/N\mathbb{Z})^*$. This Galois action permutes the functions $j_N(\gamma_k\tau)$, since $\sigma(j_N(\gamma_k\tau)) = j_N(\gamma_{rk}\tau)$ and leaves $j_N(\tau)$ fixed. Since $f(\tau)$ is a symmetric polynomial in the $j_N(\gamma_k\tau)$, it is invariant under this action, i.e. $\sigma(f(\tau)) = f(\tau)$. Therefore, all coefficients of the q-expansion of $f(\tau)$ are fixed under this Galois action, and hence lie in the fixed field of $\mathbb{Q}(\zeta_N)$, namely in $\mathbb{Q}$. Thus,

$$f \in \mathbb{Q}((q^{\frac{1}{N}})).$$

However, since $f(\tau)$ is a polynomial in $j(\tau)$, whose expansion involves only integer powers of q, its q-expansion cannot contain fractional powers of q. It follows that

$$f(\tau) \in \mathbb{Q}((q)),$$

the field of formal Laurent series with integer powers of q and rational coefficients. Moreover, the coefficients of the q-expansion of $j(N\tau) = j_N(\tau)$ are integers by above and hence are algebraic integers. For $j_N(\gamma_k\tau) = j(\frac{\tau+k}{N})$, the argument of the function involves a translation and scaling, which leads to an expansion in powers of $q^{\frac{1}{N}}$ with coefficients in $\mathbb{Z}[\zeta_N]$. These coefficients lie in the ring of integers of a cyclotomic field and thus are algebraic integers. Consequently, since $f(\tau)$ is a symmetric polynomial in the $j_N(\gamma_k\tau)$, its coefficients are algebraic integers as well, i.e.

$$f(\tau) \in \mathbb{Z}((q)),$$

By the Hasse q-expansion principle 4.4.3, we conclude that $f(\tau)$ is an integer polynomial in $j(\tau)$ and therefore $\Phi_N \in \mathbb{Z}[X, Y]$. □

4.5 Modular functions for $\Gamma_0(N)$: explicit form

Since every modular function for $\Gamma_0(N)$ can be expressed in terms of $j(\tau)$ and $j(N\tau)$ by Theorem 4.3.2, it is natural to seek a more explicit description of this dependence. Such a formula, derived via the modular polynomial Φ_N, will not only clarify the structure of these functions but will also be instrumental for the arithmetic applications in Chapter 6.

As in the previous section, we express the modular polynomial Φ_N as

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

where $\{\gamma_1, \ldots, \gamma_n\}$ is a set of right coset representatives for $\Gamma_0(N)$ in $\Gamma(1)$ with $n = [\Gamma(1) : \Gamma_0(N)]$. Now let f be a modular function for $\Gamma_0(N)$. To describe the structure of modular functions for $\Gamma_0(N)$, we introduce the auxiliary function

$$\begin{aligned} G(\tau, Y) &:= \Phi_N(j(\tau), Y) \sum_{i=1}^{n} \frac{f(\gamma_i\tau)}{Y - j(N\gamma_i\tau)} \\ &= \sum_{i=1}^{n} f(\gamma_i\tau) \prod_{\substack{k=1 \\ k\neq i}}^{n} (Y - j(N\gamma_k\tau)). \end{aligned}$$

Proposition 4.5.1. *Let f be a modular function for $\Gamma_0(N)$. Then f has the form*

$$f(\tau) = \frac{G(j(\tau), j(N\tau))}{\frac{\partial \Phi_N}{\partial Y}(j(\tau), j(N\tau))},$$

where $\Phi_N(X, Y)$ denotes the modular polynomial.

Proof. By definition, $G(\tau, Y)$ is a polynomial in Y, and we first show that its coefficients are modular functions for $\Gamma(1)$. The coefficients of $G(\tau, Y)$ are polynomials in the functions $f(\gamma_i\tau)$ and $j(N\gamma_k\tau)$, both of which are meromorphic on $\mathbb{H}$. Since sums and products of meromorphic functions are meromorphic, it follows that the coefficients of $G(\tau, Y)$ are meromorphic on $\mathbb{H}$. Moreover, these coefficients are symmetric polynomials in the $f(\gamma_i\tau)$ and $j(N\gamma_k\tau)$, so they are $\Gamma(1)$-invariant as in the proof of Proposition 4.2.6. Finally, since $f(\tau)$ and $j(N\tau)$ are meromorphic at the cusps, the same holds for $f(\gamma\tau)$ and $j(N\gamma\tau)$ for every $\gamma \in \Gamma(1)$, as elements of $\Gamma(1)$ permute the cusps (see Section 4.1). Therefore, the coefficients of $G(\tau, Y)$ are modular functions for $\Gamma(1)$.
By Proposition 4.2.5, this implies that the coefficients of $G(\tau, Y)$ are rational functions in $j(\tau)$ i.e. $G(\tau, Y) \in \mathbb{C}(j(\tau))[Y]$. Since the coefficients of $G(\tau, Y)$ are functions in τ by definition, we deduce that $G(\tau, Y)$ can be written as a polynomial of the form $G(j(\tau), Y)$. Now, assume that γ_1 is the identity element in $\Gamma(1)$. Then, by the product rule we get

$$\begin{aligned}
\frac{\partial \Phi_N}{\partial Y}(j(\tau), j(N\tau)) &= \frac{\partial}{\partial Y}\left(\prod_{k=1}^{n}(Y - j(N\gamma_k\tau))\right)(j(\tau), j(N\tau)) \\
&= \left(\prod_{k=1}^{n}(j(N\tau) - j(N\gamma_k\tau))\right)\left(\sum_{k=1}^{n}\frac{\frac{\partial}{\partial Y}(Y - j(N\gamma_k\tau))}{j(N\tau) - j(N\gamma_k\tau)}\right) \\
&= \left(\prod_{k=1}^{n}(j(N\tau) - j(N\gamma_k\tau))\right)\left(\sum_{k=1}^{n}\frac{1}{j(N\tau) - j(N\gamma_k\tau)}\right) \\
&= \sum_{k=1}^{n}\frac{\prod_{k=1}^{n}(j(N\tau) - j(N\gamma_k\tau))}{j(N\tau) - j(N\gamma_k\tau)} \\
&= \sum_{i=1}^{n}\prod_{\substack{k=1 \\ k\neq i}}^{n}(j(N\tau) - j(N\gamma_k\tau)) \\
&= \prod_{k=2}^{n}(j(N\tau) - j(N\gamma_k\tau)),
\end{aligned}$$

where in the last step all the other terms in the product involving the identity element vanish since $j(N\tau) - j(N\gamma_1\tau) = 0$. Using the definition of $G(j(\tau), Y)$ and substituting $Y = j(N\tau)$ yields

$$\begin{aligned}
G(j(\tau), j(N\tau)) &= \sum_{i=1}^{n} f(\gamma_i\tau)\prod_{\substack{k=1 \\ k\neq i}}^{n}(j(N\tau) - j(N\gamma_k\tau)) \\
&= f(\tau)\prod_{k=2}^{n}(j(N\tau) - j(N\gamma_k\tau)) \\
&= f(\tau)\ \frac{\partial \Phi_N}{\partial Y}(j(\tau), j(N\tau)).
\end{aligned}$$

In the second equality, we again used the fact that all product terms involving the identity element vanish. Since Φ_N is the minimal polynomial of j_N by definition and hence

irreducible, it follows that Φ_N is separable, as we work in characteristic 0. Therefore, $\frac{\partial \Phi_N}{\partial Y}(j(\tau), j(N\tau)) \neq 0$ and obtain

$$f(\tau) = \frac{G(j(\tau), j(N\tau))}{\frac{\partial \Phi_N}{\partial Y}(j(\tau), j(N\tau))},$$

the desired expression. □

Theorem 4.5.2. *Let $f(\tau)$ be a modular function for $\Gamma_0(N)$ whose q-expansion has rational coefficients. Then*

(i) $f(\tau) \in \mathbb{Q}(j(\tau), j(N\tau))$.

(ii) Assume in addition that $f(\tau)$ is holomorphic on $\mathbb{H}$, and let $\tau_0 \in \mathbb{H}$. Then

$$\frac{\partial \Phi_N}{\partial Y}(j(\tau_0), j(N\tau_0)) \neq 0 \implies f(\tau_0) \in \mathbb{Q}(j(\tau_0), j(N\tau_0)),$$

where Φ_N denotes the modular polynomial.

Proof. By the previous proposition, we can express an arbitrary modular function f for $\Gamma_0(N)$ as

$$f(\tau) = \frac{G(j(\tau), j(N\tau))}{\frac{\partial \Phi_N}{\partial Y}(j(\tau), j(N\tau))},$$

where $G(j(\tau), Y)$ is a polynomial in Y defined by

$$G(j(\tau), Y) = \Phi_N(j(\tau), Y) \sum_{i=1}^{n} \frac{f(\gamma_i \tau)}{Y - j(N\gamma_i \tau)},$$

whose coefficients are rational functions in $j(\tau)$. Therefore, to prove part (i), it suffices to show that both the numerator and the denominator of $f(\tau)$ lie in $\mathbb{Q}(j(\tau), j(N\tau))$. Note that the claim always holds if $f(\tau)$ is the zero function. Otherwise, since $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$ by Theorem 4.4.4, its partial derivative also lies in $\mathbb{Z}[X, Y]$, so in particular in $\mathbb{Q}[X, Y]$. Hence, the denominator $\frac{\partial \Phi_N}{\partial Y}(j(\tau), j(N\tau))$ lies in $\mathbb{Q}(j(\tau), j(N\tau))$. For the numerator, again by the proof of Proposition 4.5.1, we have that $G(j(\tau), j(N\tau))$ lies in $\mathbb{C}(j(\tau))[j(N\tau)]$, i.e. it is a polynomial in $j(N\tau)$ with coefficients that are rational functions in $j(\tau)$. Thus, we can write

$$G(j(\tau), j(N\tau)) = \frac{P(j(\tau), j(N\tau))}{Q(j(\tau))},$$

where $P(X, Y)$ and $Q(X) \neq 0$ are polynomials with complex coefficients. Explicitly, let $P(X, Y) = \sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} X^i Y^j$ and $Q(X) = \sum_{k=0}^{l} b_l Y^l$ with $a_{ij}, b_k \in \mathbb{C}$ not all zero. Then

$$\begin{aligned} f(\tau) &= \frac{\frac{P(j(\tau), j(N\tau))}{Q(j(\tau))}}{\frac{\partial \Phi_N}{\partial Y}(j(\tau), j(N\tau))} = \frac{P(j(\tau), j(N\tau))}{Q(j(\tau)) \frac{\partial \Phi_N}{\partial Y}(j(\tau), j(N\tau))} \\ &= \frac{\sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} j(\tau)^i j(N\tau)^j}{\left(\sum_{k=0}^{l} b_k j(N\tau)^k\right) \frac{\partial \Phi_N}{\partial Y}(j(\tau), j(N\tau))}, \end{aligned}$$

and rearranging yields

$$\sum_{i=0}^{n}\sum_{j=0}^{m} a_{ij} j(\tau)^i j(N\tau)^j = f(\tau)\left(\sum_{k=0}^{l} b_k j(N\tau)^k\right)\frac{\partial \Phi_N}{\partial Y}(j(\tau), j(N\tau)).$$

Now we use the q-expansions of $f(\tau), j(\tau)$ and $j(N\tau)$ to equate the coefficients of $q^{1/N}$. On one hand, since $j(\tau)$ and $j(N\tau)$ admit infinite q-expansions, raising them to various powers and multiplying them produces infinitely many terms in q. Consequently, equating the coefficients of each power of q yields infinitely many equations. Moreover, as the expressions on both sides of the equation are linear in the unknowns a_{ij} and b_k, the resulting system is homogeneous and linear. On the other hand, although the number of unknowns a_{ij} and b_k is finite by definition of the polynomials P and Q, substituting the infinite q-expansions of $f(\tau), j(\tau)$ and $j(N\tau)$ produces infinitely many equations in these variables. Thus, the system is underdetermined and therefore has a non-trivial solution over $\mathbb{C}$.

By Corollary 4.2.2, the q-expansions of $j(\tau)$ and $j(N\tau)$ have integer, and hence rational coefficients. By assumption, the q-expansion of $f(\tau)$ also has rational coefficients, and $\frac{\partial \Phi_N}{\partial Y}(j(\tau), j(N\tau))$ has rational coefficients as shown earlier. Hence, all coefficients in the infinite homogeneous system of linear equations lie in $\mathbb{Q}$. It follows that the solution space is a $\mathbb{Q}$-vector space, and since the system has a non-trivial solution over $\mathbb{C}$, it also has a non-trivial solution over $\mathbb{Q}$.

In particular, since $Q(j(\tau)) \neq 0$, the solution is non-trivial in the coefficients b_k.

As the unknowns arise only through rational combinations of the a_{ij} and b_k with the integer coefficients of the q-expansions of $f(\tau), j(\tau)$ and $j(N\tau)$, is follows that all a_{ij} and b_k are rational. Thus, the polynomials $P(X, Y)$ and $Q(X)$ can be chosen with rational coefficients, so that the numerator $G(j(\tau), j(N\tau))$ lies in $\mathbb{Q}(j(\tau), j(N\tau))$. This completes the proof of (i).

For part (ii), assume in addition that $f(\tau)$ is holomorphic on $\mathbb{H}$. Since $j(\tau)$ is also holomorphic on $\mathbb{H}$, and products of holomorphic functions are holomorphic, it follows that the coefficients of $G(j(\tau), Y)$ are holomorphic functions on $\mathbb{H}$. Moreover, by the proof of Proposition 4.5.1, these coefficients are modular functions for $\Gamma(1)$. Hence, by Lemma 4.2.4, they are polynomials in $j(\tau)$. Therefore, we can write

$$G(j(\tau), j(N\tau)) = P(j(\tau), j(N\tau)),$$

for some polynomial $P(X, Y)$ with complex coefficients. By an argument analogous to part (i), we can show that the coefficients of $P(X, Y)$ are rational. Indeed, if $f(\tau)$ is the zero-function, the claim clearly holds. Otherwise, write $P(X, Y) = \sum_{i=0}^{n}\sum_{j=0}^{m} a_{ij} X^i Y^j$ with $a_{ij} \in \mathbb{C}$ not all zero as above, so that

$$f(\tau) = \frac{P(j(\tau), j(N\tau))}{\frac{\partial \Phi_N}{\partial Y}(j(\tau), j(N\tau))} = \frac{\sum_{i=0}^{n}\sum_{j=0}^{m} a_{ij} X^i Y^j}{\frac{\partial \Phi_N}{\partial Y}(j(\tau), j(N\tau))}.$$

Hence,

$$\sum_{i=0}^{n}\sum_{j=0}^{m} a_{ij} j(\tau)^i j(N\tau)^j = f(\tau)\frac{\partial \Phi_N}{\partial Y}(j(\tau), j(N\tau)).$$

Substituting the q-expansions of $f(\tau), j(\tau)$ and $j(N\tau)$ as before yields an infinite system of inhomogeneous linear equations in the unknowns a_{ij}. Due to the infinite series expansions, this again leads to infinitely many equations involving finitely many variables a_{ij}, hence the system is underdetermined and therefore has a non-trivial solution over $\mathbb{C}$. As before, all coefficients in this system are rational, since the q-expansions $f(\tau), j(\tau)$ and $jN\tau)$, as well as $\frac{\partial \Phi_N}{\partial Y}(j(\tau), j(N\tau))$ have rational coefficients.
The solution set of an inhomogeneous linear system is obtained by the translating the solution space of the corresponding homogeneous system by a particular solution of the inhomogeneous one. Since the homogeneous system has a non-trivial solution over $\mathbb{Q}$ by the same argument as in part (i), and the inhomogeneous part has rational coefficients, any solution obtained via rational operations (for instance, Gaussian elimination) will also be rational. Thus, the solution space of the inhomogeneous system consists entirely of rational vectors. Choosing any such rational solution determines the coefficients a_{ij}, which are therefore rational. Hence $P(X, Y) \in \mathbb{Q}[X, Y]$.
Finally, whenever the denominator $\frac{\partial \Phi_N}{\partial Y}(j(\tau), j(N\tau))$ does not vanish at $\tau_0 \in \mathbb{H}$, we can evaluate $f(\tau)$ at τ_0 and conclude that $f(\tau_0) \in \mathbb{Q}(j(\tau_0), j(N\tau_0))$, which completes the proof of (ii). □

To apply the previous theorem to special values of modular functions, we need to ensure that the denominator does not vanish. The next lemma provides sufficient conditions for this. In order to state it, we first recall some basic notions.

As noted in Remark 3.3.2, every order $\mathcal{O}$ is a lattice, so we may write $\mathcal{O} = [1, \omega]$ with $\omega \in K$, where K is an imaginary quadratic number field.

Recall further that for an imaginary quadratic number field $K = \mathbb{Q}(\sqrt{d})$, the *norm* and *trace* of an element $\tau = a + b\sqrt{d} \in K$ are given by

$$\mathrm{N}(\tau) = a^2 - b^2 d \quad \text{and} \quad \mathrm{T}(\tau) = 2a.$$

When K is viewed as a subfield of $\mathbb{C}$, these can equivalently be expressed as

$$\mathrm{N}(\tau) = \tau\overline{\tau} \quad \text{and} \quad \mathrm{T}(\tau) = \tau + \overline{\tau},$$

where $\overline{\tau}$ denotes the Galois conjugate of τ in K, which coincides with the complex conjugation of τ in K.

Finally, recall from Section 2.2 that the index of two lattices L_1 and L_2 in $\mathbb{C}$ with $L_1 \subseteq L_2$ is given by

$$[L_2 : L_1] = \frac{|\det(M_1)|}{|\det(M_2)|} = |\det(A)|,$$

where M_1 and M_2 denote the matrices whose columns are formed by basis vectors of L_1 and L_2, respectively, and A is the transition matrix satisfying $M_1 = M_2 A$.

Lemma 4.5.3. *Let $\mathcal{O}$ be an order in an imaginary quadratic number field K, and assume that the group of units of $\mathcal{O}$ is given by $\mathcal{O}^* = \{\pm 1\}$. Write $\mathcal{O} = [1, \tau]$ with $\tau \in K$, and*

assume $s \mid \mathrm{T}(\tau)$ and $\gcd(s^2, \mathrm{N}(\tau))$ is squarefree for some integer s. Then for every positive integer N,

$$\frac{\partial \Phi_N}{\partial Y}\left(j\left(\frac{\tau}{s}\right), j\left(\frac{N\tau}{s}\right)\right) \neq 0.$$

Proof. Although we showed $\frac{\partial \Phi_N}{\partial Y}(j(\tau), j(N\tau)) \neq 0$ in the proof of Proposition 4.5.1, we cannot deduce our claim from it, since dividing τ by s does not guarantee that $\frac{\tau}{s}$ and $\frac{N\tau}{s}$ lie in different $\Gamma(1)$-equivalence classes of $\mathbb{H}$. Therefore, we need a different approach. In the same proof, we computed the partial derivative of the modular polynomial Φ, which at $(j(\frac{\tau}{s}), j(\frac{N\tau}{s}))$ is given by

$$\frac{\partial \Phi_N}{\partial Y}\left(j\left(\frac{\tau}{s}\right), j\left(\frac{N\tau}{s}\right)\right) = \prod_{k=2}^{n}\left(j\left(\frac{N\tau}{s}\right) - j\left(\frac{N\gamma_k\tau}{s}\right)\right),$$

where $\{\gamma_1, \ldots, \gamma_n\} \subseteq \Gamma(1)$ is a set of right coset representatives for $\Gamma_0(N)$, where $n = [\Gamma(1) : \Gamma_0(N)]$ and γ_1 is the identity in $\Gamma(1)$. Thus we need to show that $j(\frac{N\tau}{s}) \neq j(\frac{N\gamma_k\tau}{s})$ for all $2 \leq k \leq n$. Assume the contrary, i.e. there exists $k \in \{2, \ldots, n\}$ such that $j(\frac{N\tau}{s}) = j(\frac{N\gamma_k\tau}{s})$. We want to rewrite this statement in terms of lattices. By definition of the j-function we have $j([1, \frac{N\tau}{s}]) = j([1, \frac{N\gamma_k\tau}{s}])$, so by Theorem 2.5.5 the lattices $[1, \frac{N\tau}{s}]$ and $[1, \frac{N\gamma_k\tau}{s}]$ are homothetic. Thus there exists $\lambda \in \mathbb{C}\backslash\{0\}$ such that

$$\lambda\left[1, \frac{N\tau}{s}\right] = \left[1, \frac{N\gamma_k\tau}{s}\right] = \left[1, N\frac{a\frac{\tau}{s} + b}{c\frac{\tau}{s} + d}\right] = \left[c\frac{\tau}{s} + d, N\left(a\frac{\tau}{s} + b\right)\right]$$

where the second equality follows from linear fractional transformation with $\gamma_k = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Now, observe that both lattices $[1, \frac{N\tau}{s}]$ and $[c\frac{\tau}{s} + d, N(a\frac{\tau}{s} + b)]$ are sublattices of $[1, \frac{\tau}{s}]$ (see $[c\frac{\tau}{s} + d, N(a\frac{\tau}{s} + b)] = \{(d + mNb)1 + (nc + mNa)\frac{\tau}{s} \mid d + mNb, nc + mNa \in \mathbb{Z}\} \subseteq [1, \frac{\tau}{s}]$ for the second one). Since both lattices are of index N in $[1, \frac{\tau}{s}]$ (the transition matrices are $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & N \end{smallmatrix}\right)$ and $A = \left(\begin{smallmatrix} d & Nb \\ c & Na \end{smallmatrix}\right)$), taking norms on both sides yields $\mathrm{N}(\lambda) = 1$. Moreover,

$$\lambda s \in [\lambda s, \lambda N\tau] = [c\tau + sd, N(a\tau + sb)] \subseteq [s, \tau],$$

so there exist $u, v \in \mathbb{Z}$ with $\lambda s = us + v\tau$. Taking norms again gives

$$s^2 = s^2\mathrm{N}(\lambda) = \mathrm{N}(\lambda s) = \mathrm{N}(us + v\tau) = u^2s^2 + uvs\mathrm{T}(\tau) + v^2\mathrm{N}(\tau).$$

Since $s \mid \mathrm{T}(\tau)$ by assumption, we have $s^2 \mid v^2\mathrm{N}(\tau)$, and since $\gcd(s^2, \mathrm{N}(\tau))$ is squarefree, it follows that $s \mid v$. Hence, $\lambda s = s(u + w\tau)$ for some $w \in \mathbb{Z}$ and so $\lambda \in [1, \tau] = \mathcal{O}$. As λ has norm 1, it is a unit, which by the assumption $\mathcal{O}^* = \{\pm 1\}$ implies that $\lambda \in \{\pm 1\}$. Thus, $\left[1, \frac{N\tau}{s}\right] = [c\frac{\tau}{s} + d, N(a\frac{\tau}{s} + b)]$, which implies $\gamma_k = \gamma_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, a contradiction to $k \in \{2, \ldots, n\}$. Therefore, the assumption is false and the theorem is proven. □

Remark 4.5.4. *This lemma establishes a uniqueness property among the coset representatives: assuming that $\mathcal{O}^* = \{\pm 1\}$, $s \mid \mathrm{T}(\tau)$ and that $\gcd(s^2, \mathrm{N}(\tau))$ is squarefree, the equality $j(\frac{N\gamma_k\tau}{s}) = j(\frac{N\tau}{s})$ holds if and only if γ_k is the identity element γ_1.*

Lemma 4.5.3 provides a sufficient condition to ensure that the partial derivative of the modular polynomial does not vanish at the points of interest. This will be important for the applications to modular functions in Chapter 6.

5 The First main theorem of complex multiplication

Complex multiplication of elliptic curves reveals a deep and remarkable connection between arithmetic and geometry. Building on the lattices, endomorphism rings, and ideal class groups introduced in the previous chapters, our goal in this chapter is to prove the First main theorem of complex multiplication. This theorem establishes a precise link between the Galois action on elliptic curves and the ideal class group, representing a central result of the theory developed so far.
To reach it, we proceed through seven sections. We begin by defining the action of the ideal class group on elliptic curves, which creates a natural link between ideals and isomorphism classes of elliptic curves with complex multiplication. This is then refined in the section on the ideal class group action via isogenies, where we further explore the connection between ideal actions and morphisms of elliptic curves. Building on this, we establish the algebraicity of the j-invariant. A key ingredient is the integrality of the modular polynomial, proved in the previous chapter, which allows us to deduce that the j-invariant of an elliptic curve with complex multiplication is an algebraic integer, enabling us to work within number fields. Next, we study the Galois group action on elliptic curves and their ring class polynomials, preparing the ground to relate ideal class group actions to Galois actions. With all these tools in place, we finally state and prove the First main theorem of complex multiplication itself, splitting the proof into injectivity and surjectivity. Finally, we explore the consequences and ring class fields, showing how the theorem allows us to construct finite abelian extensions of K generated by j-invariants, and culminating in a key result for proving the near-integer value $e^{\pi\sqrt{163}}$, the ultimate goal of this work. We conclude the chapter with a classification of orders in imaginary quadratic number fields with class number one.

The exposition in this chapter is primarily based on [14, Lec. 17, 20, 21], supplemented by explanations from [13, Ch. II §1] in the first section.

Throughout the chapter, let $\mathcal{O}$ be an order in an imaginary quadratic number field K.

5.1 The ideal class group action on elliptic curves

We turn our attention to the action of the ideal class group on elliptic curves and their j-invariants, building on the correspondence established in Chapter 3. This action translates the arithmetic structure of the ideal class group into geometric transformations and prepares the ground for the Galois-theoretic results that follow.

We start with a *short consideration*. By Corollary 3.5.4, every lattice L with $\mathrm{End}(E_L) \cong \mathcal{O}$ is homothetic to a proper $\mathcal{O}$-ideal, say $\mathfrak{b}$, so there exists $\lambda \in K\backslash\{0\}$ such that $L = \lambda\mathfrak{b} = \mathfrak{a}$. Moreover, by Corollary 2.5.14, for every elliptic curve E over $\mathbb{C}$ there exists a lattice L in $\mathbb{C}$ such that $E \cong E_L$. We deduce that every elliptic curve E over $\mathbb{C}$ with $\mathrm{End}(E) \cong \mathcal{O}$ is isomorphic to $E_\mathfrak{a}$ for some proper $\mathcal{O}$-ideal $\mathfrak{a}$. In particular, it follows that $\mathrm{End}(E_\mathfrak{a}) \cong \mathcal{O}$.

In Subsection 2.5.1 we established that the j-invariant classifies elliptic curves over $\mathbb{C}$ up to isomorphism. This naturally leads us to consider the set

$$\mathrm{Ell}_\mathcal{O}(\mathbb{C}) \coloneqq \{j(E) \in \mathbb{C} \mid E \text{ is an elliptic curve over } \mathbb{C} \text{ with } \mathrm{End}(E) \cong \mathcal{O}\}.$$

By Corollary 3.5.9, there is a natural bijection

$$C(\mathcal{O}) \longrightarrow \mathrm{Ell}_\mathcal{O}(\mathbb{C}), \quad [\mathfrak{a}] \mapsto j(E_\mathfrak{a}) = j(\mathfrak{a}),$$

where $[\mathfrak{a}]$ denotes the class of a proper $\mathcal{O}$-ideal $\mathfrak{a}$ in the ideal class group $C(\mathcal{O})$. Explicitly, each proper $\mathcal{O}$-ideal $\mathfrak{a}$ is a free $\mathbb{Z}$-module of rank 2, hence a lattice in $\mathbb{C}$ under the embedding $K \hookrightarrow \mathbb{C}$. The elliptic curve $E_\mathfrak{a}$ associated to this lattice then has endomorphism ring $\mathcal{O}$, and its j-invariant coincides with $j(\mathfrak{a})$ by definition. Since the ideal class group $C(\mathcal{O})$ is finite (see end of Chapter 3), it follows that $\mathrm{Ell}_\mathcal{O}(\mathbb{C})$ is finite as well. In fact, its cardinality equals the class number $h(\mathcal{O})$.

We will now show that these sets are not only in bijection, but that $\mathrm{Ell}_\mathcal{O}(\mathbb{C})$ also carries a natural group action of $C(\mathcal{O})$.

Proposition 5.1.1. *Let E be an elliptic curve over $\mathbb{C}$ with $\mathrm{End}(E) \cong \mathcal{O}$ and let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ be proper $\mathcal{O}$-ideals. Then we have*

(i) $E_{\mathfrak{a}\mathfrak{b}}$ *is well-defined,*

(ii) $\mathrm{End}(E_{\mathfrak{a}\mathfrak{b}}) \cong \mathcal{O}$*,*

(iii) $E_{\mathfrak{a}\mathfrak{b}} \cong E_{\mathfrak{c}\mathfrak{b}}$ *if and only if* $[\mathfrak{a}] = [\mathfrak{c}]$ *in* $C(\mathcal{O})$*.*

Proof. (i): The *short consideration* at the beginning of this section tells us that every elliptic curve E over $\mathbb{C}$ with $\mathrm{End}(E) \cong \mathcal{O}$ is isomorphic to $E_\mathfrak{b}$ for some proper $\mathcal{O}$-ideal $\mathfrak{b}$ and that $\mathrm{End}(E_\mathfrak{b}) \cong \mathcal{O}$. Thus, to show that $E_{\mathfrak{a}\mathfrak{b}}$ is well-defined, it suffices to verify that $\mathfrak{a}\mathfrak{b}$ is a proper $\mathcal{O}$-ideal. This is immediate since $\mathfrak{a}$ is proper by assumption and the group $I(\mathcal{O})$ of proper $\mathcal{O}$-ideals is closed under ideal multiplication.
(ii): For every $\alpha \in \mathbb{C}$ and proper $\mathcal{O}$-ideals $\mathfrak{a}, \mathfrak{b}$ we have

$$\alpha\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b} \iff \mathfrak{a}^{-1}\alpha\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{a}\mathfrak{b} \iff \alpha\mathfrak{b} \subseteq \mathfrak{b}.$$

Hence by part (i),

$$\mathrm{End}(E_{\mathfrak{a}\mathfrak{b}}) = \{\alpha \in \mathbb{C} \mid \alpha\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b}\} = \{\alpha \in \mathbb{C} \mid \alpha\mathfrak{b} \subseteq \mathfrak{b}\} = \mathrm{End}(E_\mathfrak{b}) \cong \mathcal{O}.$$

(*iii*): By Corollary 2.5.6 and Remark 3.5.7 we know that $E_{\mathfrak{ab}} \cong E_{\mathfrak{cb}}$ holds if and only if $\mathfrak{ab} = \lambda\mathfrak{cb}$ for some $\lambda \in \mathbb{C}\backslash\{0\}$. Since $\mathfrak{a}$ is a proper $\mathcal{O}$-ideal and thus invertible, multiplying by $\mathfrak{a}^{-1}$ gives

$$E_{\mathfrak{ab}} \cong E_{\mathfrak{cb}} \iff \mathfrak{b} = \lambda\mathfrak{a}^{-1}\mathfrak{cb},$$

using the fact that $\mathcal{O}\mathfrak{b} = \mathfrak{b}$ as $\mathfrak{b}$ is an $\mathcal{O}$-ideal. Similarly, multiplying by $\lambda^{-1}\mathfrak{c}^{-1}$ yields

$$E_{\mathfrak{ab}} \cong E_{\mathfrak{cb}} \iff \mathfrak{b} = \lambda^{-1}\mathfrak{ac}^{-1}\mathfrak{b}.$$

Hence, if $E_{\mathfrak{ab}} \cong E_{\mathfrak{cb}}$, both $\lambda\mathfrak{a}^{-1}\mathfrak{c}$ and $\lambda^{-1}\mathfrak{ac}^{-1}$ are contained in $\mathcal{O}$ as $\mathfrak{b} \in \mathcal{O}$. These two ideals are clearly inverse to each other and contained in $\mathcal{O}$, so by the properties of ideals, they must both equal $\mathcal{O}$. Thus, $\mathfrak{a} = \lambda\mathfrak{c}$, with $\lambda \in K\backslash\{0\}$, and therefore $[\mathfrak{a}] = [\mathfrak{c}]$ in $C(\mathcal{O})$. Conversely, if $[\mathfrak{a}] = [\mathfrak{c}]$ in $C(\mathcal{O})$, so that $\mathfrak{a} = \lambda\mathfrak{c}$ for some $\lambda \in K\backslash\{0\} \subseteq \mathbb{C}\backslash\{0\}$, then for any proper $\mathcal{O}$-ideal $\mathfrak{b}$ we have $\mathfrak{ab} = \lambda\mathfrak{cb}$, and hence $E_{\mathfrak{ab}} \cong E_{\mathfrak{cb}}$ by Remark 3.5.7 and Corollary 2.5.6. □

Now, let $E_{\mathfrak{b}}$ be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$. For a proper $\mathcal{O}$-ideal $\mathfrak{a} \in I(\mathcal{O})$, its inverse $\mathfrak{a}^{-1}$ exists, so $E_{\mathfrak{a}^{-1}\mathfrak{b}}$ is well-defined by (*i*) and has complex multiplication by $\mathcal{O}$ by (*ii*) of the previous proposition. We then define the action of $\mathfrak{a}$ on $E_{\mathfrak{b}}$ by

$$\mathfrak{a}E_{\mathfrak{b}} = E_{\mathfrak{a}^{-1}\mathfrak{b}},$$

obtaining a group action of the set of proper $\mathcal{O}$-ideals $I(O)$ on the set of elliptic curves with complex multiplication by $\mathcal{O}$.
Note that we use $E_{\mathfrak{a}^{-1}\mathfrak{b}}$ rather than $E_{\mathfrak{ab}}$ because $\mathfrak{ab} \subseteq \mathfrak{b}$, whereas $\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{b}$.

The j-invariant induces an action of the ideal class group $C(\mathcal{O})$ on the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ of isomorphism classes of elliptic curves with complex multiplication by $\mathcal{O}$, defined by

$$[\mathfrak{a}]j(E_{\mathfrak{b}}) = j(E_{\mathfrak{a}^{-1}\mathfrak{b}}),$$

or equivalently, identifying elliptic curves with their corresponding lattices,

$$[\mathfrak{a}]j(\mathfrak{b}) = j(\mathfrak{a}^{-1}\mathfrak{b}).$$

This action is well-defined, independent of the representatives $\mathfrak{a}$ and $\mathfrak{b}$, since proper $\mathcal{O}$-ideals in the same ideal class define isomorphic elliptic curves by Proposition (*iii*).

To verify the action axioms, for a non-zero principal $\mathcal{O}$-ideal $\mathfrak{a}$, i.e. $\mathfrak{a} \in P(\mathcal{O})$, we have that $\mathfrak{b}$ and $\mathfrak{a}^{-1}\mathfrak{b}$ are equivalent as $\mathcal{O}$-ideals, and by Theorem 2.5.6,

$$\mathfrak{a}E_{\mathfrak{b}} = E_{\mathfrak{a}^{-1}\mathfrak{b}} \cong E_{\mathfrak{b}}$$

Hence, the identity element of $C(\mathcal{O})$ acts trivially. Finally, for any proper $\mathcal{O}$-ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$, we have

$$[\mathfrak{a}]([\mathfrak{c}]E_{\mathfrak{b}}) = [\mathfrak{a}]E_{\mathfrak{c}^{-1}\mathfrak{b}} = E_{\mathfrak{a}^{-1}(\mathfrak{c}^{-1}\mathfrak{b})} = E_{(\mathfrak{ac})^{-1}\mathfrak{b}} = ([\mathfrak{a}][\mathfrak{c}])E_{\mathfrak{b}}.$$

This establishes a well-defined group action of $I(\mathcal{O})$ on the set of elliptic curves with CM by $\mathcal{O}$, and hence of $C(\mathcal{O})$ on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ via the j-invariant.

Remark 5.1.2. *The above action is simply transitive.*
Indeed, consider two proper $\mathcal{O}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$ and suppose $[\mathfrak{a}]j(\mathfrak{b}) = j(\mathfrak{a}^{-1}\mathfrak{b}) = j(\mathfrak{b})$. By Theorem 2.5.5, this means the lattices $\mathfrak{b}$ and $\mathfrak{a}^{-1}\mathfrak{b}$ are homothetic, i.e., there exists $\lambda \in K\backslash\{0\}$ such that $\mathfrak{a}\mathfrak{b} = \lambda\mathfrak{b}$. Cancelling $\mathfrak{b}$, which is possible since it is a proper $\mathcal{O}$-ideal and hence non-zero, yields $\mathfrak{a} = \lambda\mathcal{O}$. Hence $\mathfrak{a}$ is a principal, so $[\mathfrak{a}]$ is trivial in $C(\mathcal{O})$. This shows that the action is not only faithful, but also free.
To see transitivity, note that $C(\mathcal{O})$ and $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ have the same cardinality by the previously established bijection. Indeed, fix any $j_0 \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ and consider its orbit under the action of $C(\mathcal{O})$, that is, the set of elements of the form $[\mathfrak{a}]j_0$ for $[\mathfrak{a}] \in C(\mathcal{O})$. Since the action is free, all these values are distinct, and hence the orbit contains exactly $|C(\mathcal{O})|$ elements. But $|\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})| = |C(\mathcal{O})|$, so the orbit of j_0 must be the entire set.
Therefore, the action is both free and transitive, i.e., simply transitive.

5.2 The ideal class group action on elliptic curves via isogenies

We reinterpret the action of the ideal class group on elliptic curves with complex multiplication, introduced in the previous section, in terms of isogenies. This geometric perspective allows us to compute degrees and kernels explicitly, which will be essential for the surjectivity part of the First main theorem of complex multiplication.

Let L_1 and L_2 be lattices in $\mathbb{C}$ and E_1 and E_2 the corresponding elliptic curves. By Theorem 3.2.1, there exists a unique $\alpha = \alpha_\phi$ satisfying $\alpha L_1 \subseteq L_2$, such that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{C}/L_1 & \xrightarrow{\varphi_\alpha} & \mathbb{C}/L_2 \\ \downarrow{\scriptstyle \Phi_1} & & \downarrow{\scriptstyle \Phi_2} \\ E_1(\mathbb{C}) & \xrightarrow{\phi_\alpha} & E_2(\mathbb{C}). \end{array}$$

This follows from the fact that the larger diagram in Theorem 3.1.3 (*iii*) commutes, as well as its left square (see Section 3.1). Since we are interested in lattices up to homothety and elliptic curves up to isomorphism, we may replace L_1 by the homothetic lattice αL_1 and E_1 with an isomorphic elliptic curve, so that we can assume $\alpha = 1$. This allows us to view the isogeny $\phi = \phi_1 : E_1 \to E_2$ as being induced by the inclusion $L_1 \subseteq L_2$. As we compose ϕ_α with an isomorphism, its degree remains unchanged. Then,

$$\begin{aligned} \ker(\phi) = \ker(\Phi_2 \circ 1 \circ \Phi_1^{-1}) &= \{\omega \in E_1(\mathbb{C}) \mid (\Phi_2 \circ 1 \circ \Phi_1^{-1})(\omega) = 0\} \\ &= \{\omega = \Phi_1(z) \in E_1(\mathbb{C}) \mid \Phi_2(z) = 0,\ z \in \mathbb{C}\} \\ &= \{\Phi_1(z) \in E_1(\mathbb{C}) \mid z \in L_2\}. \end{aligned}$$

Since $\Phi_1(z) = 0$ if and only if $z \in L_1$, it follows that

$$\ker(\phi) \cong L_2/L_1,$$

and its order is given by $|\ker(\phi)| = |L_2/L_1| = [L_2 : L_1]$, which is exactly the index of L_1 in L_2 (see Section 2.2). This index is finite, as both lattices are of full-rank by definition.

Since ϕ is defined by a non-constant polynomial map and we are working in characteristic zero, it follows that ϕ is separable. Moreover, one can show that the degree of a separable isogeny equals the order of its kernel (see [14, Section 4.5]), i.e.

$$\deg(\phi) = |\ker(\phi)| = [L_2 : L_1].$$

Thus, over a field of characteristic zero, every separable isogeny has finite degree. In particular, a separable isogeny of degree 1 has trivial kernel and thus is an isomorphism. Since every isogeny arises from a lattice inclusion by Corollary 3.2.1, this discussion applies to any isogeny of elliptic curves over $\mathbb{C}$. In particular, the inclusion $nL \subseteq L$ induces the multiplication-by-n endomorphism $[n]$ of the corresponding elliptic curve E_L.

Moreover, note that Corollary 3.2.2 establishes a ring isomorphism between the endomorphism ring $\mathrm{End}(E_L)$ of the elliptic curve $E = E_L$ and the set $\{\alpha \in \mathbb{C} \mid \alpha L \subseteq L\}$. By the preceding discussion, each such lattice inclusion induces an isogeny from E_L to itself. Thus, every endomorphism of an elliptic curve over $\mathbb{C}$ is, in particular, an isogeny.

Proposition 5.2.1. *For any two elliptic curves with complex multiplication by $\mathcal{O}$ there exists an isogeny ϕ and, up to isomorphism, every such isogeny is of the form $E_\mathfrak{b} \to \mathfrak{a}E_\mathfrak{b}$, where $\mathfrak{a}$ and $\mathfrak{b}$ are proper $\mathcal{O}$-ideals of degree $\mathrm{N}\mathfrak{a}$.*

Proof. Let L_1 be a lattice in $\mathbb{C}$ with corresponding elliptic curve E_1 with $\mathrm{End}(E_1) \cong \mathcal{O}$. By the *short consideration* at the beginning of this chapter, every elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$ is isomorphic to $E_\mathfrak{b}$ for some proper $\mathcal{O}$-ideal $\mathfrak{b}$. Hence, $E_1 \cong E_\mathfrak{a}$ for some proper $\mathcal{O}$-ideal $\mathfrak{a}$. Now let $\mathfrak{b}$ be an another proper $\mathcal{O}$-ideal. Then the inclusion of lattices $\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{b}$ induces an isogeny

$$\phi_\mathfrak{a} : E_\mathfrak{b} \to E_{\mathfrak{a}^{-1}\mathfrak{b}} = \mathfrak{a}E_\mathfrak{b},$$

which corresponds to the action of $\mathfrak{a}$ on $E_\mathfrak{b}$ defined previously.
If E_2 is another elliptic curve with $\mathrm{End}(E_2) \cong \mathcal{O}$, then $E_2 \cong E_\mathfrak{c}$ for some proper $\mathcal{O}$-ideal $\mathfrak{c}$ by the same argument. Let $\alpha = \mathrm{N}\mathfrak{c}$. Then $\mathfrak{b}$ and $\alpha\mathfrak{b}$ are equivalent, and since $\alpha \in \mathbb{Z}_{>0} \subseteq \mathcal{O}$, we have $\alpha\mathfrak{b} = (\alpha)\mathfrak{b}$. Considering $\mathfrak{b}$ instead of $(\alpha)\mathfrak{b}$ and using Remark 3.5.5, we get $(\mathrm{N}\mathfrak{c}) = \mathfrak{c}\bar{\mathfrak{c}}$, so $(\alpha)\mathfrak{b} = \mathfrak{c}\bar{\mathfrak{c}}\mathfrak{b} \subseteq \mathfrak{b}$, which shows that $\mathfrak{c}$ divides (and hence contains) $\mathfrak{b}$. Thus we may set $\mathfrak{c} = \mathfrak{a}^{-1}\mathfrak{b}$, and the isogeny $\phi_\mathfrak{a} : E_\mathfrak{b} \to E_\mathfrak{c} = \mathfrak{a}E_\mathfrak{b}$ induced by the inclusion $\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{b} = \mathfrak{c}$ corresponds to the action of $\mathfrak{a}$ on $E_\mathfrak{b}$. After rescaling $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ by integer multiples if necessary, we may assume that $\mathfrak{a}$ is a proper $\mathcal{O}$-ideal. As the elliptic curves with complex multiplication by $\mathcal{O}$ were arbitrary, this proves the first part.
For the degree, let L_1 and L_2 be the lattices corresponding to $E_\mathfrak{b}$ and $E_{\mathfrak{a}^{-1}\mathfrak{b}}$, where we may assume $L_1 = \mathfrak{b}$ and $L_2 = \mathfrak{a}^{-1}\mathfrak{b}$ by the *short consideration* above. We have seen earlier that degree of the isogeny $\phi : E_\mathfrak{b} \to E_{\mathfrak{a}^{-1}\mathfrak{b}} = \mathfrak{a}E_\mathfrak{b}$ induced by the inclusion $\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{b}$ is given by the index of L_1 in L_2. Since both $\mathfrak{a}$ and $\mathfrak{b}$ are proper by assumption and hence invertible, we get

$$\deg(\phi) = [L_2 : L_1] = [\mathfrak{a}^{-1}\mathfrak{b} : \mathfrak{b}] = [\mathfrak{b} : \mathfrak{a}\mathfrak{b}] = [\mathfrak{b}\mathfrak{b}^{-1} : \mathfrak{a}\mathfrak{b}\mathfrak{b}^{-1}] = [\mathcal{O} : \mathfrak{a}] = \mathrm{N}\mathfrak{a}$$

by definition of the norm of a non-zero $\mathcal{O}$-ideal (Remark 3.5.6 (*iii*)) in the last equality. □

5.3 Algebraic integrality of j

Now that we understand how the ideal class group acts via isogenies, we focus on cyclic isogenies, whose kernels correspond to cyclic sublattices of a lattice. Classifying these sublattices allows us to connect the action of ideals with the roots of modular polynomials and, ultimately, to deduce the algebraic integrality of the j-invariant.

Definition 5.3.1 (Cyclic sublattice)**.** Let L_1 and L_2 be lattices in $\mathbb{C}$. We say that L_1 is a cyclic sublattice of L_2, if L_1 is a sublattice of L_2 and the group L_2/L_1 is cyclic. Similarly, an isogeny $\phi : E_1 \to E_2$ between elliptic curves over $\mathbb{C}$ is called cyclic, if its kernel is a cyclic group.

By definition, it follows that if ϕ is induced by a lattice inclusion $L_1 \subseteq L_2$, then ϕ is cyclic if and only if L_1 is a cyclic sublattice of L_2.

Note that, up to isomorphism, every isogeny is a composition of cyclic isogenies of prime degree (for a proof see [14, Cor. 5.12]). Since isogenies of prime degree are necessarily cyclic, we may restrict our attention to cyclic isogenies ϕ of prime degree N.

Lemma 5.3.2. *Let $L = [1, \tau]$ be a lattice in $\mathbb{C}$, and let N be prime. The cyclic sublattices of L of index N are the lattice $[1, N\tau]$ and the lattices $[N, \tau + k]$ for $0 \leq k < N$.*

Proof. Clearly, the lattices $[1, N\tau]$ and $[N, \tau + k]$ for $0 \leq k < N$ are sublattices of L of index N. Since the quotient L/L' of a lattice L by a sublattice L' of index N has order $|L/L'| = [L : L'] = N$, and every group of prime order is cyclic, each such sublattice is cyclic. Conversely, any sublattice $L' \subseteq L$ can be written as $[d, a\tau + k]$, where d is the least positive integer in L' and the index of L' in L is $ad = N$. Since N is prime, either $d = 1$ and $a = N$, giving $L' = [1, N\tau]$, or $d = N$ and $a = 1$, giving $L' = [N, \tau + k]$ with $0 \leq k < N$. □

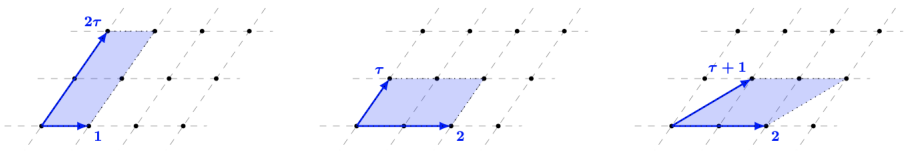

Figure 5.1: The three cyclic sublattices of $[1, \tau]$ of index 2.
Reproduced from [14, Lec. 20]. Changes: none.

Proposition 5.3.3. *Let $j_1, j_2 \in \mathbb{C}$. Then $\Phi_N(j_1, j_2) = 0$ if and only if j_1 and j_2 are the j-invariants of elliptic curves over $\mathbb{C}$ that are related by a cyclic isogeny of degree N.*

Proof. We show the proposition for N prime (cf. Section 4.4); the case of composite N is analogous but involves more complicated combinatorics of sublattices and coset representatives. We will prove the equivalent statement that $\Phi_N(j(L_1), j(L_2)) = 0$ if

and only if L_2 is homothetic to a cyclic sublattice of L_1 of index N. Since every lattice is homothetic to one of the form $[1, \tau]$, we may assume $L_1 = [1, \tau_1]$ and $L_2 = [1, \tau_2]$ for some $\tau_1, \tau_2 \in \mathbb{H}$. As in the proof of Theorem 4.4.4, we have

$$\Phi_N(j(\tau), Y) = (Y - j_N(\tau)) \prod_{k=0}^{N-1} (Y - j_N(\gamma_k \tau)),$$

where $\gamma_k = ST^k$ and $j_N(\gamma_k \tau) = j(N\gamma_k \tau) = j\left(\frac{\tau+k}{N}\right)$ with $N = \left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Thus

$$\Phi_N(j(L_1), j(L_2)) = \Phi_N(j(\tau_1), j(\tau_2)) = (j(\tau_2) - j_N(\tau_1)) \prod_{k=0}^{N-1} (j(\tau_2) - j_N(\gamma_k \tau_1))$$

is zero if and only if τ_2 is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to $N\tau_1$ or $\frac{\tau_1+k}{N}$ with $0 \leq k < N$, and hence if and only if L_2 is homothetic to cyclic sublattice of L_1 of index N by Lemma 5.3.2. □

Remark 5.3.4. *Note that we cannot assume that the j-invariants of lattices are distinct, but we can assume that the cyclic sublattices are. It may happen that two different cyclic isogenies have the same j-invariant for their images, even though their kernels, i.e. their cyclic sublattices they correspond to, are different. This occurs because distinct sublattices may be homothetic, meaning they are scalar multiples of each other, which results in isomorphic elliptic curves with the same j-invariant.*

Note that if L_1 and L_2 are homothetic, then finding all cyclic sublattices of L_1 of index N to which L_2 is homothetic is equivalent to finding all cyclic sublattices of L_2 of index N to which L_1 is homothetic. This observation provides insight for our next proposition.

Proposition 5.3.5. *Let $N > 1$ be an integer. Then $\Phi_N(X, Y) = \Phi_N(Y, X)$.*

Proof. As in the previous proof, let $\gamma_k = ST^k$ and

$$\Phi_N(j(\tau), Y) = (Y - j_N(\tau)) \prod_{k=0}^{N-1} (Y - j_N(\gamma_k \tau)).$$

In particular, $j_N(\gamma_0 \tau) = j(N\gamma_k \tau) = j\left(\frac{\tau}{N}\right)$ is a root of $\Phi_N(j(\tau), Y)$. By definition, $\Phi_N(j(\tau), j_N(\tau)) = 0$, which implies $\Phi_N(j\left(\frac{\tau}{N}\right), j(\tau)) = 0$, hence $j\left(\frac{\tau}{N}\right)$ is also a root of $\Phi_N(Y, j(\tau))$. Since $\Phi_N(j, Y)$ is the minimal polynomial of j_N over $\mathbb{C}(j)$, it is irreducible in $\mathbb{C}(j)[Y]$, and therefore must properly divide $\Phi_N(Y, j)$ in $\mathbb{C}(j)[Y]$. The numbers of roots (counted with multiplicity) of $\Phi_N(j(L), Y)$ and $\Phi_N(Y, j(L))$ for a lattice $L \subseteq \mathbb{C}$ coincide, although the roots need not be distinct (cf. Remark 5.3.4). Since these numbers also equal the number of cyclic sublattices of index N by Proposition 5.3.3, both polynomials have the same degree. It follows that $\Phi_N(Y, j) = f(j)\Phi_N(j, Y)$ for some $f \in \mathbb{C}(j)$. Substituting $Y = j$ gives $f(j) = 1$, because $\Phi_N(j, j) \neq 0$ as $j(\tau)$ is not a root of the minimal polynomial $j_N(\tau)$ for $N > 1$. Thus, the modular polynomial is symmetric in X and Y. □

The symmetry of $\Phi_N(X,Y)$ in X and Y implies that the diagonal substitution $Y = X$ is well-defined, so $\Phi_N(X,X)$ is a legitimate polynomial in X.

Lemma 5.3.6. *Let N be prime. Then the leading term of $\Phi_N(X,X)$ is $-X^{-2N}$.*

Proof. Again consider the expression of the modular polynomial from the proof of Theorem 4.4.4, and replace Y with $j(\tau)$ to obtain

$$\Phi_N(j(\tau), j(\tau)) = (j(\tau) - j(N\tau)) \prod_{k=0}^{N-1} \left(j(\tau) - j\left(\frac{\tau + k}{N}\right)\right).$$

In that proof we also computed the q-expansions

$$\begin{aligned} j(N\tau) &= \frac{1}{q^N} + \dots \\ j\left(\frac{\tau + k}{N}\right) &= \frac{\zeta_N^{-k}}{q^{\frac{1}{N}}} + \dots, \end{aligned}$$

where $q = e^{2\pi i \tau}$ and $\zeta_N = e^{\frac{2\pi i}{N}}$. Hence,

$$\begin{aligned} j(\tau) - j(N\tau) &= -\frac{1}{q^N} + \frac{1}{q} \dots \\ j(\tau) - j\left(\frac{\tau + k}{N}\right) &= \frac{1}{q} - \frac{\zeta_N^{-k}}{q^{\frac{1}{N}}} + \dots, \end{aligned}$$

Multiplying these leading terms shows that the q-expansion of $\Phi_N(j(\tau), j(\tau))$ begins with $-\frac{1}{q^{2N}} + \dots$. Since $\Phi_N(j(\tau), j(\tau))$ is a polynomial in $j(\tau) = \frac{1}{q} + \dots$, it follows that the leading term of $\Phi_N(X,X)$ is $-X^{2N}$. □

Lemma 5.3.7. *Every ideal class in $C(\mathcal{O})$ contains infinitely many proper $\mathcal{O}$-ideals of prime norm.*

Proof. This follows from Lemma 7.7 and Corollary 9.12 in [3]. □

Theorem 5.3.8. *Let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$. Then $j(E)$ is an algebraic integer.*

Proof. Let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$, and let $\mathfrak{p}$ be a principal $\mathcal{O}$-ideal of prime norm p, which exists by the previous lemma. By definition, the class $[\mathfrak{p}]$ represents the identity element in $C(\mathcal{O})$, so $\mathfrak{p}$ acts trivially on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$, i.e. $[\mathfrak{p}]j(E) = j(E)$, and hence $\mathfrak{p}E \cong E$ by the classification of elliptic curves over $\mathbb{C}$ via their j-invariants (see Section 5.1). Therefore, the action of $\mathfrak{p}$ on E corresponds, after composing with an isomorphism if necessary, to an isogeny $\phi : E \to \mathfrak{p}E$ of degree p by Proposition 5.2.1. As p is prime, the isogeny ϕ is cyclic. Hence, by Proposition 5.3.3, we have $\Phi_p(j(E), j(E)) = 0$, and so $j(E)$ is a root of the polynomial $\Phi_p(X,X)$, which is monic by Lemma 5.3.6 and has integer coefficients by Theorem 4.4.4. Thus $j(E)$ is an algebraic integer. □

5.4 The Galois action on elliptic curves and ring class polynomials

We now turn to a complementary perspective, considering the action of the absolute Galois group on elliptic curves with complex multiplication and, in particular, on their j-invariants. While the ideal class group action on elliptic curves translates ideal-theoretic structure into geometry, the Galois action provides an arithmetic perspective, permuting the j-invariants in a way that preserves the endomorphism ring. Studying this action allows us to understand important properties of the associated ring class polynomials.

Recall the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) = \{j(E) \in \mathbb{C} \mid E \text{ is an elliptic curve over } \mathbb{C} \text{ with } \mathrm{End}(E) \cong \mathcal{O}\}$ of j-invariants of elliptic curves over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$.
Also recall that, by Theorem 3.3.3, every discriminant $D \equiv 0, 1 \bmod 4$ determines a unique order $\mathcal{O}$ in $K = \mathbb{Q}(\sqrt{d_K})$, and can be written uniquely as $D = f^2 d_K$ for some integer $f \geq 1$. This ensures that the following polynomial is well-defined:

Definition 5.4.1 (Ring class polynomial, Hilbert class polynomial)**.** Let $\mathcal{O}$ be an order of discriminant D. The ring class polynomial of discriminant D is defined as

$$H_D(X) \coloneqq H_{\mathcal{O}}(X) \coloneqq \prod_{j(E) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})} (X - j(E)).$$

A special case arises when $\mathcal{O} = \mathcal{O}_K$ is the maximal order of K. In this case, the discriminant equals the field discriminant d_K, and the polynomial $H_{d_K}(X) \coloneqq H_{\mathcal{O}_K}(X)$ is called the Hilbert class polynomial.

Note that the ring class polynomial is monic and its roots are precisely the distinct j-invariants of elliptic curves with complex multiplication by $\mathcal{O}$. By, definition, these form the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ by definition, on which the ideal class group $C(\mathcal{O})$ acts by Section 5.1. Therefore, $C(\mathcal{O})$ naturally acts on the roots of the ring class polynomial by permutation.

Our next goal is to study two important natural actions of the absolute Galois group and prove related theorems. To prepare for this, we first recall some Galois theory.
A *Galois extension* is an algebraic field extension L/K, which is both normal and separable. Then the *Galois group* $\mathrm{Gal}(L/K)$ of a Galois extension L/K is defined to be the automorphism group $\mathrm{Aut}(L/K)$ of L/K, which is the group consisting of all field automorphisms of L that fix K.
The separable closure K^{sep} of K is always normal. Indeed, if an irreducible polynomial $f \in K[x]$ has a root α in K^{sep}, then f is the minimal polynomial of α over K (up to scalars) and hence separable over K, so all its roots lie in K^{sep}. Thus K^{sep}/K is a Galois extension and its Galois Group $\mathrm{Gal}(K^{sep}/K)$ is called the *absolute Galois group* of K. For finite Galois extensions, L/K the *order* is defined by $|\mathrm{Gal}(L/K)| = [L : K]$.

Now, the j-invariant $j(E)$ of an elliptic curve E over $\mathbb{C}$, given in Weierstrass form $E : y^2 = x^3 + Ax + B$, clearly lies in the number field $\mathbb{Q}(j(E))$, so we have $j(E) = j_0$ for some $j_0 \in \mathbb{Q}(j(E))$. Since $\mathrm{char}(\mathbb{Q}(j(E))) \neq 2, 3$, the proof of Theorem 2.5.7 shows that

the coefficients A and B can be expressed explicitly by the formulas

$$A = 3j_0(1728 - j_0) \quad \text{and} \quad B = 2j_0(1728 - j_0)^2,$$

as long as $j_0 \notin \{0, 1728\}$. In the two special cases $j_0 = 0$ and $j_0 = 1728$, the same proof gives the equations $y^2 = x^3 + 1$ and $y^2 = x^3 + x$ for E, respectively, both of which are also defined over $\mathbb{Q}(j(E))$. Hence, in all cases, the coefficients A and B lie in the $\mathbb{Q}(j(E))$.

Now consider the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$ of $\mathbb{Q}$, which by definition, is the group of all automorphisms of the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ that fix $\mathbb{Q}$ pointwise. In other words, each $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$ is an isomorphism $\sigma : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$, such that $\sigma(a) = a$ for all $a \in \mathbb{Q}$. Since the coefficients A and B of E lie in $\mathbb{Q}(j(E))$, and hence in the closure $\overline{\mathbb{Q}}$, the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$ acts naturally on them, and we have $\sigma(A), \sigma(B) \in \sigma(\mathbb{Q}(j(E))) = \mathbb{Q}(\sigma(j(E)))$. The transformed coefficients still satisfy the relation $4\sigma(A)^3 + 27\sigma(B)^2 \neq 0$ since the Galois group automorphisms preserve algebraic relations, ensuring that the new curve is also non-singular. Therefore, σ maps E to another non-singular elliptic curve

$$E^\sigma : y^2 = x^3 + \sigma(A)x + \sigma(B)$$

defined over $\mathbb{Q}(\sigma(j(E)))$. Thus, we obtain a natural action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the set of elliptic curves defined over $\overline{\mathbb{Q}}$, given by applying σ to the coefficients of their defining equations.

This Galois action extends naturally to isogenies and, in particular, to endomorphisms. Indeed, every endomorphism of an elliptic curve over $\mathbb{C}$ arises as an isogeny induced by a lattice inclusion, as discussed in Section 5.2. Moreover, every isogeny can be expressed by a rational map of the form $\phi(x, y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$, where u, v, s, t are polynomials with coefficients in $\mathbb{C}$, and this representation is unique up to multiplication by a non-zero scalar in $\mathbb{C}$, as seen in Section 3.1. Now, given an automorphism $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, this standard form allows us to define a Galois conjugate of ϕ by letting σ act on the coefficients of these rational functions, yielding the new map

$$\phi^\sigma(x, y) = \left(\frac{\sigma(u)(x)}{\sigma(v)(x)}, \frac{\sigma(s)(x)}{\sigma(t)(x)}y\right).$$

This gives rise to an isogeny $\phi^\sigma : E^\sigma \to E^\sigma$, and if ϕ is an endomorphism of E, then ϕ^σ is an endomorphism of the Galois conjugate curve E^σ.
Moreover, this action respects the algebraic structure of the endomorphism ring: for all $\phi, \psi \in \mathrm{End}(E)$, we have $(\phi + \psi)^\sigma = \phi^\sigma + \psi^\sigma$ and $(\phi \circ \psi)^\sigma = \phi^\sigma \circ \psi^\sigma$. Hence, every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$ induces a ring homomorphism $\mathrm{End}(E) \xrightarrow{\sigma} \mathrm{End}(E^\sigma)$. Applying the inverse endomorphism σ^{-1} to E^σ gives the inverse map, so this is correspondence is, in fact, a ring isomorphism

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

In particular, this shows that if E has complex multiplication by an order $\mathcal{O}$, then its Galois conjugate E^σ also has complex multiplication by $\mathcal{O}$.

Another natural and important action is that of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$ on the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$. Since $j(E)$ is, by definition, a rational function of the coefficients A and B, we have $j(E)^\sigma = j(E^\sigma)$ for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$. From the previous discussion, E^σ has complex multiplication by the same order $\mathcal{O}$, and hence $j(E^\sigma) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$. Therefore, the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$ acts on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$, the set of roots of the ring class polynomial $H_D(X)$, by permuting its elements.

This observation will be useful in the theory that follows and already allows us to deduce the following remark.

Remark 5.4.2. *The coefficients of the ring class polynomial $H_D(X)$ are integers. Indeed, by definition, these coefficients are symmetric polynomials in the roots $j(E) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$. By the discussion above, the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ by permutation, so the coefficients of $H_D(X)$ are fixed under this action and therefore lie in the fixed field $\mathbb{Q}$. Moreover, by Theorem 5.3.8, the roots of $j(E)$ are algebraic integers, which implies that the symmetric polynomials in these roots are also algebraic integers. Combining these two facts, the coefficients lie in $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.*

5.5 The First main theorem of complex multiplication

We have now reached the central result of this chapter: the First main theorem of complex multiplication. This theorem establishes a precise correspondence between the action of the ideal class group on elliptic curves via isogenies and the action of the absolute Galois group on their j-invariants, thereby connecting the arithmetic of an imaginary quadratic order with the geometry of elliptic curves possessing complex multiplication. To prove this correspondence, we divide the argument into two parts. In the first subsection, we verify injectivity and compatibility of the class group action with the Galois action. In the second subsection, we establish surjectivity, completing the theorem.

For the next two sections, we assume that $\mathcal{O}$ is an order in an imaginary quadratic field K with discriminant D, so that the corresponding ring class polynomial $H_D(X)$ is well-defined.

5.5.1 Injectivity and compatibility

We begin with injectivity and compatibility of this correspondence.

By the previous section, we now have two groups acting on the coefficients of the ring class polynomial $H_D(X)$: the ideal class group $C(\mathcal{O})$ and the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$. In the latter case, instead of considering the whole Galois group, we can restrict ourselves to any subfield of $\overline{\mathbb{Q}}$ that contains the splitting field L of $H_D(X)$. Indeed, every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$ acts on the roots of $H_D(X)$ by permuting them, so the action is determined by its restriction to $\mathrm{Gal}(L, \mathbb{Q})$.
Since L is a finite extension of $\mathbb{Q}$, the Galois group $\mathrm{Gal}(L, \mathbb{Q})$ is finite, just as $C(\mathcal{O})$ is finite, as discussed at the end of Chapter 3. Both groups act on the same set of elements, so it is natural to ask whether these actions are compatible.

Note that the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ may contain automorphisms which do not fix the order $\mathcal{O}$, so instead of working with the splitting field L of $H_D(X)$ over $\mathbb{Q}$, we will restrict our attention to the splitting field L of $H_D(X)$ over $K = \mathbb{Q}(\sqrt{D})$.

Now, let E_1 be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$ and let $\sigma \in \mathrm{Gal}(L/K)$. As established in the previous section, $\mathrm{End}(E_1) \cong \mathrm{End}(E_1^\sigma)$, so the conjugate curve E_1^σ also has complex multiplication by $\mathcal{O}$. Since the action of $C(\mathcal{O})$ on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ is transitive by Remark 5.1.2, there exists a proper $\mathcal{O}$-ideal $\mathfrak{a}$ such that $E_1^\sigma \cong \mathfrak{a}E_1$.
Let E_2 be another elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$. Then by the same argument, there exists a proper $\mathcal{O}$-ideal $\mathfrak{b}$ such that $E_2 \cong \mathfrak{b}E_1$, and therefore

$$E_2^\sigma \cong (\mathfrak{b}E_1)^\sigma = \mathfrak{b}^\sigma E_1^\sigma = \mathfrak{b}E_1^\sigma \cong \mathfrak{b}\mathfrak{a}E_1 = \mathfrak{a}\mathfrak{b}E_1 \cong \mathfrak{a}E_2,$$

where the second equality holds since $\mathfrak{b} \subseteq K$ and every $\sigma \in \mathrm{Gal}(L/K)$ fixes K.
Note that this would not have been true if we had taken $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Moreover, the first equality is not immediate and requires a more detailed argument involving a diagram chase, which we omit here, see [13, Prop. II.2.5] for a proof.
Since E_2 was arbitrary, it follows that the action of σ on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ coincides with the action of the ideal class $[\mathfrak{a}] \in C(\mathcal{O})$. Moreover, as the action of $C(\mathcal{O})$ on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ is not only transitive but also free by Remark 5.1.2, the map that sends each $\sigma \in \mathrm{Gal}(\overline{K}, K)$ to the unique class $[\mathfrak{a}] \in C(\mathcal{O})$ satisfying $E_1^\sigma = \mathfrak{a}E_1$ defines a group homomorphism

$$\Psi : \mathrm{Gal}(L/K) \to C(\mathcal{O}).$$

Theorem 5.5.1. *Let L be the splitting field of the ring class polynomial $H_D(X)$ over $K = \mathbb{Q}(\sqrt{D})$. The map $\Psi : \mathrm{Gal}(L/K) \to C(\mathcal{O}) : \sigma \mapsto \alpha_\sigma$, which assigns to each $\sigma \in \mathrm{Gal}(L/K)$ the unique class $\alpha_\sigma \in C(\mathcal{O})$ satisfying $j(E)^\sigma = \alpha_\sigma j(E)$ for all $j(E) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ is a well-defined and injective group homomorphism.*

Proof. Transitivity of the action of $C(\mathcal{O})$ on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ guarantees the existence of an ideal class $[\mathfrak{a}] \in C(\mathcal{O})$ for each $\sigma \in \mathrm{Gal}(L/K)$ such that $E^\sigma \cong \mathfrak{a}E$. Freeness of the action ensures the uniqueness of this class, so the the map Φ is well-defined. Since elliptic curves are classified up to isomorphism by their j-invariant (see Subection 2.5.1), we have $j(E)^\sigma = [\mathfrak{a}]j(E)$.
To show that Ψ is a homomorphism, let $\sigma_1, \sigma_2 \in \mathrm{Gal}(L/K)$, and let $[\mathfrak{a}_1], [\mathfrak{a}_2] \in C(\mathcal{O})$ be the corresponding classes with $E^{\sigma_i} = \mathfrak{a}_i E$. Then

$$E^{\sigma_1\sigma_2} = (E^{\sigma_1})^{\sigma_2} = (\mathfrak{a}_1 E)^{\sigma_2} = \mathfrak{a}_1 E^{\sigma_2} = \mathfrak{a}_1\mathfrak{a}_2 E,$$

so $\Psi(\sigma_1\sigma_2) = [\mathfrak{a}_1\mathfrak{a}_2] = \Psi(\sigma_1)\Psi(\sigma_2)$.
For injectivity, suppose $\sigma \in \mathrm{Gal}(L/K)$ satisfies $\Psi(\sigma) = \mathrm{id}_{C(\mathcal{O})}$. The trivial class in $C(\mathcal{O})$ is given by $\mathrm{id}_{C(\mathcal{O})} = [\mathcal{O}]$. Then, $E^\sigma = \mathcal{O}E = E$ for all $E \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$, which implies $j(E)^\sigma = j(E^\sigma) = j(E)$ by the previous section. Since the roots of the ring class polynomial $H_D(X)$ are precisely the j-invariants of elliptic curves with complex multiplication by $\mathcal{O}$ and $\mathrm{Gal}(L/K)$ acts on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ by permuting these roots, it follows that σ fixes all the roots of $H_D(X)$. By the definition of the splitting field L, the only element of $\mathrm{Gal}(L/K)$ that fixes all the roots of $H_D(X)$ is the identity automorphism. Hence, $\sigma = \mathrm{id}_{\mathrm{Gal}(L/K)}$, proving injectivity. □

It follows directly from the proof of the previous theorem that Ψ is $\mathrm{Gal}(L/K)$-*equivariant*, i.e. $j(E^\sigma) = \Psi(\sigma)j(E)$ for all $j(E) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ and $\sigma \in \mathrm{Gal}(L/K)$, which shows that the actions of $\mathrm{Gal}(L/K)$ and $C(\mathcal{O})$ on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ are compatible via the homomorphism Ψ. This can be illustrated by the commutative diagram:

$$\begin{array}{ccc} \mathrm{Gal}(L/K) \times \mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) & \longrightarrow & \mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) \\ \downarrow{\scriptstyle \Psi \times \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{id}} \\ C(\mathcal{O}) \times \mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) & \longrightarrow & \mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) \end{array},$$

where the top row represents the Galois action $(\sigma, j(E)) \mapsto j(E)^\sigma$ and the bottom row the ideal class group action $([\mathfrak{a}], j(E)) \mapsto [\mathfrak{a}]j(E)$. Following either path in the diagram yields $(\sigma, j(E)) \mapsto j(E)^\sigma = \alpha_\sigma j(E)$. Since $j(E)^\sigma = j(E^\sigma)$ by definition of the Galois action on j-invariants in the previous section, we obtain $j(E^\sigma) = \Psi(\sigma)j(E)$, showing that the diagram commutes and the actions are compatible via Φ.

5.5.2 Surjectivity

To prove surjectivity in the First main theorem of complex multiplication, we require a few additional tools that will allow us to describe the image of the Galois action more precisely.

i. The Frobenius automorphism as generator of Galois groups of finite fields
Consider the *Frobenius endomorphism*

$$x \mapsto x^p.$$

When regarded as a map on the finite field $\mathbb{F}_p$ of prime order p, it acts as the identity. However, when extended to the algebraic closure $\overline{\mathbb{F}}_p$, it becomes a nontrivial field automorphism, called the *Frobenius automorphism*, which we denote by π.
Every power π^n is again an automorphism of $\overline{\mathbb{F}}_p$, and its fixed field is precisely the finite field $\mathbb{F}_{p^n}$ with p^n elements. In particular, for a finite field $\mathbb{F}_q = \mathbb{F}_{p^n}$, the map $x \mapsto x^q$ is called the *q-power Frobenius automorphism.*

The Frobenius automorphism generates the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ for each finite extension $\mathbb{F}_{p^n} \subseteq \overline{\mathbb{F}}_p$. Indeed, $\mathbb{F}_{p^n}$ is a Galois extension of $\mathbb{F}_p$ for all $n \geq 1$ and its Galois group is cyclic of order n. The generator of this cyclic group is precisely the Frobenius automorphism π, whose powers act as

$$\pi^k(x) = x^{p^k}.$$

Since $\pi^n(x) = x^{p^n} = x$ for all $x \in \mathbb{F}_{p^n}$ and $\pi^k \neq \mathrm{id}$ for $0 < k < n$, the order of π is exactly n. Thus, we have

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \pi \rangle \cong \mathbb{Z}/n\mathbb{Z}.$$

ii. Ramification in finite Galois extensions
The ring of integers $\mathcal{O}_K$ of a number field K is a Dedekind domain, which means that every nonzero proper ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ admits a unique factorization into a product of prime ideals, i.e.

$$\mathfrak{p} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r},$$

where the $\mathfrak{p}_i$ are distinct non-zero prime ideals of $\mathcal{O}_K$ and $\nu_i \in \mathbb{Z}_{>0}$ for $1 \leq i \leq r$.
Now let L be a finite Galois extension of K and consider the ideal extension $\mathfrak{p}\mathcal{O}_L$. This is typically not a prime ideal, but it factors uniquely as

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1 \cdots \mathfrak{q}_r,$$

where the $\mathfrak{q}_i$ are (not necessarily distinct) prime ideals of $\mathcal{O}_L$ satisfying $\mathfrak{q}_i \cap \mathcal{O}_K = \mathfrak{p}$ for $1 \leq i \leq r$. The prime ideals $\mathfrak{q}_i$ are said to *lie above* $\mathfrak{p}$. Moreover, when the $\mathfrak{q}_i$ are distinct, we say that $\mathfrak{p}$ is *unramified* in L.

iii. The decomposition group, the Frobenius element and the Artin map
Let $\sigma \in \mathrm{Gal}(L/K)$ and apply it to both sides of the above factorization $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1 \cdots \mathfrak{q}_r$. By definition, σ fixes all elements of K and respects algebraic relations over K, so it maps algebraic integers to algebraic integers. In particular, it preserves the ring of integers $\mathcal{O}_L$, i.e. $\sigma(\mathcal{O}_L) = \mathcal{O}_L$. Consequently, $\sigma(\mathfrak{p}\mathcal{O}_L) = \mathfrak{p}\mathcal{O}_L$. We now turn to the right hand side. Since automorphisms preserve sums and products, σ maps each prime ideal $\mathfrak{q}_i \subseteq \mathcal{O}_L$ to another prime ideal $\sigma(\mathfrak{q}_i) \subseteq \mathcal{O}_L$. Again by the automorphism property, the image of a prime ideal is a prime ideal and so σ sends each prime ideal in the factorization to another prime ideal lying over $\mathfrak{p}$, i.e. $\sigma(\mathfrak{q}_i) \cap \mathcal{O}_K = \mathfrak{p}$. Hence, $\mathrm{Gal}(L/K)$ acts on the set $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\}$ by permutation. For each $\mathfrak{q}_i$, its stabilizer under this action is a subgroup

$$D_{\mathfrak{q}} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{q}) = \mathfrak{q}\} \subseteq \mathrm{Gal}(L/K)$$

called the *decomposition group* of $\mathfrak{q}_i$.

Now, given $\sigma \in D_{\mathfrak{q}}$, we define a map on the residue field $\mathbb{F}_{\mathfrak{q}} \coloneqq \mathcal{O}_L/\mathfrak{q}$ by

$$\overline{\sigma} : \mathbb{F}_{\mathfrak{q}} \to \mathbb{F}_{\mathfrak{q}} : \overline{x} \mapsto \overline{\sigma(x)},$$

where $\overline{x}$ denotes the image of $x \in \mathcal{O}_L$ under the natural projection $\mathcal{O}_L \to \mathcal{O}_L/\mathfrak{q}$. This map is well-defined since $\sigma \in D_{\mathfrak{q}}$ fixes $\mathfrak{q}$: if $x \equiv y \bmod \mathfrak{q}$, then $x - y \in \mathfrak{q}$, which implies $\sigma(x - y) \in \mathfrak{q}$ and so $\sigma(x) \equiv \sigma(y) \bmod \mathfrak{q}$.
Since in a Dedekind domain every prime ideal is maximal, the quotient $\mathcal{O}_L/\mathfrak{q}$ is a field. Moreover, $\mathfrak{q}$ has finite index $\mathrm{N}\mathfrak{q} = [\mathcal{O}_L : \mathfrak{q}]$ in $\mathcal{O}_L$, so $\mathbb{F}_{\mathfrak{q}}$ is a finite field of cardinality $\mathrm{N}\mathfrak{q}$ (which must be a prime power). Furthermore, since σ fixes K, it also fixes $\mathcal{O}_K$, and the image of $\mathcal{O}_K$ under the natural projection $\mathcal{O}_L \to \mathcal{O}_L/\mathfrak{q} = \mathbb{F}_{\mathfrak{q}}$ is $\mathcal{O}_K/(\mathfrak{q} \cap \mathcal{O}_K) = \mathcal{O}_K/\mathfrak{p} =: \mathbb{F}_{\mathfrak{p}}$, so $\mathbb{F}_{\mathfrak{p}}$ is a subfield of $\mathbb{F}_{\mathfrak{q}}$ (and necessarily has the same characteristic). Since the extension $\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}}$ is finite and hence Galois, it follows that $\overline{\sigma} \in \mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$ and we obtain a group homomorphism

$$D_{\mathfrak{q}} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}}) : \sigma \mapsto \overline{\sigma}.$$

This homomorphism is surjective (by the exactness of the sequence $1 \to I_\mathfrak{q} \to D_\mathfrak{q} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p}) \to 1$, where $I_\mathfrak{q}$ denotes the inertia group; see [8, Prop. I.9.4]. Moreover, if $\mathfrak{p}$ is unramified, the kernel $I_\mathfrak{q}$ is trivial (see [8, Prop. I.9.6]), so the map is an isomorphism. From now on, we assume that $\mathfrak{p}$ is unramified.

We already know that the group $\mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ is cyclic, generated by the Frobenius automorphism $x \mapsto x^{\mathrm{N}\mathfrak{p}}$, where $\mathrm{N}\mathfrak{p} = [\mathcal{O}_K : \mathfrak{p}] = |\mathbb{F}_\mathfrak{p}|$. The unique element $\sigma_\mathfrak{q} \in D_\mathfrak{q}$ whose reduction $\overline{\sigma}_\mathfrak{q}$ is the Frobenius automorphism, is called the *Frobenius element* of $\mathrm{Gal}(L/K)$ at $\mathfrak{q}$. Note that uniqueness holds by the injectivity of the reduction map, and the existence follows from its surjectivity.
In general, the Frobenius element $\sigma_\mathfrak{q}$ depends on the choice of the prime ideal $\mathfrak{q}$ lying over $\mathfrak{p}$. However, if $\mathfrak{q}_i$ and $\mathfrak{q}_j$ are two such prime ideals and $\sigma(\mathfrak{q}_i) = \mathfrak{q}_j$ for some $\sigma \in \mathrm{Gal}(L/K)$, then conjugation by σ sends $D_{\mathfrak{q}_i}$ to $D_{\mathfrak{q}_j}$. This means that if $\sigma_{\mathfrak{q}_i} \in D_{\mathfrak{q}_i}$, then $\sigma\sigma_{\mathfrak{q}_i}\sigma^{-1} \in D_{\mathfrak{q}_j}$ and so $\sigma_{\mathfrak{q}_j} = \sigma\sigma_{\mathfrak{q}_i}\sigma^{-1}$. Hence, all Frobenius elements at prime ideals lying over $\mathfrak{p}$ are conjugate in $\mathrm{Gal}(L/K)$.
It follows that the $\overline{\sigma}_{\mathfrak{q}_i}$ are also conjugate in their respective residue field Galois groups, since the reduction map respects conjugation, and thus have the same order. Each Galois group $\mathrm{Gal}(\mathbb{F}_{\mathfrak{q}_i}/\mathbb{F}_\mathfrak{p})$ is cyclic and generated by the Frobenius automorphisms $\overline{\sigma}_{\mathfrak{q}_i}$, so the order of $\overline{\sigma}_{\mathfrak{q}_i}$ equals the degree of the field extension $\mathbb{F}_{\mathfrak{q}_i}/\mathbb{F}_\mathfrak{p}$. By injectivity of the reduction map, the order of the $\sigma_{\mathfrak{q}_i}$ equals the order of its image $\overline{\sigma}_{\mathfrak{q}_i}$, so the degrees of the extensions $\mathbb{F}_{\mathfrak{q}_i}/\mathbb{F}_\mathfrak{p}$ are equal for all i. Since finite fields are uniquely determined up to isomorphism by their size, the extensions $\mathbb{F}_{\mathfrak{q}_i}/\mathbb{F}_\mathfrak{p}$ are all isomorphic.

However, when $\mathrm{Gal}(L/K)$ is abelian, all elements commute, so for any $\sigma, \tau \in \mathrm{Gal}(L/K)$ we have $\sigma\tau\sigma^{-1} = \tau$, i.e. conjugation has no effect Therefore, the Frobenius element no longer depends on the choice of $\mathfrak{q}$ lying over $\mathfrak{p}$.Consequently, each unramified prime ideal $\mathfrak{p}$ determines a unique Frobenius element $\sigma_\mathfrak{p}$. We define the map

$$\mathfrak{p} \mapsto \sigma_\mathfrak{p},$$

known as the *Artin map*, which assignes to each unramified prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ its corresponding Frobenius element $\sigma_\mathfrak{p}$ in $\mathrm{Gal}(L/K)$. While this map extends multiplicatively to all $\mathcal{O}_K$-ideals that are products of unramified prime ideals, here we only focus on prime ideals. The automorphism $\sigma_\mathfrak{p}$ is uniquely characterized by property

$$\sigma_\mathfrak{p}(x) \equiv x^{\mathrm{N}\mathfrak{p}} \bmod \mathfrak{q}$$

for all $x \in \mathcal{O}_L$ and for every prime ideal $\mathfrak{q} \subseteq \mathcal{O}_L$ lying above $\mathfrak{p}$.

iv. Elliptic curves over number fields and good reduction modulo $\mathfrak{q}$
While the theory of elliptic curves over $\mathbb{C}$ provides the analytic and geometric foundations, studying curves over number fields reveals their deep arithmetic properties and connection to prime numbers. We have already encountered elliptic curves over number fields when observing that an elliptic curve E with j-invariant $j(E)$ gives rise to Galois conjugates E^σ, defined over $\mathbb{Q}(\sigma(j(E)))$. This motivates working over number fields such as $\mathbb{Q}(j(E))$ rather than over $\mathbb{C}$ alone. We now expand this idea by passing to a finite

Galois extension L of $\mathbb{Q}$ - for instance, the splitting field of the ring class polynomial - so that all j-invariants of elliptic curves with complex multiplication lie in L.
In particular, since all j-invariants of elliptic curves with complex multiplication by $\mathcal{O}$ lie in L, and every root of the ring class polynomial $H_D(X)$ (which splits in L) corresponds to a complex elliptic curve with complex multiplication by $\mathcal{O}$, the sets of j-invariants of elliptic curves with complex multiplication by $\mathcal{O}$ over $\mathbb{C}$ and L coincide:

$$\mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) = \mathrm{Ell}_{\mathcal{O}}(L).$$

Given this identity, for an elliptic curve E over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$, we have $j(E) \in L$, which implies that (up to isomorphism) E can be defined by a Weierstrass equation $y^2 = x^3 + Ax + B$ with $A, B \in L$. As in the proof of Theorem 2.5.7, we can express A and B in terms of $j(E)$ as $A = 3j(E)(1728 - j(E))$ and $B = 2j(E)(1728 - j(E))^2$ for $j(E) \neq 0, 1728$, which ensures that $A, B \in \mathcal{O}_L$ since $j(E)$ is an algebraic integer.
Then, for any prime ideal $\mathfrak{q}$ of L, as long the discriminant $\Delta(E) = -16(4A^3 + 27B^2)$ does not lie in $\mathfrak{q}$, or equivalently, the image of $\Delta(E)$ under the quotient map $\mathcal{O}_L \to \mathcal{O}_L/q = \mathbb{F}_{\mathfrak{q}}$ is non-zero, reducing E modulo $\mathfrak{q}$ yields an elliptic curve $\overline{E}$ over $\mathbb{F}_{\mathfrak{q}}$ defined by $y^2 = x^3 + \overline{A}x + \overline{B}$. We then say that E has *good reduction modulo* $\mathfrak{q}$. This holds for all but finitely many prime ideals $\mathfrak{q}$ of L, since the principal ideal $(\Delta(E))$ is divisible by only finitely many prime ideals, by the finite unique factorization of ideals in Dedekind domains.

v. The Frobenius endomorphism and the decomposition of isogeny degree
Let E be an elliptic curve over a finite field $\mathbb{F}_q$. The *Frobenius endomorphism of* E is the map

$$\pi_E : (x, y) \mapsto (x^q, y^q)$$

where $q = |\mathbb{F}_{\mathfrak{q}}|$. This map reflects the action of the q-power Frobenius automorphism on the coordinates of points on E. It defines an isogeny of degree q from E to the curve $E^{(q)}$, given by the equation $y^2 = x^3 + \overline{A}^q x + \overline{B}^q$.
In particular, π_E is the standard example of an inseparable isogeny.

In Section 5.2, we saw that all isogenies over a field of characteristic zero are separable. In positive characteristic, however, not all isogenies are separable. Indeed, every isogeny ϕ of elliptic curves over a field K of characteristic $p > 2$ can be decomposed into a separable part and an inseparable part involving the Frobenius endomorphism of E as

$$\phi = \phi_{\mathrm{sep}} \circ \pi^n,$$

where ϕ_{sep} is a separable isogeny and $n \geq 0$ is an integer. The degree of ϕ then satisfies $\deg(\phi) = p^n \deg(\phi_{\mathrm{sep}})$. For a proof, see [14, Cor. 5.4].
Accordingly, the *separable degree* $\deg_s(\phi)$ and *inseparable degree* $\deg_i(\phi)$ of ϕ are defined by

$$\deg_s(\phi) = \deg(\alpha_{\mathrm{sep}}) \quad \text{and} \quad \deg_i(\phi) = p^n,$$

so that

$$\deg(\phi) = \deg_s(\phi)\deg_i(\phi).$$

Note that the inseparable isogeny π^n has separable degree 1, and such isogenies are called *purely inseparable*. In particular, this shows that the Frobenius endomorphism π_E is purely inseparable.

vi. The dual isogeny

In Section 5.2, we saw that the degree of separable isogenies is finite and equals to the order of its kernel. More generally, for any isogeny, the order of its kernel equals the separable degree; a proof can be found in [14, Thm. 5.8].

Recall also that for all $n \in \mathbb{Z}$, the map $[n]$ denotes multiplication-by-n on an elliptic curve. Using the fact that the order of the kernel of an isogeny ϕ equals its separable degree, which ensures the existence of a separable isogeny with any given finite kernel, and the fact that the separable degree divides the degree of ϕ as seen earlier, one can show the following: for any isogeny $\phi : E_1 \to E_2$ of elliptic curves over a field K, there exists a unique isogeny $\hat{\phi} : E_2 \to E_1$ such that

$$\hat{\phi} \circ \phi = [n],$$

where $n = \deg(\phi)$. This isogeny $\hat{\phi}$ is called the *dual isogeny* of ϕ. See [14, Section 6.3] for more details.

With these preparations in place, we are now ready to state the full First main theorem of complex multiplication and establish surjectivity.

Theorem 5.5.2 (First main theorem of complex multiplication)**.** *Let L be the splitting field of the ring class polynomial $H_D(X)$ over $K = \mathbb{Q}(\sqrt{D})$. The map $\Psi : \mathrm{Gal}(L/K) \to C(\mathcal{O}) : \sigma \mapsto \alpha_\sigma$, which assigns to each $\sigma \in \mathrm{Gal}(L/K)$ the unique class $\alpha_\sigma \in C(\mathcal{O})$ satisfying $j(E)^\sigma = \alpha_\sigma j(E)$ for all $j(E) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ is a group isomorphism and is compatible with the actions of $\mathrm{Gal}(L/K)$ and $C(\mathcal{O})$ on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$.*

Proof. In Theorem 5.5.1 and the subsequent discussion, we have already seen that Ψ is well-defined, injective, and commutes with the group actions of $\mathrm{Gal}(L/K)$ and $C(\mathcal{O})$ on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$. It remains to show surjectivity.

Let $\alpha \in C(\mathcal{O})$ and choose a prime ideal $\mathfrak{p}$ in K such that:

(i) $\mathfrak{p} \cap \mathcal{O}$ is a proper $\mathcal{O}$-ideal of prime norm p with $[\mathfrak{p}] = \alpha$,
(ii) p is unramified in K and $\mathfrak{p}$ is unramified in L,
(iii) Each $j(E) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ corresponds to an elliptic curve E over L that has good reduction modulo every prime ideal $\mathfrak{q}$ lying over $\mathfrak{p}$,
(iv) The reductions of the j-invariants of elliptic curves in $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ modulo every prime ideal $\mathfrak{q}$ lying over $\mathfrak{p}$ are distinct.

By Lemma 5.3.7, there are infinitely many prime ideals $\mathfrak{p}$ satisfying (i), while conditions (ii)-(iv) exclude only finitely many prime ideals, so such a $\mathfrak{p}$ exists.

For simplicity, we will also use $\mathfrak{p}$ to denote the $\mathcal{O}$-ideal $\mathfrak{p} \cap \mathcal{O}$; the context will clarify whether we view it as an $\mathcal{O}_K$-ideal or an $\mathcal{O}$-ideal.

Now consider a prime ideal $\mathfrak{q}$ lying over $\mathfrak{p}$ and an elliptic curve E over L with complex multiplication by $\mathcal{O}$ that has good reduction modulo $\mathfrak{q}$. Then E can be written as $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathcal{O}_L$ and $\mathfrak{q} \nmid (\Delta(E))$ in $\mathcal{O}_L$, where $(\Delta(E))$ denotes the principal ideal generated by the discriminant $\Delta(E)$ in $\mathcal{O}_L$. Let $\mathbb{F}_\mathfrak{q} = \mathcal{O}_L/\mathfrak{q}$ and denote by $\overline{E}$ the reduction of E modulo $\mathfrak{q}$, given by the equation $y^2 = x^3 + \overline{A}x + \overline{B}$ over $\mathbb{F}_\mathfrak{q}$, where $\overline{A}, \overline{B}$ are the images of A, B under the reduction map.
Since $\mathrm{N}\mathfrak{p} = p$ by (i), the Frobenius element $\sigma_\mathfrak{p}$ induces the p-power Frobenius automorphism $\overline{\sigma}_\mathfrak{p} \in \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_p)$. Correspondingly, we have the isogeny

$$\pi : \overline{E} \to \overline{E^{\sigma_\mathfrak{p}}} = \overline{E}^{\overline{\sigma}_p} = \overline{E}^{(p)},$$

given by $(x, y) \mapsto (x^p, y^p)$. The second equality follows from the fact that $\overline{\sigma}_\mathfrak{p}$ acts on the coefficients of E by raising them to the p-th power, giving the curve $\overline{E}^{(p)}$ defined by the equation $y^2 = x^3 + \overline{A}^p x + \overline{B}^p$. As seen above, the isogeny π is purely inseparable of degree p.
By Proposition 5.2.1, the proper $\mathcal{O}$-ideal $\mathfrak{p} \cap \mathcal{O}$ corresponds to an isogeny $\phi_\mathfrak{p} : E \to \mathfrak{p}E$ of degree $\mathrm{N}\mathfrak{p}$, where $\mathfrak{p}E$ has good reduction modulo $\mathfrak{q}$ by (iii). We may assume that $\phi_\mathfrak{p}$ is given by a rational map of the form $\left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$, with $u, v, s, t \in \mathcal{O}_L[x]$, u monic and v non-zero modulo $\mathfrak{q}$, as seen in Section 3.1. Reducing the coefficients of u, v, s and t modulo $\mathfrak{q}$ yields an isogeny

$$\phi : \overline{E} \to \overline{\mathfrak{p}E}$$

over $\mathbb{F}_\mathfrak{q}$, which has the same degree as π, namely p. This follows from the fact that we can assume $\deg(v) < \deg(u)$ and since u is monic, the degree of the rational map is preserved under reduction. The composition of ϕ with his dual $\hat{\phi}$ equals the multiplication-by-p map on $\overline{E}$ as discussed in the preparation, which is inseparable, since $\mathbb{F}_\mathfrak{q}$ has characteristic p. Hence at least one of ϕ or $\hat{\phi}$ must be inseparable.
Without loss of generality, assume that ϕ is inseparable. If not, replace E by $\mathfrak{p}E$ and $\mathfrak{p}$ by its complex conjugate $\overline{\mathfrak{p}}$, which still satisfies conditions (i)-(iv) and induces the dual isogeny $\hat{\phi}_\mathfrak{p} : \mathfrak{p}E \to E$ (up to isomorphism). Indeed, since $\overline{\mathfrak{p}}\mathfrak{p} = (\mathrm{N}\mathfrak{p}) = (p)$, this induces the multiplication-by-p map on E and reducing the rational maps defining $\overline{\mathfrak{p}}$ yields the dual isogeny $\hat{\phi} : \mathfrak{p}E \to E$. This ensures that we always have an inseparable isogeny to work with. By the preparation, an inseparable isogeny of degree p factors as $\phi = \phi_{\mathrm{sep}} \circ \pi$, where ϕ_{sep} is a separable isogeny of degree 1, hence an isomorphism (see Section 5.2). Therefore,

$$\overline{\mathfrak{p}E} \cong \mathrm{Im}(\phi) = \mathrm{Im}(\phi_{\mathrm{sep}} \circ \pi) \cong \mathrm{Im}(\pi) = E^{(p)} = \overline{E^{\sigma_\mathfrak{p}}},$$

and so $j(\overline{\mathfrak{p}E}) \cong j(\overline{E^{\sigma_\mathfrak{p}}})$ by the classification of elliptic curves over $\mathbb{C}$ by their j-invariant (Subsection 2.5.1). Then condition (iv) gives $j(\mathfrak{p}E) \cong j(E^{\sigma_\mathfrak{p}})$ over L, hence $\mathfrak{p}E \cong E^{\sigma_\mathfrak{p}}$, i.e. that the action of the ideal class $[\mathfrak{p}]$ on E coincides with the Galois action of $\sigma_\mathfrak{p}$ on E. Finally, since this class in $C(\mathcal{O})$ is uniquely determined by its action on E by the freeness of the action of $C(\mathcal{O})$ on $\mathrm{Ell}_\mathcal{O}(\mathbb{C})$ (Remark 5.1.2), we conclude that $\Psi(\sigma_\mathfrak{p}) = [\mathfrak{p}] = \alpha$, establishing surjectivity. □

Remark 5.5.3. *The title of this theorem suggests the existence of a broader result, known as the Second main theorem of complex multiplication. This theorem generalizes the First main theorem and relates the field of complex multiplication to the maximal abelian extension of a quadratic field. While the First main theorem constructs the ring class field via j-invariants of elliptic curves with complex multiplication, the Second main theorem describes how all abelian extensions of an imaginary quadratic field can be generated by the values of more general modular functions - such as modular units or values of Weber and Siegel functions - evaluated at elliptic curves with complex multiplication. This requires a deeper understanding of class field theory beyond the ring class field. For more details, see [3, p.189-190].*

5.6 Consequences and ring class fields

Having established the First main theorem of complex multiplication, we can now explore its arithmetic consequences. In particular, the theorem allows us to describe the fields generated by the j-invariants of elliptic curves with complex multiplication. This leads naturally to the notion of ring class fields and their relation to the ideal class group. By examining these fields, we not only obtain information about the degrees and Galois groups of the extensions they generate but also recover important integrality properties of the j-invariants themselves.

Corollary 5.6.1. *The ring class polynomial $H_D(X)$ is irreducible over $K = \mathbb{Q}(\sqrt{D})$. Moreover, for any elliptic curve E over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$, the field $K(j(E))$ is a finite abelian extension of K with $\mathrm{Gal}(K(j(E))/K) \cong C(\mathcal{O})$.*

Proof. Let L be the splitting field of the ring class polynomial $H_D(X)$ over K. Since the ideal class group $C(\mathcal{O})$ acts transitively on the set of isomorphism classes in $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ (Remark 5.1.2), it also acts transitively on the set of roots of $H_D(X)$ via its action on the corresponding j-invariants. By the First main theorem of complex multiplication 5.5.2, the Galois group $\mathrm{Gal}(L/K)$ is isomorphic to $C(\mathcal{O})$ and thus also acts transitively on the roots of $H_D(X)$ as well. It follows from a standard result in Galois theory that $H_D(X)$ is irreducible over K and hence it is the minimal polynomial of each of its roots. Since $H_D(X)$ is defined as the product over all j-invariants of elliptic curves with complex multiplication by $\mathcal{O}$, its roots correspond bijectively to the isomorphism classes in $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$, which in turn are in bijection with $C(\mathcal{O})$ (see Section 5.1). Therefore, the degree of $H_D(X)$ equals the class number $h(\mathcal{O}) = |C(\mathcal{O})|$. Thus, we obtain

$$\deg(H_D(X)) = h(\mathcal{O}) = |C(\mathcal{O})| = |\mathrm{Gal}(L/K)| = [L : K].$$

Since $H_D(X)$ is irreducible over K, it follows that the field L is generated over K by any of its roots, i.e. $L = K(j(E))$ for every root $j(E)$ of $H_D(X)$, or equivalently, for every $j(E) \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$. The claim then follows from the isomorphism $\mathrm{Gal}(L/K) \cong C(\mathcal{O})$ by the First main theorem of complex multiplication 5.5.2, noting that this group is abelian. □

Definition 5.6.2 (Ring class field, Hilbert class field)**.** The *ring class field* of $\mathcal{O}$ is the splitting field of the ring class polynomial $H_D(X)$ over K, or equivalently, the extension of K generated by the j-invariant of any elliptic curve with complex multiplication by $\mathcal{O}$. The *Hilbert class field* of K is defined analogously by taking $\mathcal{O} = \mathcal{O}_K$, the maximal order of K.

Using this definition, we can restate Corollary 5.6.1 more conceptually as follows.

Corollary 5.6.3. *Let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$. Then the ring class field of $\mathcal{O}$ is given by $K(j(E))$. In particular, its degree over K equals the class number $h(\mathcal{O})$.*

Note that for two orders $\mathcal{O}$ and $\mathcal{O}'$ with $\mathcal{O}' \subseteq \mathcal{O}$ and corresponding ring class fields L and L', we have $L \subseteq L'$. Indeed, let E be an elliptic curve over $\mathbb{C}$ with $\mathrm{End}(E) \cong \mathcal{O}$. Since $\mathcal{O}' \subseteq \mathcal{O}$, the endomorphisms in $\mathcal{O}'$ act on E, so E admits complex multiplication by $\mathcal{O}'$ (though $\mathrm{End}(E) \cong \mathcal{O}$). It follows that the j-invariant of E is also a root of the ring class polynomial $H_{\mathcal{O}'}$. By definition, the ring class field of L' is generated by any root of $H_{\mathcal{O}'}$, i.e. by the j-invariant of any elliptic curve with complex multiplication by $\mathcal{O}'$. Hence, $j(E) \in L'$. Since E was an arbitrary elliptic curve with complex multiplication by $\mathcal{O}$, every j-invariant generating the ring class field L of $\mathcal{O}$ lies in L', and thus $L \subseteq L'$.

We now examine the consequences of this corollary for the arithmetic of $j(E)$, particularly its integrality and its relation to the class number of $\mathcal{O}$.
As seen in Theorem 5.3.8 that $j(E)$ is an algebraic integer, and therefore naturally lies in the ring of integers of the field it generates. By Corollary 5.6.3, the ring class field of the order $\mathcal{O}$ is generated over $K = \mathbb{Q}(\sqrt{D})$ by the j-invariant $j(E)$ of any elliptic curve E with complex multiplication by $\mathcal{O}$, and the degree $[K(j(E)) : K]$ of this extension equals the class number $h(\mathcal{O}) = |C(\mathcal{O})|$. Since the ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$, $j(E)$ lies in $\mathbb{Z}$ exactly when it is rational. This happens exactly when the ring class field $K(j(E))$ coincides with K itself, so when $h(\mathcal{O}) = 1$. This leads directly to the following significant result, which will play a key role in our ultimate goal of showing that $e^{\pi\sqrt{163}}$ is almost an integer:

Corollary 5.6.4. *Let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$. Then $j(E) \in \mathbb{Z}$ if and only if $h(\mathcal{O}) = 1$.*

5.7 Orders in imaginary quadratic number fields with class number one

Building on the previous corollary linking j-invariant integrality to class numbers, we now aim to classify orders in imaginary quadratic number fields. To this end, we recall the necessary tools and then use them to determine all orders of class number one, both maximal and non-maximal, along with their discriminants.

Throughout this section, let $\mathcal{O}$ and $\mathcal{O}'$ denote orders in an imaginary quadratic number field K, with maximal order $\mathcal{O}_K$ and conductor $f = [\mathcal{O}_K : \mathcal{O}]$ for $\mathcal{O}$.

Recall the definition of the *Legendre symbol* $(\frac{a}{p})$ for odd primes $p > 2$:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \bmod p, \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \bmod p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p, \end{cases}$$

where an integer a is called a *quadratic residue* modulo p, if there is an integer x such that $x^2 \equiv q \bmod p$. Otherwise a is called a *quadratic non-residue* modulo p.
By Euler's criterion, Legendre's symbol can be calculated more explicitly:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p \quad \text{and} \quad \left(\frac{a}{p}\right) \in \{0, 1, -1\}.$$

For $p = 2$, the symbol $(\frac{a}{2})$ is called the Kronecker symbol and is defined as

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & \text{if } 2 \mid a \\ 1 & \text{if } a \equiv \pm 1 \bmod 8 \\ -1 & \text{if } a \equiv \pm 3 \bmod 8. \end{cases}$$

Also recall from Remark 3.3.2 that an order $\mathcal{O}$ can be written as $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = [1, f\omega_K]$.

Proposition 5.7.1. *Let $\mathcal{O}^*$ and $\mathcal{O}_K^*$ denote the groups of units of $\mathcal{O}$ and $\mathcal{O}_K$, respectively, d_K be the discriminant of K, and $(\frac{d_K}{p})$ the Legendre-Kronecker symbol. Then*

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K) f}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{\substack{p \mid f \\ p \text{ prime}}} \left(1 - \left(\frac{d_K}{p}\right) \frac{1}{p}\right).$$

Moreover, $h(\mathcal{O})$ is an integer multiple of $h(\mathcal{O}_K)$.

Proof. For a proof, see [3, Thm. 7.24]. □

For future reference, we state the following consequence of the previous proposition, which relates the class number of an order $\mathcal{O}$ of discriminant D to that of some suborder $\mathcal{O}'$ of index N.

Proposition 5.7.2. *Let $D \equiv 0, 1 \bmod 4$ be negative and let N be a positive integer. Furthermore, let $\mathcal{O}$ and $\mathcal{O}'$ be orders of discriminant D and $N^2 D$, respectively. Then*

$$h(\mathcal{O}') = \frac{h(\mathcal{O}) N}{[\mathcal{O}^* : \mathcal{O}'^*]} \prod_{\substack{p \mid N \\ p \text{ prime}}} \left(1 - \left(\frac{D}{p}\right) \frac{1}{p}\right),$$

where $\mathcal{O}^*$ and $\mathcal{O}'^*$ denote the groups of units of $\mathcal{O}$ and $\mathcal{O}'$, respectively.

Proof. See [3, Cor 7.28] for a proof. □

For our calculations, we will also need the following proposition:

Proposition 5.7.3. *Let K be an imaginary quadratic number field of discriminant d_K. Then for the group of units $\mathcal{O}_K^*$ we have:*

$$\mathcal{O}_K^* = \begin{cases} \{\pm 1, \pm\omega, \pm\omega^2\} & \text{for } d_K = -3 \\ \{\pm 1, \pm i\} & \text{for } d_K = -4 \\ \{\pm 1\} & \text{for } d_K < 0,\ d_K \notin \{-3, -4\}, \end{cases}$$

where $\omega = e^{\frac{2\pi i}{3}}$ denotes the third root of unity.

Proof. A proof can be found in [8, Prop. 4.2]. □

Remark 5.7.4. *We observe that:*

- *If $|\mathcal{O}_K| = 2$, then $[\mathcal{O}_K^* : \mathcal{O}^*] = 1$, since ± 1 are always units,*
- *If $|\mathcal{O}_K| = 4$, then $[\mathcal{O}_K^* : \mathcal{O}^*] = 2$, since $\pm i \notin [1, fi]$ for $f > 1$,*
- *If $|\mathcal{O}_K| = 6$, then $[\mathcal{O}_K^* : \mathcal{O}^*] = 3$, since $\pm e^{\frac{2\pi i}{3}}$, $e^{\frac{4\pi i}{3}} \notin [1, fe^{\frac{2\pi i}{3}}]$ for $f > 1$.*

The formula in Proposition 5.7.1 provides a practical tool for identifying orders with a given class number h. To this end, we rewrite the formula by introducing the function

$$\Theta_K(f) \coloneqq f \prod_{\substack{p \mid f \\ p \text{ prime}}} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right),$$

which can be regarded as an analogue of Euler's totient function in the setting of quadratic orders. With this notation, the task of finding all orders of class number h reduces to solving

$$\Theta_K(f) = \frac{h(\mathcal{O})}{h(\mathcal{O}_K)}[\mathcal{O}_K^* : \mathcal{O}^*]$$

for the pair (f, d_K). Once a solution is found, the corresponding order $\mathcal{O}$ is uniquely determined by its discriminant $D = f^2 d_K$, as stated in Theorem 3.3.3.

Guided by Corollary 5.6.4, we are particularly interested in the case where the order $\mathcal{O}$ has class number one, and therefore assume $h(\mathcal{O}) = 1$. Since the class number $h(\mathcal{O})$ is an integer multiple of $h(\mathcal{O}_K)$ by Proposition 5.7.1, it follows that $h(\mathcal{O}_K) = 1$. Our task thus reduces to solving the following equation for (f, d_K):

$$\Theta_K(f) = [\mathcal{O}_K^* : \mathcal{O}^*].$$

In the special case $f = 1$, we have $\mathcal{O}_K = \mathcal{O}$ by definition of the conductor. This identifies the nine maximal orders with class number one in imaginary quadratic number fields, which were explicitly determined through the work of Baker, Heegner, and Stark:

Theorem 5.7.5. *There are exactly* 9 *maximal orders of class number one in imaginary quadratic number fields K, with discriminants*

$$d_K = -3, -4, -7, -8, -11, -19, -43, -67, -163.$$

Proof. A proof can be found in [3, Thm. 7.30]. □

It remains to check if there are non-maximal orders $\mathcal{O}$ with class number one. For that we assume $f > 1$ and examine the three cases of $[\mathcal{O}_K^* : \mathcal{O}^*]$ given by Remark 5.7.4. This allows us to identify all possible values for the conductor f.

Let $f = \prod_i p_i^{k_i}$ be the prime factorization of f. Then we can rewrite $\Theta_K(f)$ as

$$\Theta_K(f) = f \prod_{\substack{p \mid f \\ p \text{ prime}}} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right) = \prod_i p_i^{k_i - 1}\left(p_i - \left(\frac{d_K}{p_i}\right)\right).$$

Case 1: $[\mathcal{O}_K^* : \mathcal{O}^*] = 1$. Then we need to solve $\Theta_K(f) = 1$.
Since each factor $p_i^{k_i-1}\left(p_i - \left(\frac{d_K}{p_i}\right)\right)$ is a positive integer and their product equals 1, every factor must be 1 for each prime $p_i \mid f$.

Case 1.1: $\left(\frac{d_K}{p_i}\right) = 1$. Then $p_i^{k_i-1}(p_i - 1) = 1$ and so $p_i = 2$ and $k_i = 1$. Thus $d_K \equiv \pm 1 \bmod 8$ by definition of the Kronecker symbol and so $d_K = -7$ by Theorem 5.7.5.

Case 1.2: $\left(\frac{d_K}{p_i}\right) = -1$. Then $p_i^{k_i-1}(p_i + 1) = 1$, which is impossible.

Case 1.3: $\left(\frac{d_K}{p_i}\right) = 0$. Then $p_i^{k_i-1}p_i = p_i^{k_i} = 1$, which is impossible.

Hence $p_i = 2$ is the only prime dividing f, so $f = 2$. This identifies one non-maximal order with $(f, d_K) = (2, -7)$ and discriminant $D = f^2 d_K = -28$.

Case 2: $[\mathcal{O}_K^* : \mathcal{O}^*] = 2$. Then $d_K = -4$ by Proposition 5.7.3, and we solve $\Theta_K(f) = 2$.

Case 2.1: $\left(\frac{d_K}{p_i}\right) = 1$. Then $p_i^{k_i-1}(p_i - 1) \mid 2$ and so $p_i = 2$ and $k_i = 2$ or $p_i = 3$ and $k_i = 1$.

If $p_i = 2$, then $\left(\frac{-4}{2}\right) = 0$, which contradicts the assumption.

If $p_i = 3$, then $\left(\frac{-4}{3}\right) = -1$, which contradicts the assumption.

Case 2.2: $\left(\frac{d_K}{p_i}\right) = -1$. Then $p_i^{k_i-1}(p_i + 1) \mid 2$, which is impossible.

Case 2.3: $\left(\frac{d_K}{p_i}\right) = 0$. Then $p_i^{k_i-1}p_i = p_i^{k_i} \mid 2$ and so $p_i = 2$ and $k_i = 1$. Then $2 \mid d_K$ by definition of the Kronecker symbol, which is valid.

Thus $p_i = 2$ is the only prime dividing f, so again $f = 2$. This yields the non-maximal order with $(f, d_K) = (2, -4)$ and discriminant $D = -16$.

Case 3: $[\mathcal{O}_K^* : \mathcal{O}^*] = 3$. Then $d_K = -3$ by Proposition 5.7.3, and we solve $\Theta_K(f) = 3$.

Case 3.1: $\left(\frac{d_K}{p_i}\right) = 1$. Then $p_i^{k_i-1}(p_i - 1) \mid 3$ and so $p_i = 2$ and $k_i = 1$. Thus $d_K \equiv \pm 1 \bmod 8$ by definition of the Kronecker symbol, a contradiction to $-3 \equiv 5 \bmod 8$.

Case 3.2: $\left(\frac{d_K}{p_i}\right) = -1$. Then $p_i^{k_i-1}(p_i+1) \mid 3$ so $p_i = 2$ and $k_i = 1$. Then $d_K \equiv \pm 3 \mod 8$ by definition of the Kronecker symbol, which is valid.
Case 3.3: $\left(\frac{d_K}{p_i}\right) = 0$. Then $p_i^{k_i-1}p_i = p_i^{k_i} \mid 3$ and so $p_i = 3$ and $k_i = 1$. Thus $d_K \equiv 0 \mod 3$ by definition of the Kronecker symbol, which is valid.

Hence, $p_i = 2$ and $p_i = 3$ are the only primes dividing f, each occurring with exponent 1. Both contribute a factor of 3 to $\Theta_K(f)$, and since the total product must equal 3, at most one primes can appear. Thus the only possibilities are $f = 2$ or $f = 3$. This gives the two remaining non-maximal orders with $(f, d_K) = (2, -3)$ and $(f, d_K) = (3, -3)$ and discriminants $D = -12$ and $D = -27$, respectively.

Collecting all cases, we obtain the complete list of orders of class number one in imaginary quadratic number fields.

Corollary 5.7.6. *There are exactly* 13 *orders of class number one in imaginary quadratic number fields, thereof* 4 *are not maximal, with discriminants*

$$D = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163.$$

6 The cube root of the j-function and its role in ring class fields

In this chapter, we study a modular function closely related to the j-function: a specific cube root of j, denoted γ_2. Building on the First main theorem of complex multiplication and the theory of modular functions developed in Chapter 4, we explore an alternative path to constructing ring class fields through this cube root, providing a complementary perspective on the arithmetic of imaginary quadratic orders.
The chapter is organized into two sections. In the first, we introduce γ_2 and establish its modularity. The second section investigates the algebraic integrality of $\gamma_2(\tau)$ and its role in the explicit construction of ring class fields. Altogether, these results form a key ingredient for understanding the remarkable near-integer value of $e^{\pi\sqrt{163}}$, which serves as a central motivation for the computations presented here.

This chapter follows the presentation of [3, §12 A], with additional explanations and proofs included where appropriate.

6.1 The function γ_2 and its modularity

Our first step is to introduce the function γ_2 and demonstrate that it is itself modular, thereby preparing the ground for its role in the theory of ring class fields.

We begin by recalling the definition of the j-function of a lattice $L = [1, \tau]$, given by

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

where $\Delta(\tau)$ denotes the discriminant of L, defined by $\Delta(\tau) = g_2(\tau)^2 - 27g_3(\tau)^2$. To understand how a cube root of $j(\tau)$ can be defined, we first take a closer look at the functions involved.
The functions $g_2(\tau)$ and $g_3(\tau)$ are holomorphic on the upper half plane $\mathbb{H}$ as seen in the proof of Theorem 2.5.9, and hence so is $\Delta(\tau)$. Moreover, $\Delta(\tau)$ is non-zero on $\mathbb{H}$ by Theorem 2.3.22, which implies that a holomorphic cube root of $\Delta(\tau)$ exists on $\mathbb{H}$.
Since taking a complex cube root involves choosing a branch due to its multivalued nature, we first examine how $\Delta(\tau)$ and $j(\tau)$ behave under complex conjugation.

Definition 6.1.1 (Complex conjugate of a lattice)**.** Let L be a lattice in $\mathbb{C}$. The complex conjugate of L is defined by $\overline{L} = \{\overline{\omega} \mid \omega \in L\}$.

By definition, $\omega \in L$ holds if and only if $\overline{\omega} \in \overline{L}$.

Lemma 6.1.2. *Let L be a lattice in $\mathbb{C}$ and $\overline{L}$ its complex conjugate. Then $\overline{j(L)} = j(\overline{L})$.*

Proof. For any lattice $L \subseteq \mathbb{C}$, we have

$$\overline{g_2(L)} = 60 \sum_{\omega \in L \setminus \{0\}} \overline{\frac{1}{\omega^4}} = 60 \sum_{\omega \in L \setminus \{0\}} \frac{1}{\overline{\omega}^4} = 60 \sum_{\omega \in \overline{L} \setminus \{0\}} \frac{1}{\omega^4} = g_2(\overline{L}),$$

and similarly,

$$\overline{g_3(L)} = 140 \sum_{\omega \in L \setminus \{0\}} \overline{\frac{1}{\omega^6}} = 140 \sum_{\omega \in L \setminus \{0\}} \frac{1}{\overline{\omega}^6} = 140 \sum_{\omega \in \overline{L} \setminus \{0\}} \frac{1}{\omega^6} = g_3(\overline{L}),$$

where the first equality in each line follows from continuity of the complex conjugation. Thus,

$$\overline{j(L)} = 1728 \, \frac{\overline{g_2(L)}^3}{\overline{g_2(L)}^3 - 27\overline{g_3(L)}^2} = 1728 \, \frac{g_2(\overline{L})^3}{g_2(\overline{L})^3 - 27 g_3(\overline{L})^2} = j(\overline{L}).$$

□

Lemma 6.1.3. *Let $\tau \in \mathbb{H}$ be purely imaginary, i.e. $\tau = iy$ with $y > 0$. Then $\Delta(\tau) \in \mathbb{R}$.*

Proof. Let $\tau = iy$ with $y > 0$. Since $\Delta(\tau) = g_2(\tau)^3 - 27 g_3(\tau)^2$, it suffices to show that $g_2(\tau)$ and $g_3(\tau)$ are real-valued. Note that with $L = [1, \tau]$, we have

$$L = [1, iy] = [1, -iy] = [1, \overline{iy}] = \overline{[1, iy]} = \overline{L}.$$

Using Lemma 6.1.2, we obtain

$$\overline{g_2(L)} = g_2(\overline{L}) = g_2(L) \qquad \text{and} \qquad \overline{g_3(L)} = g_3(\overline{L}) = g_3(L).$$

Since $g_2(L) = g_2(\tau)$ and $g_3(L) = g_3(\tau)$ by definition, it follows that

$$g_2(\tau) = g_2(iy) = g_2([1, iy]) = g_2(\overline{[1, iy]}) = \overline{g_2([1, iy])} = \overline{g_2(iy)} = \overline{g_2(\tau)}$$

and similarly,

$$g_3(\tau) = g_3(iy) = g_3([1, iy]) = g_3(\overline{[1, iy]}) = \overline{g_3([1, iy])} = \overline{g_3(iy)} = \overline{g_3(\tau)}.$$

Thus $g_2(\tau)$ and $g_3(\tau)$, and hence $\Delta(\tau)$, are real-valued for purely imaginary $\tau = iy$.

□

Since $\Delta(\tau)$ is real-valued when $\tau \in \mathbb{H}$ is purely imaginary by the previous lemma, and since cube roots of real numbers are uniquely defined within the real numbers, we may fix a holomorphic branch of $\sqrt[3]{\Delta(\tau)}$ on $\mathbb{H}$ by requiring it to agree with the real cube root along the imaginary axis. This choice determines a unique holomorphic cube rootof $\Delta(\tau)$ on all of $\mathbb{H}$.

Moreover, since $g_2(\tau)$ is also real for purely imaginary τ (Lemma 6.1.2), it follows that the function

$$\gamma_2(\tau) \coloneqq 12\frac{g_2(\tau)}{\sqrt[3]{\Delta(\tau)}}$$

is real-valued on the imaginary axis. Since both the numerator and the denominator are holomorphic on $\mathbb{H}$, and the denominator never vanishes (Theorem 2.3.22), $\gamma_2(\tau)$ defines a holomorphic function on $\mathbb{H}$ that coincides with the real cube root of $j(\tau)$ for purely imaginary τ. This ensures that the function is well-defined.

We are now ready to study the transformation properties of $\gamma_2(\tau)$ under the action of $\mathrm{SL}_2(\mathbb{Z})$, which will allow us to establish its modularity.

Lemma 6.1.4. *Let $F(q) = 1 + \sum_{n=1}^{\infty} a_n q^n$ be a power series converging in a neighbourhood of $0 \in \mathbb{C}$. Then:*

(*i*) *For any positive integer m, there exists a unique power series $G(q)$, converging in a possibly smaller neighbourhood of 0, such that $F(q) = G(q)^m$ and $G(0) = 1$.*

(*ii*) *If, in addition, the coefficients of $F(q)$ are rational, then the series $G(q)$ from part (i) also has rational coefficients.*

Proof. (*i*): Let $F(q) = 1 + \sum_{n=1}^{\infty} a_n q^n$ be a power series converging in a neighbourhood of the origin. Define the function $H(z) = \sqrt[m]{z}$ in a small neighbourhood U of $1 \in \mathbb{C}$ such that $H(1) = 1$. Then H is holomorphic on U and satisfies $H(z)^m = z$ for all $z \in U$. Since F is analytic and hence holomorphic with $F(0) = 1$, and power series are continuous inside their radius of convergence, $F(q)$ is continuous at $0 \in \mathbb{C}$, so there exists a neighbourhood V of 0 such that $F(V) \subseteq U$. Then the composition $G = H \circ F$ is holomorphic on V, since the composition of holomorphic functions is holomorphic. Moreover, for $q \in V$ we have $G(q)^m = (H(F(q)))^m = F(q)$ and $G(0) = H(F(0)) = 1$.
(*ii*): By part (*i*), G is holomorphic and hence analytic, so it can be written as a power series $G(q) = 1 + \sum_{n=1}^{\infty} b_n q^n$ with $b_n \in \mathbb{C}$. The equation $G(q)^m = F(q)$ implies $(1 + \sum_{n=1}^{\infty} b_n q^n)^m = 1 + \sum_{n=1}^{\infty} a_n q^n$. We now compare the coefficients of q^n on both sides. Expanding the left hand side using the Binomial theorem gives

$$\left(1 + \sum_{n=1}^{\infty} b_n q^n\right)^m = \sum_{k=0}^{m} \binom{m}{k} \left(\sum_{n=1}^{\infty} b_n q^n\right)^k = 1 + \sum_{k=1}^{m} \binom{m}{k} \left(\sum_{n=1}^{\infty} b_n q^n\right)^k,$$

meaning that q^n appears in the expansion whenever we select terms of the form $b_{n_1} b_{n_2} \cdots b_{n_k} q^{n_1+n_2+\ldots+n_k}$ whose indices add up to n. In particular, the only way b_n appears in the sum is when $n_i = n$ for some $1 \leq i \leq k$ and $n_j = 0$ for all $j \neq i$. Since there are exactly k choices for which index i takes the value n, we obtain

$$a_n = k b_n + \sum_{\substack{1 \leq n_1, \ldots, n_k < n \\ n_1 + \ldots + n_k = n}} b_{n_1} \cdots b_{n_k}.$$

In particular, $a_1 = k b_1$, so b_1 is rational because a_1 is rational by assumption. Then, by complete induction on n, it follows that all b_n are rational. □

Proposition 6.1.5. *For $\tau \in \mathbb{H}$, the following relations hold*

$$\gamma_2\left(-\frac{1}{\tau}\right) = \gamma_2(\tau)$$
$$\gamma_2(\tau+1) = \zeta_3^{-1}\gamma_2(\tau),$$

where $\zeta_3^{-1} = e^{\frac{2\pi i}{3}}$ is a primitive third root of unity.

Proof. For the first relation, note that $-\frac{1}{\tau}$ lies on the imaginary axis whenever τ does. Hence, $\gamma_2(-\frac{1}{\tau})$ is real whenever $\gamma_2(\tau)$ is. Therefore, $\gamma_2(-\frac{1}{\tau})$ is the cube root of $j(-\frac{1}{\tau}) = j(\tau)$ (Theorem 2.5.9) for purely imaginary $\tau \in \mathbb{H}$.
For the second relation, note that replacing τ by $\tau+1$ does not affect $j(\tau)$ by Theorem 2.5.9, but $\tau+1$ is not purely imaginary anymore. We instead use the q-expansion of $j(\tau)$ by Corollary 4.2.2:

$$j(\tau) = q^{-1} + \sum_{n=0}^{\infty} a_n q^n = q^{-1}\left(1 + \sum_{n=0}^{\infty} a_n q^{n+1}\right) = q^{-1}\left(1 + \sum_{n=1}^{\infty} a_n q^n\right) =: q^{-1}h(q),$$

where the geometric series $h(q)$ converges for $|q| < 1$ and so is analytic, and hence holomorphic. Moreover, $h(0) = 1$. By part (i) of Lemma 6.1.4, there exists a holomorphic function $u(q)$ with $u(0) = 1$ such that $h(q) = u(q)^3$. Since the coefficients of $j(\tau)$ are rational as they are obtained by a polynomial division of two polynomials with integer coefficients, as shown in the proof of Corollary 4.2.2, the coefficients of $h(q)$ are rational as well, and by part (ii) of Lemma 6.1.4, the coefficients of $u(q)$ are also rational. Now, for $\tau = iy$ with $y > 0$, we have

$$q^{-\frac{1}{3}}u(q) = e^{-\frac{2\pi i^2 y}{3}}\left(1 + \sum_{n=1}^{\infty} b_n e^{2\pi i^2 y}\right) = e^{\frac{2\pi y}{3}}\left(1 + \sum_{n=1}^{\infty} \underbrace{b_n}_{\in\mathbb{Q}} e^{-2\pi y}\right) \in \mathbb{R}, \tag{6.1}$$

and since $(q^{-\frac{1}{3}}u(q))^3 = j(\tau)$ by construction, it follows that $q^{-\frac{1}{3}}u(q)$ is the real-valued cube root of $j(\tau)$ when $\tau \in \mathbb{H}$ is purely imaginary. Finally, using Euler's identity, we conclude

$$\begin{aligned}
\gamma_2(\tau+1) &= e^{-\frac{1}{3}2\pi i(\tau+1)}u(q)\left(1 + \sum_{n=1}^{\infty} b_n e^{2\pi i n(\tau+1)}\right) \\
&= e^{-\frac{2\pi i}{3}}e^{-\frac{2\pi i\tau}{3}}u(q)\left(1 + \sum_{n=1}^{\infty} b_n e^{2\pi i\tau n}e^{2\pi i n}\right) \\
&= \zeta_3^{-1}q^{-\frac{1}{3}}u(q)\left(1 + \sum_{n=1}^{\infty} b_n q^n\right) \\
&= \zeta_3^{-1}\gamma_2(\tau).
\end{aligned}$$

where $\zeta_3 = e^{2\pi i/3}$ is a primitive third root of unity. □

Proposition 6.1.6. *For $\tau \in \mathbb{H}$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, the following relation holds*

$$\gamma_2(\gamma\tau) = \gamma_2\left(\frac{a\tau+b}{c\tau+d}\right) = \zeta_3^{ac-ab+a^2cd-cd}\gamma_2(\tau).$$

Proof. Since $\mathrm{SL}_2(\mathbb{Z})$ is generated by the matrices $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, we can prove the relation by induction on the length of $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ as a word in S and T.
For the induction base, note that the identity holds for the generators S and T by the relations from Proposition 6.1.5. Indeed, we have

$$\gamma_2(S\tau) = \gamma_2\left(\frac{-1}{\tau}\right) = \gamma_2(\tau) = \zeta_3^0\gamma_2(\tau)$$
$$\gamma_2(T\tau) = \gamma_2(\tau+1) = \zeta_3^{-1}\gamma_2(\tau).$$

Next, we show that the relation holds for S^{-1} and T^{-1}. The linear fractional transformation $\tau \mapsto \frac{a\tau+b}{c\tau+d} = \gamma\tau$ is injective with respect to τ but not necessarily with respect to $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, i.e. $\gamma\tau = \gamma\tau'$ so $\tau = \tau'$ but not necessarily $\gamma = \gamma'$ if $\gamma\tau = \gamma'\tau$, it could happen that $\gamma \neq \gamma'$ when $\gamma_2(\gamma\tau) = \gamma_2(\gamma'\tau)$. Consequently, it may happen that $\gamma_2(\gamma\tau) = \gamma_2(\gamma'\tau)$ for $\gamma \neq \gamma'$, so we must keep track of the exponent $\rho(\gamma) = ac - ab + a^2cd - cd$ of ζ_3 whenever two different matrices yield the same $\gamma\tau$.
Since $S^{-1} = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, we have $S\tau = -\frac{1}{\tau} = S^{-1}\tau$, so $\gamma_2(S^{-1}\tau) = \gamma_2(S\tau) = \gamma_2(\tau)$ by above. As $\rho(S) = 0 = \rho(S^{-1})$, the relation holds for S^{-1}. Since $T^{-1} = \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$, we have $T\tau = \tau + 1 \neq \tau - 1 = T^{-1}\tau$. By above we have $\gamma_2(\tau) = \gamma_2(T^{-1}T\tau) = \zeta_3^{-1}\gamma_2(T^{-1}\tau)$, so $\gamma_2(T^{-1}\tau) = \zeta_3\gamma_2(\tau)$ and the relation holds also for T^{-1}.
For the induction step, we first need to prove the following claim:

$$\gamma \in \mathrm{SL}_2(\mathbb{Z}),\ \delta \in \{S^{\pm 1}, T^{\pm 1}\} \implies \rho(\delta) + \rho(\gamma) \equiv \rho(\delta\gamma) \bmod 3. \qquad (*)$$

Fix $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, and treat the four cases separately:

(*I*) For $\delta = S$, we have $\rho(S) = 0$ and so we show that $\rho(\gamma) - \rho(S\gamma) \equiv 0 \bmod 3$. We have $S\gamma = \left(\begin{smallmatrix} -c & -d \\ a & b \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $\rho(S\gamma) = -ac - cd + c^2ab - ab$. With $\rho(\gamma) = ac - ab + a^2cd - cd$ and $ad - bc = 1$, it follows that

$$\rho(\gamma) - \rho(S\gamma) = 2ac + ac(ad - bc) = 3ac \equiv 0 \bmod 3.$$

(*II*) Let $\delta = S^{-1}$. Using case (*I*) with $\delta = S$ and $\gamma = S^{-1}\gamma$ in the last step, together with associativity of multiplication of matrices in $\mathrm{SL}_2(\mathbb{Z})$, we get

$$\rho(\gamma) = \rho((SS^{-1})\gamma) = \rho(S(S^{-1}\gamma)) \equiv \rho(S) + \rho(S^{-1}\gamma) \bmod 3.$$

Thus, $\rho(S^{-1}\gamma) \equiv -\rho(S) + \rho(\gamma) \bmod 3$, and since $\rho(S) = \rho(S^{-1}) = 0$, we have $\rho(S^{-1}\gamma) \equiv \rho(S^{-1}) + \rho(\gamma) \bmod 3$.

(III) For $\delta = T$, we have $\rho(T) = -1$ and so we show that $\rho(T\gamma) \equiv \rho(\gamma) - 1 \bmod 3$. We have $T\gamma = \left(\begin{smallmatrix} a+c & b+d \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and using $ad - bc = 1$ in the third step, we obtain

$$\begin{aligned}
\rho(T\gamma) &= (a+c)c - (a+c)(b+d) + (a+c)^2cd - cd \\
&= \rho(\gamma) + c^2 - ad - bc - cd + 2ac^2d + c^3d \\
&= p(\gamma) + c^2 - (1+bc) - bc - cd + 2c^2(1+bc) + c^3d \\
&= p(\gamma) - 1 + c(3c - 2b - d + 2bc^2 + c^2d) \\
&\equiv p(\gamma) - 1 + c(-2b - d + 2bc^2 + c^2d) \bmod 3 \\
&= p(\gamma) - 1 + c(c+1)(c-1)(2b+d) \bmod 3 \\
&= p(\gamma) - 1 \bmod 3,
\end{aligned}$$

where the last equality holds since one of $c, c-1$ and $c-2$ is divisible by 3.

(IV) Let $\delta = T^{-1}$. Note that $-\rho(T) = -(-1) = 1 = \rho(T^{-1})$ and by using case (III) with $\gamma = T^{-1}\gamma$ together with with associativity of multiplication of matrices in $\mathrm{SL}_2(\mathbb{Z})$, gives the desired relation with the same argument as in case (II).

For the induction step, we assume that the identity holds for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and show that it holds for $\delta\gamma$, where $\delta \in \{S^{\pm 1}, T^{\pm 1}\}$. This is now easy:

$$\begin{aligned}
\gamma_2((\delta\gamma)\tau) = \gamma_2(\delta(\gamma\tau)) &\overset{\text{(IB)}}{=} \zeta_3^{\rho(\delta)}\gamma_2(\gamma\tau) \overset{\text{(IH)}}{=} \zeta_3^{\rho(\delta)}\zeta_3^{\rho(\gamma)}\gamma_2(\tau) \\
&= \zeta_3^{\rho(\delta)+\rho(\gamma)}\gamma_2(\tau) \overset{(*)}{=} \zeta_3^{\rho(\delta\gamma)}\gamma_2(\tau),
\end{aligned}$$

where the first line uses the associativity of the linear fractional transformation, the induction base (IB) and hypothesis (IH) and the second line uses the claim $(*)$. Hence, the relation holds for $\delta\gamma$, completing the induction. □

With the transformation behaviour of $\gamma_2(\tau)$ under $\mathrm{SL}_2(\mathbb{Z})$ established, we can now deduce the modularity of its scaled version:

Theorem 6.1.7. *$\gamma_2(3\tau)$ is a modular function for the congruence subgroup $\Gamma_0(9)$.*

Proof. Consider the congruence subgroup

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; b \equiv c \equiv 0 \bmod 3 \right\}.$$

First, by Proposition 6.1.6 the function $\gamma_2(\tau)$ is G-invariant. Indeed, for any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$ and $\tau \in \mathbb{H}$, we have $b \equiv c \equiv 0 \bmod 3$, which implies $\rho(\gamma) = ac - ab + a^2cd - cd \equiv 0 \bmod 3$. Hence $\zeta_3^{\rho(\gamma)} = 1$ and said proposition gives $\gamma_2(\gamma\tau) = \gamma_2(\tau)$.
Next, the group G is related to the congruence subgroup

$$\Gamma_0(9) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \bmod 9 \right\},$$

via the identity

$$\Gamma_0(9) = \begin{pmatrix} \frac{1}{3} & 0 \\ 0 & 1 \end{pmatrix} G \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}.$$

Indeed, for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$, we compute

$$\begin{pmatrix} \frac{1}{3} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & \frac{b}{3} \\ 3c & d \end{pmatrix}$$

Since $b \equiv c \equiv 0 \bmod 3$, b is an integer and $3c \equiv 0 \bmod 9$. Moreover, the determinant is 1, so the matrix lies in $\Gamma_0(9)$. Conversely, for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(9)$, we have

$$\begin{pmatrix} \frac{1}{3} & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \frac{1}{3} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 3b \\ \frac{c}{3} & d \end{pmatrix}$$

As $c \equiv 0 \bmod 9$, we have $c \equiv 0 \bmod 3$. Also $3b \equiv 0 \bmod 3$ and since again the determinant is 1, the matrix lies in G. Thus the above identity holds, connecting the congruence groups G and $\Gamma_0(9)$.
Now, we show that $\gamma_2(3\tau)$ is invariant under $\Gamma_0(9)$. Let $\gamma \in \Gamma_0(9)$ and by writing $\gamma = \left(\begin{smallmatrix} \frac{1}{3} & 0 \\ 0 & 1 \end{smallmatrix}\right)\bar{\gamma}\left(\begin{smallmatrix} 3 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ with $\bar{\gamma} \in G$ by the above identity gives $\left(\begin{smallmatrix} 3 & 0 \\ 0 & 1 \end{smallmatrix}\right)\gamma = \bar{\gamma}\left(\begin{smallmatrix} 3 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. By the fractional linear transformation with $\tau \in \mathbb{H}$ we have

$$3\gamma\tau = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \gamma\tau = \bar{\gamma} \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \tau = \bar{\gamma} 3\tau,$$

where we may view 3 as the matrix $\left(\begin{smallmatrix} 3 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, since $3\tau = \frac{3\tau+0}{0\tau+1}$. It follows that

$$\gamma_2(3\gamma\tau) = \gamma_2(\bar{\gamma}3\tau) = \gamma_2(3\tau),$$

where the last equality holds since $\gamma_2(\tau)$ is G-invariant by above. Thus $\gamma_2(3\tau)$ is invariant under $\Gamma_0(9)$. As $\gamma_2(\tau)$ is holomorphic on $\mathbb{H}$ and hence meromorphic on $\mathbb{H}$, it remains to check that $\gamma_2(3\tau)$ is meromorphic at the cusps.
Let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. By Theorem 4.3.1 $j(3\tau)$ is a modular function for $\Gamma_0(3)$, so it is meromorphic at the cusps, i.e. $j(3\gamma\tau)$ has a meromorphic expansion of the form

$$j(3\gamma\tau) = \sum_{n=n_0}^{\infty} a_n q^{\frac{n}{3}},$$

with $a_{n_0} \neq 0$ for some $n_0 \in \mathbb{N}$. Taking cube roots then gives a meromorphic expansion for $\gamma_2(3\gamma\tau)$ of the form

$$\gamma_2(3\gamma\tau) = \sum_{n=n_0}^{\infty} b_n q^{\frac{n}{9}},$$

with $b_{n_0} \neq 0$ for some $n_0 \in \mathbb{N}$, so $\gamma_2(3\tau)$ is meromorphic at the cusps, completing the proof that $\gamma_2(3\tau)$ is indeed a modular function for $\Gamma_0(9)$. □

Remark 6.1.8. *Note that G is not the largest subgroup of $\mathrm{SL}_2(\mathbb{Z})$ fixing $\gamma_2(\tau)$, but it is the one that relates the most directly to the congruence subgroups $\Gamma_0(N)$. One can show that the largest such subgroup fixing $\gamma_2(\tau)$ is actually the following:*

$$\mathcal{S} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; a \equiv d \equiv 0 \bmod 3 \text{ or } b \equiv c \bmod 3 \right\}.$$

6.2 Algebraic integrality of γ_2 and the construction of ring class fields

With the modularity of γ_2 established, we are now ready to investigate its arithmetic properties. In particular, we focus on the algebraic integrality of its values and on how they can be used to explicitly construct the ring class fields associated with imaginary quadratic orders.

Ensuring that $\gamma_2(\tau)$ faithfully reflects the arithmetic of an order $\mathcal{O}$ in an imaginary quadratic number field requires a careful choice of the representative $\tau \in \mathbb{H}$ for the lattice defining $\mathcal{O}$. While replacing τ by $\tau + 1$ does not affect $j(\tau)$, it does change the value of $\gamma_2(\tau)$ (see Proposition 6.1.5); selecting the appropriate τ guarantees that the value correctly encodes the structure of the lattice and the order.

To describe the appropriate choice of τ, recall that any imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$, with $d < 0$, has an integral basis given by $\{1, \omega_K\}$, where

$$\omega_K = \begin{cases} \sqrt{d} & \text{if } d \not\equiv 1 \bmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

The discriminant d_K of K is defined in terms of this basis as

$$d_K = \begin{cases} 4d & \text{if } d \not\equiv 1 \bmod 4 \\ d & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

Accordingly, the maximal order is $\mathcal{O}_K = [1, \omega_K]$ and any suborder $\mathcal{O} \subseteq \mathcal{O}_K$ of conductor $f \geq 1$ has the form $\mathcal{O} = [1, \omega]$ with $\omega = f\omega_K$ (cf. Remark 3.3.2). Its discriminant D is then $D = f^2 d_K$, as stated in Theorem 3.3.3, and satisfies $D \equiv 0$ or $1 \bmod 4$.

Associating $\mathcal{O}$ with a complex number $\tau \in \mathbb{H}$ such that $\mathcal{O} = [1, \tau]$, suggests taking $\tau = \omega$. However, since the modular function γ_2 is not invariant under the transformation $\tau \mapsto \tau + 1$, which corresponds to the matrix $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, the chosen τ might lie outside the appropriate domain for the modular subgroup relevant for γ_2. Thus, to ensure that $\gamma_2(\tau)$ is evaluated correctly, we must ensure that τ lies a fundamental domain for $\mathbb{H}/\mathcal{S}$, where $\mathcal{S}$ is the maximal subgroup of $\mathrm{SL}_2(\mathbb{Z})$ fixing γ_2 seen in Remark 6.1.8. In the case $d \not\equiv 1 \bmod 4$, the value $\omega = f\sqrt{d}$ already lies in the appropriate domain, so we may safely take $\tau = \omega$. In contrast, when $d \equiv 1 \bmod 4$, the expression $\omega = f\frac{1+\sqrt{d}}{2}$ typically lies outside the above domain. Although ω still defines the correct lattice,

evaluating γ_2 at this point may yield an incorrect value. To avoid this, we instead take the $\mathrm{SL}_2(\mathbb{Z})$-equivalent representative

$$\tau = \omega + 1,$$

which lies in the appropriate domain and satisfies $j(\tau) = j(\omega)$ by Lemma 2.5.10.
By Theorem 2.5.5 it follows that the lattices $[1, \tau]$ and $[1, \omega]$ are homothetic and hence define the same order $\mathcal{O}$ by Corollary 3.5.4. Thus, this normalization preserves both the algebraic structure of $\mathcal{O}$ and the transformation behaviour of γ_2, ensuring the correct value for the associated class field.

We are now ready to state the theorem.

Theorem 6.2.1. *Let $\mathcal{O}$ be an order in an imaginary quadratic number field K of discriminant D not divisible by 3, and write $\mathcal{O} = [1, \tau_0]$, where*

$$\tau_0 = \begin{cases} \sqrt{d} & \text{if } D = 4d \equiv 0 \bmod 4 \\ \frac{3+\sqrt{d}}{2} & \text{if } D = d \equiv 1 \bmod 4. \end{cases}$$

Then $\gamma_2(\tau_0)$ is an algebraic integer, and $K(\gamma_2(\tau_0))$ is the ring class field of $\mathcal{O}$. Moreover, $\mathbb{Q}(\gamma_2(\tau_0)) = \mathbb{Q}(j(\tau_0))$.

Proof. Let $\mathcal{O} = [1, \tau_0]$ be an order in an imaginary quadratic number field K of discriminant D not divisible by 3. Since every order in K can be viewed as a lattice in $\mathbb{C}$ (see Remark 3.3.2), Corollary 3.5.4 implies that the elliptic curve E corresponding to the lattice $L = [1, \tau_0]$ has complex multiplication by $\mathcal{O}$, as L is homothetic to itself and every order $\mathcal{O}$ is, by definition, a proper $\mathcal{O}$-ideal. Then Theorem 5.3.8 implies that $j(E) = j(\tau_0)$ is an algebraic integer. As $\gamma_2(\tau_0)^3 = j(\tau_0)$, it follows that $\gamma_2(\tau_0)$ satisfies the monic polynomial $x^3 - j(\tau_0) = 0$, whose coefficients are algebraic integers. Therefore, $\gamma_2(\tau_0)$ is an algebraic integer as well.
Since E is an elliptic curve with complex multiplication by $\mathcal{O}$, Corollary 5.6.3 shows that $K(j(\tau_0))$ is the ring class field of $\mathcal{O}$. As $\gamma_2(\tau_0)$ is the real cube root of $j(\tau_0)$, we have

$$K(j(\tau_0)) = K(\gamma_2(\tau_0))$$

and therefore, $K(\gamma_2(\tau_0))$ is also the ring class field of $\mathcal{O}$.
It remains to prove $\mathbb{Q}(\gamma_2(\tau_0)) = \mathbb{Q}(j(\tau_0))$. By equation (6.1) in the proof of Proposition 6.1.5, we know that the q-expansion of $\gamma_2(3\tau)$ has rational coefficients. Moreover, since $\gamma_2(3\tau)$ is a modular function for $\Gamma_0(9)$ by Theorem 6.1.7, we can apply Theorem 4.5.2 (i), which implies that

$$\gamma_2(3\tau) \in \mathbb{Q}(j(\tau), j(9\tau)).$$

As we are interested in $\gamma_2(\tau_0)$, we need to evaluate this expression at $\tau = \frac{\tau_0}{3}$.
Since $\gamma_2(3\tau)$ is holomorphic by definition, and Lemma 4.5.3 ensures that

$$\frac{\partial \Phi_9}{\partial Y}\left(j\left(\frac{\tau_0}{3}\right), j\left(3\tau_0\right)\right) \neq 0$$

for $N = 9, s = 3$ and $\tau = \tau_0$, we may apply Theorem 4.5.2 (ii) to conclude that $\gamma_2(\tau_0) \in \mathbb{Q}(j(\frac{\tau_0}{3}), j(3\tau_0))$, which we can rewrite as

$$\gamma_2(\tau_0) \in \mathbb{Q}\left(j\left(\left[1, \frac{\tau_0}{3}\right]\right), j([1, 3\tau_0])\right), \tag{6.2}$$

by definition of the j-function. Now set $\mathcal{O} = [1, \tau_0]$. Then $\mathcal{O}' = [1, 3\tau_0]$ is an order of $\mathcal{O}$ of index 3 by Lemma 5.3.2. Then by the same argument as above, Corollary 3.5.4 implies that the elliptic curve corresponding to the lattice $[1, 3\tau_0]$ has complex multiplication by $\mathcal{O}'$. Now we claim that $[1, \frac{\tau_0}{3}]$ is a proper $\mathcal{O}'$-ideal, so that the elliptic curve corresponding to the lattice $[1, \frac{\tau_0}{3}]$ also has complex multiplication by $\mathcal{O}'$ by the same corollary.
Indeed, note that the assumption $3 \nmid D$ implies $3 \nmid d$. If on one hand $D \equiv 0 \bmod 4$, then $\tau_0 = \sqrt{d}$ and the minimal polynomial of $\frac{\tau_0}{3}$ is $9x^2 - d$. Since $3 \nmid d$, this polynomial has relatively prime integer coefficients, thus Remark 3.5.6 shows that $[1, \frac{\tau_0}{3}]$ is a proper $[1, 9\frac{\tau_0}{3}] = [1, 3\tau_0]$-ideal. If on the other hand $D \equiv 1 \bmod 4$, then $\tau_0 = \frac{3+\sqrt{d}}{2}$, and $\frac{\tau_0}{3}$ is a root of the polynomial $36x^2 - 36x + 9 - d$. Since we have $d \equiv 1 \bmod 4$, $d - 9$ is a multiple of 4, so that $9x^2 - 9x + \frac{d-9}{4}$ has integer coefficients and still has $\frac{\tau_0}{3}$ as a root. Since $3 \nmid d$, the coefficients are relatively prime and so by Remark 3.5.6, $[1, \frac{\tau_0}{3}]$ is again a proper $([1, 9\frac{\tau_0}{3}] = [1, 3\tau_0])$-ideal, which proves our claim.
It follows by Corollary 5.6.3, that both $j(\frac{\tau_0}{3})$ and $j(3\tau_0)$ generate the ring class field L' of the order $\mathcal{O}'$. Thus (6.2) implies that $\gamma_2(\tau_0)$ lies in L'.
Now let L denote the ring class field of $\mathcal{O}$. Then we have $L \subseteq L'$ as seen in Section 5.6. Let f be the conductor of $\mathcal{O}$. Since $\mathcal{O}$ is an order of discriminant D by assumption, then D is of the form $D = f^2 d_K$ by Theorem 3.3.3, where $f \geq 1$ is an integer. As $\mathcal{O}'$ is an order of index 3 in $\mathcal{O}$, it follows that the order $\mathcal{O}'$ has conductor $f' = [\mathcal{O}_K : \mathcal{O}'] = [\mathcal{O}_K : \mathcal{O}] \cdot [\mathcal{O} : \mathcal{O}'] = 3f$ and discriminant

$$D' = (f')^2 d_K = 3^2 f^2 d_K = 9D.$$

Then, by the degree formula for field extensions and the isomorphism $\mathrm{Gal}(L/K) \cong C(\mathcal{O})$ by the First main theorem of complex multiplication 5.5.2, we have

$$[L' : L] = \frac{[L' : K]}{[L : K]} = \frac{|\mathrm{Gal}(L'/K)|}{|\mathrm{Gal}(L/K)|} = \frac{|C(\mathcal{O}')|}{|C(\mathcal{O})|} = \frac{h(\mathcal{O}')}{h(\mathcal{O})} = \frac{h(9D)}{h(D)}.$$

Then, by Proposition 5.7.2, we get

$$\begin{aligned} \frac{h(9D)}{h(D)} &= \frac{3}{[\mathcal{O}^* : \mathcal{O}'^*]}\left(1 - \left(\frac{D}{3}\right)\frac{1}{3}\right) \\ &= \frac{3}{[\mathcal{O}^* : \mathcal{O}'^*]}\left(1 \pm \frac{1}{3}\right) \\ &= \frac{3 \pm 1}{[\mathcal{O}^* : \mathcal{O}'^*]}, \end{aligned}$$

where we used the assumption $3 \nmid D$ and hence $(\frac{D}{3}) \in \{\pm 1\}$ by the Legendre-Kronecker symbol. We simplify this expression by considering the three possible cases for the

group of units $\mathcal{O}_K$ of the maximal order, given by Proposition 5.7.3. Since $3 \nmid D$ we have $D \neq -3$, so we only need to consider the cases $\mathcal{O}_K^* = \{\pm 1\}$ and $\mathcal{O}_K^* = \{\pm 1, \pm i\}$.
In the first case we clearly have $\mathcal{O}^* = \mathcal{O}'^* = \{\pm 1\}$ and so $[\mathcal{O}^* : \mathcal{O}'^*] = 1$. In the second case we have $\mathcal{O}^* = \{\pm 1\}$ or $\mathcal{O}^* = \{\pm 1, \pm i\}$, since $\mathcal{O} \subseteq \mathcal{O}_K$ and the smallest order containing i is the maximal order $\mathcal{O}_K$. As $\mathcal{O}'$ is a proper suborder of $\mathcal{O}$ (namely of index 3), we get $\mathcal{O}'^* = \{\pm 1\}$ in both subcases, and therefore the index is either 1 or 2.
Note that the case where both the numerator and denominator are 2 cannot occur, as this would imply $(\frac{D}{3}) = -1$ and the class number formula would give $\frac{h(9D)}{h(D)} = 2$, which contradicts $\frac{2}{2} = 1$. Therefore we get

$$\frac{h(9D)}{h(D)} = \frac{3 \pm 1}{[\mathcal{O}^* : \mathcal{O}'^*]} = 3 \pm 1.$$

It follows that L' is an extension of degree 2 or 4 over L.
As L is the ring class field of $\mathcal{O} = [1, \tau_0]$, and the ring class field is the field extension of $\mathbb{Q}(\sqrt{D})$ generated by the j-invariant of any elliptic curve with complex multiplication by $\mathcal{O}$, we have

$$L = K(j(\tau_0)) = \mathbb{Q}(\sqrt{D}, j(\tau_0)).$$

Since $\mathbb{Q}(\sqrt{D})$ is a quadratic extension of $\mathbb{Q}$, and $j(\tau_0)$ is real while $\sqrt{D}$ is imaginary, and hence $\sqrt{D} \notin \mathbb{Q}(j(\tau_0))$, it follows that L is an extension of degree 2 over $\mathbb{Q}(j(\tau_0))$.
So we have the following tower of field extensions:

$$\begin{array}{ccc} \mathbb{Q}(\gamma_2(\tau_0)) & \subseteq & L' \\ \cup| & & \cup| \\ \mathbb{Q}(j(\tau_0)) & \subseteq & L. \end{array}$$

Then

$$[L' : \mathbb{Q}(j(\tau_0))] = [L' : L] \cdot [L : \mathbb{Q}(j(\tau_0))] = (2 \text{ or } 4) \cdot 2 = 4 \text{ or } 8.$$

We deduce that $\mathbb{Q}(\gamma_2(\tau_0))$ has to be an extension of degree at most 8 over $\mathbb{Q}(j(\tau_0))$. But since we know that $\gamma_2(\tau_0)$ is the real cube root of $j(\tau_0)$, the extension of $\mathbb{Q}(\gamma_2(\tau_0))$ over $\mathbb{Q}(j(\tau_0))$ has degree 1 or 3. Hence its degree has to be 1, since the degree of the field extension $\mathbb{Q}(\gamma_2(\tau_0))/\mathbb{Q}(j(\tau_0))$ has to divide the degree of the extension $L'/\mathbb{Q}(j(\tau_0))$. This proves $\mathbb{Q}(\gamma_2(\tau_0)) = \mathbb{Q}(j(\tau_0))$. □

Note that we restricted to orders whose discriminant D is not divisible by 3 to guarantee that $\gamma_2(\tau)$ is an algebraic integer. This condition avoids complications arising from the cube root in the definition of γ_2 and ensures that the value $\gamma_2(\tau)$ generates the corresponding ring class field. For completeness, we record the case where the discriminant is divisible by 3.

Theorem 6.2.2. *Let $\mathcal{O}$ be an order in an imaginary quadratic number field K of discriminant D divisible by 3, and write $\mathcal{O} = [1, \tau_0]$, where*

$$\tau_0 = \begin{cases} \sqrt{d} & \text{if } D = 4d \equiv 0 \bmod 4 \\ \frac{3+\sqrt{d}}{2} & \text{if } D = d \equiv 1 \bmod 4. \end{cases}$$

Then $K(\gamma_2(\tau_0))$ is the ring class field of $\mathcal{O}' = [1, 3\tau_0]$ and is an extension of degree 3 of the ring class field of $\mathcal{O}$. Moreover, $\mathbb{Q}(\gamma_2(\tau_0)) = \mathbb{Q}(j(3\tau_0))$.

Proof. For a proof see [3, Thm. 12.13]. □

Remark 6.2.3. *Besides the cube root $\gamma_2(\tau)$ of $j(\tau)$, there is also an interesting square root to consider. Since $\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)$, it follows that*

$$j(\tau) - 1728 = 1728\left(\frac{g_2(\tau)^3}{\Delta(\tau)} - 1\right) = 6^6\frac{g_3(\tau)}{\Delta(\tau)}$$

and hence we can define

$$\gamma_3(\tau) = \sqrt{j(\tau) - 1728} = 216\frac{g_3(\tau)}{\sqrt{\Delta(\tau)}}.$$

Similar to Theorems 6.2.1 and 6.2.2, one can choose τ_0 such that $\gamma_3(\tau_0)$ generates a field closely related to the ring class field of $\mathcal{O} = [1, \tau_0]$. For more details, see [11, Thm. 3].

The integrality of $\gamma_2(\tau_0)$ leads to an interesting arithmetic property of the j-invariant. We have seen in Corollary 5.6.4 that for an elliptic curve E with complex multiplication by an order $\mathcal{O}$ of class number one, the associated j-invariant $j(E) = j(\tau_0)$ is an integer. By definition, we have $\gamma_2(\tau_0)^3 = j(\tau_0)$, and Theorem 6.2.1 shows that $\gamma_2(\tau_0) \in \mathbb{Z}$ whenever $3 \nmid D$. Hence, $j(E)$ is a perfect cube in $\mathbb{Z}$, i.e. the cube of an integer, which not only explains the following result, but also provides a crucial ingredient for our ultimate goal of explaining the near-integer phenomenon of $e^{\pi\sqrt{163}}$:

Corollary 6.2.4. *Let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by an order $\mathcal{O}$ of discriminant D and class number one in an imaginary quadratic number field. If $3 \nmid D$, then $j(E)$ is a perfect cube.*

7 Algebraic construction of γ_2

In order to conclude the ultimate goal of this work, we need to prove the remaining part of Corollary 4.2.2: the coefficients a_n in the j-function's q-expansion

$$j(\tau) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} a_n q^n$$

are integers. While the expansion itself has already been established, this chapter is devoted to that last missing piece. By constructing γ_2 algebraically and linking it to the arithmetic of j, we obtain the integrality result and close the final gap in the argument. The chapter is divided into three sections. The first two focus on introducing the necessary analytic functions: we begin with the Weber functions, whose q-expansions encode modular information in a form suitable for algebraic manipulation, and then consider the Weierstrass σ-function, which, through its relation to the Weierstrass $\wp$-function, links the geometry of lattices to these modular quantities. The third section combines these tools in the algebraic computation of γ_2, thereby completing the connection between analytic constructions and arithmetic properties and establishing the integrality of the j-function coefficients.

The exposition in this chapter is based on [3, §12 B], and has been expanded with explanations and proofs for material not detailed in the original exposition.

7.1 The Weber functions

We start with the Dedekind η-function and the Weber functions, focusing on their q-product expansions, which will serve as the basis for the subsequent algebraic computation of γ_2.

Definition 7.1.1 (Dedekind η-function)**.** Let $\tau \in \mathbb{H}$ and $q = e^{2\pi i \tau}$. The Dedekind η-function is defined by

$$\eta(\tau) \coloneqq q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n).$$

Since $\tau \in \mathbb{H}$, we have $0 < |q| < 1$, which ensures that the infinite product defining $\eta(\tau)$ converges absolutely and defines a non-vanishing holomorphic function on $\mathbb{H}$.

Definition 7.1.2 (Weber functions)**.** Let $\tau \in \mathbb{H}$. The Weber functions are defined by

$$\begin{aligned}
\mathfrak{f}(\tau) &\coloneqq \zeta_{48}^{-1}\ \frac{\eta(\frac{\tau+1}{2})}{\eta(\tau)},\\
\mathfrak{f}_1(\tau) &\coloneqq \frac{\eta(\frac{\tau}{2})}{\eta(\tau)},\\
\mathfrak{f}_2(\tau) &\coloneqq \sqrt{2}\ \frac{\eta(2\tau)}{\eta(\tau)},
\end{aligned}$$

where $\zeta_{48} = e^{\frac{2\pi i}{48}} = e^{\frac{\pi i}{24}}$ denotes a primitive 48th root of unity.

Note that the Dedekind η-function and the Weber functions are modular functions for certain congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$, but for the full group they satisfy only a weaker form of modularity, being invariant up to roots of unity. We will examine their transformation properties in the next chapter; here, the full modular property is not needed.

Many functions arising in complex analysis, number theory, or combinatorics can be written as infinite series in powers of $q = e^{2\pi i\tau}$, known as q-expansions (see Section 4.1). Some of these functions also admit a representation as an infinite product in powers of q, these are known as *q-product expansions*. While q-expansions highlight the additive structure of a function through its Fourier coefficients, q-product expansions reflect their multiplicative structure and often arise in explicit constructions or factorizations.
Recall that for a meromorphic function f on $\mathbb{H}$ that is invariant under a congruence subgroup of level $N \in \mathbb{Z}_{>0}$, then invariance under translations implies that f is periodic with period N. Therefore, f can be expressed as a function in q. Consequently, the q-product expansion of f generally takes the form

$$f(\tau) = q^{\alpha} \prod_{n=1}^{\infty} (1 - c \cdot q^{an+b})^{c_n},$$

where $c \in \{\pm 1\}$, $\alpha, a, b \in \mathbb{Q}$, and $c_n \in \mathbb{C}$, defined for $0 < |q| < 1$.

Proposition 7.1.3. *Let $\tau \in \mathbb{H}$. The Weber functions have the following q-product expansions:*

$$\begin{aligned}
\mathfrak{f}(\tau) &= q^{-\frac{1}{48}} \prod_{n=1}^{\infty} (1 + q^{n-\frac{1}{2}})\\
\mathfrak{f}_1(\tau) &= q^{-\frac{1}{48}} \prod_{n=1}^{\infty} (1 - q^{n-\frac{1}{2}})\\
\mathfrak{f}_2(\tau) &= \sqrt{2}\ q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 + q^{n}).
\end{aligned}$$

Proof. We compute the expansions one after another, starting with $\mathfrak{f}(\tau)$.
Using $q = e^{2\pi i\tau}$, we calculate

$$\begin{aligned}
\eta\left(\frac{\tau+1}{2}\right) &= (e^{2\pi i\frac{\tau+1}{2}})^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-(e^{2\pi i\frac{\tau+1}{2}})^n) \\
&= (e^{2\pi i\tau})^{\frac{1}{48}}(e^{i\pi})^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-e^{\pi in\tau}e^{\pi in}) \\
&= q^{\frac{1}{48}}\zeta_{48} \prod_{n=1}^{\infty}(1-q^{\frac{n}{2}}(-1)^n) \\
&= q^{\frac{1}{48}}\zeta_{48} \prod_{\substack{n=1\\ n \text{ even}}}^{\infty}(1-q^{\frac{n}{2}}(-1)^n) \prod_{\substack{n=1\\ n \text{ odd}}}^{\infty}(1-q^{\frac{n}{2}}(-1)^n) \\
&= q^{\frac{1}{48}}\zeta_{48} \prod_{n=1}^{\infty}(1-q^n) \prod_{n=1}^{\infty}(1+q^{n-\frac{1}{2}}).
\end{aligned}$$

Thus, by using the definitions of the Weber functions and the η-function, we get

$$\begin{aligned}
\mathfrak{f}(\tau) = \frac{\eta(\frac{\tau+1}{2})}{\eta(\tau)} &= \zeta_{48}^{-1}\frac{q^{\frac{1}{48}}\zeta_{48}\prod_{n=1}^{\infty}(1-q^n)\prod_{n=1}^{\infty}(1+q^{n-\frac{1}{2}})}{q^{\frac{1}{24}}\prod_{n=1}^{\infty}(1-q^n)} \\
&= q^{-\frac{1}{48}} \prod_{n=1}^{\infty}(1+q^{n-\frac{1}{2}}).
\end{aligned}$$

Similarly, for $\mathfrak{f}_1(\tau)$ we compute

$$\begin{aligned}
\eta\left(\frac{\tau}{2}\right) &= (e^{2\pi i\frac{\tau}{2}})^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-(e^{2\pi i\frac{\tau}{2}})^n) \\
&= (e^{2\pi i\tau})^{\frac{1}{48}} \prod_{n=1}^{\infty}(1-e^{\frac{2\pi in\tau}{2}}) \\
&= q^{\frac{1}{48}} \prod_{n=1}^{\infty}(1-q^{\frac{n}{2}}) \\
&= q^{\frac{1}{48}} \prod_{n=1}^{\infty}(1-q^n) \prod_{n=1}^{\infty}(1-q^{n-\frac{1}{2}}),
\end{aligned}$$

which leads to

$$\begin{aligned}
\mathfrak{f}_1(\tau) = \frac{\eta(\frac{\tau}{2})}{\eta(\tau)}) &= \frac{q^{\frac{1}{48}}\prod_{n=1}^{\infty}(1-q^n)\prod_{n=1}^{\infty}(1-q^{n-\frac{1}{2}})}{q^{\frac{1}{24}}\prod_{n=1}^{\infty}(1-q^n)} \\
&= q^{-\frac{1}{48}} \prod_{n=1}^{\infty}(1-q^{n-\frac{1}{2}}).
\end{aligned}$$

Finally, for $\mathfrak{f}_2(\tau)$ we have

$$\begin{aligned}\eta(\sqrt{2}\tau) &= (e^{2\pi i 2\tau})^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-e^{2\pi i n 2\tau}) \\ &= q^{\frac{1}{12}} \prod_{n=1}^{\infty}(1-q^{2n}) \\ &= q^{\frac{1}{12}} \prod_{n=1}^{\infty}(1-q^{n}) \prod_{n=1}^{\infty}(1+q^{n}),\end{aligned}$$

using the third binomial formula. It follows that

$$\begin{aligned}\mathfrak{f}_2(\tau) = \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)} &= \sqrt{2}\frac{q^{\frac{1}{12}}\prod_{n=1}^{\infty}(1-q^n)\prod_{n=1}^{\infty}(1+q^n)}{q^{\frac{1}{24}}\prod_{n=1}^{\infty}(1-q^n)} \\ &= \sqrt{2}q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1+q^n),\end{aligned}$$

which gives the last expansion. □

From the q-product expansions we can derive the following identities connecting the Weber functions:

Corollary 7.1.4. *Let $\tau \in \mathbb{H}$. The Weber functions fulfil the relations*

$$\begin{aligned}\mathfrak{f}(\tau)\mathfrak{f}_1(\tau)\mathfrak{f}_2(\tau) &= \sqrt{2} \\ \mathfrak{f}_1(2\tau)\mathfrak{f}_2(\tau) &= \sqrt{2}.\end{aligned}$$

Proof. Using the q-product expansions of the Weber functions calculated in the previous proposition, we have

$$\begin{aligned}\mathfrak{f}(\tau)\mathfrak{f}_1(\tau) &= q^{-\frac{1}{48}} \prod_{n=1}^{\infty}(1+q^{n-\frac{1}{2}}) \cdot q^{-\frac{1}{48}} \prod_{n=1}^{\infty}(1-q^{n-\frac{1}{2}}) \\ &= q^{-\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^{2n-1}),\end{aligned}$$

and

$$\begin{aligned}\mathfrak{f}_2(\tau)\eta(\tau) &= \sqrt{2}\ q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1+q^{n}) \cdot q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^{n}) \\ &= \sqrt{2}\ q^{\frac{1}{12}} \prod_{n=1}^{\infty}(1-q^{2n}).\end{aligned}$$

Multiplying these two expressions yields

$$\begin{aligned}\mathfrak{f}(\tau)\mathfrak{f}_1(\tau)\mathfrak{f}_2(\tau)\eta(\tau) &= q^{-\frac{1}{24}}\prod_{n=1}^{\infty}(1-q^{2n-1})\cdot\sqrt{2}\,q^{\frac{1}{12}}\prod_{n=1}^{\infty}(1-q^{2n})\\ &= q^{-\frac{1}{24}}\prod_{\substack{n=1\\ n\text{ odd}}}^{\infty}(1-q^n)\cdot\sqrt{2}\,q^{\frac{1}{12}}\prod_{\substack{n=1\\ n\text{ even}}}^{\infty}(1-q^n)\\ &= q^{\frac{1}{24}}\sqrt{2}\prod_{n=1}^{\infty}(1-q^n)\\ &= \sqrt{2}\,\eta(\tau).\end{aligned}$$

Dividing both sides of the equation by $\eta(\tau)$ gives the first relation.
The second relation follows from the definitions of the Weber functions and the η-function:

$$\mathfrak{f}_1(2\tau)\mathfrak{f}_2(\tau) = \frac{\eta(\tau)}{\eta(2\tau)}\cdot\sqrt{2}\,\frac{\eta(2\tau)}{\eta(\tau)} = \sqrt{2}.$$

□

7.2 The Weierstrass σ-function

Building on the q-product expansions of the Weber functions, we now turn to the Weierstrass σ-function. We introduce its definition and develop its own q-product expansion, highlighting its relation to the Weierstrass $\wp$-function, which will play a key role in linking lattice structures to modular functions and, ultimately, in the computation of γ_2.

Definition 7.2.1 (Weierstrass σ-function)**.** For a lattice $L \subseteq \mathbb{C}$ and $z \in \mathbb{C}$, the Weierstrass σ-function for L is defined by

$$\sigma(z;L) := z\prod_{\omega\in L\setminus\{0\}}\left(1-\frac{z}{\omega}\right)e^{\frac{z}{\omega}+\frac{1}{2}(\frac{z}{\omega})^2}$$

We will write $\sigma(z)$ instead of $\sigma(z;L)$ whenever the lattice L is clear from context.
Moreover, note that the only zeros of the Weierstrass σ-function are simple zeros at the lattice points (including $z=0$), which follows from the factor $1-\frac{z}{\omega}=\frac{\omega-z}{\omega}$.
The σ-function is defined by a convergent infinite product of functions that are holomorphic except at isolated points, and the product is arranged so that these singularities cancel out. Since $\sigma(z)$ has simple zeros exactly at the lattice points and no poles anywhere in $\mathbb{C}$, it follows that $\sigma(z)$ is holomorphic on all of $\mathbb{C}$.
Moreover, using the fact that $\{-\omega \mid \omega \in L\} = L$, a short calculation shows that $\sigma(z)$ is

an odd function:

$$\begin{aligned}\sigma(-z) &= -z \prod_{\omega\in L\setminus\{0\}} \left(1-\frac{-z}{\omega}\right) e^{\frac{-z}{\omega}+\frac{1}{2}(\frac{-z}{\omega})^2} \\ &= -z \prod_{\omega\in L\setminus\{0\}} \left(1-\frac{z}{-\omega}\right) e^{\frac{z}{-\omega}+\frac{1}{2}(\frac{z}{\omega})^2} \\ &= -z \prod_{\omega\in L\setminus\{0\}} \left(1-\frac{z}{\omega}\right) e^{\frac{z}{\omega}+\frac{1}{2}(\frac{z}{\omega})^2} = -\sigma(z),\end{aligned}$$

which will be useful to show its quasi-periodical behaviour.

Proposition 7.2.2. *Let $\tau \in \mathbb{H}$. The Weierstrass σ-function for the lattice $L = [1,\tau]$ satisfies the following relations:*

$$\begin{aligned}\sigma(z+\tau) &= -e^{\eta_1(z+\frac{\tau}{2})}\sigma(z) \\ \sigma(z+1) &= -e^{\eta_2(z+\frac{1}{2})}\sigma(z),\end{aligned}$$

where $\eta_1,\eta_2 \in \mathbb{C}$ fulfil the Legendre relation $\eta_2\tau - \eta_1 = 2\pi i$.

Proof. We prove this proposition in four steps:
Step 1: Define the Weierstrass ζ-function by

$$\zeta(z) \coloneqq \frac{\sigma'(z)}{\sigma(z)},$$

which should not be confused by the Riemann ζ-function. Since

$$\ln(\sigma(z)) = \ln(z) + \sum_{\omega\in L\setminus\{0\}} \left(\ln\left(1-\frac{z}{\omega}\right) + \frac{z}{\omega} + \frac{z^2}{2\omega^2}\right),$$

applying the chain rule yields

$$\begin{aligned}\zeta(z) = \frac{\sigma'(z)}{\sigma(z)} = (\ln(\sigma(z)))' &= \frac{1}{z} + \sum_{\omega\in L\setminus\{0\}} \left(\frac{-\frac{1}{\omega}}{1-\frac{z}{\omega}} + \frac{1}{\omega} + \frac{z}{\omega^2}\right) \\ &= \frac{1}{z} + \sum_{\omega\in L\setminus\{0\}} \left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right).\end{aligned}$$

It follows that $\zeta(z)$ has poles at every lattice point L (including 0).
Step 2: Differentiating once more gives

$$\zeta'(z) = \left(\frac{\sigma'(z)}{\sigma(z)}\right)' = -\frac{1}{z^2} + \sum_{\omega\in L\setminus\{0\}} \left(-\frac{1}{(z-\omega)^2} + \frac{1}{\omega^2}\right),$$

so that we obtain the fundamental relation $\wp(z) = -\zeta'(z)$. Therefore, for any $\omega_0 \in L$,

$$\frac{\mathrm{d}}{\mathrm{d}z}(\zeta(z+\omega_0) - \zeta(z)) = \zeta'(z+\omega_0) - \zeta'(z) = -\wp(z+\omega_0) + \wp(z) = 0,$$

since the Weierstrass $\wp$-function is L-periodic, i.e. $\wp(z+\omega_0)=\wp(z)$. This implies that the function $\zeta(z+\omega_0)-\zeta(z)$ is constant for every $\omega_0 \in L$.
Step 3: Using the definition of the ζ-function and the identity $\eta_1 = \zeta(z+\tau)-\zeta(z)$, which is independent of z by *Step* 2, the quotient rule yields

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}z}\frac{\sigma(z+\tau)}{\sigma(z)} &= \frac{\sigma(z)\sigma'(z+\tau)-\sigma'(z)\sigma(z+\tau)}{\sigma^2(z)}\\ &= \frac{\sigma(z)\sigma(z+\tau)\zeta(z+\tau)-\sigma(z)\sigma(z+\tau)\zeta(z)}{\sigma^2(z)}\\ &= \frac{\sigma(z+\tau)(\zeta(z)+\eta_1)-\sigma(z+\tau)\zeta(z)}{\sigma(z)}\\ &= \eta_1\frac{\sigma(z+\tau)}{\sigma(z)}.\end{aligned}$$

Now define $f(z)=\frac{\sigma(z+\tau)}{\sigma(z)}$. Then $f(z)$ satisfies the first-order linear differential equation $f'(z)=\eta_1 f(z)$, whose general solution is $f(z)=Ce^{\eta_1 z}$ for some constant C depending on τ. Hence,

$$\sigma(z+\tau)=Ce^{\eta_1 z}\sigma(z).$$

To determine C, we evaluate at $z=-\frac{\tau}{2}$. Using the oddness of $\sigma(z)$, we get

$$\sigma\left(\frac{\tau}{2}\right)=Ce^{-\eta_1\frac{\tau}{2}}\sigma\left(-\frac{\tau}{2}\right)=-Ce^{-\eta_1\frac{\tau}{2}}\sigma\left(\frac{\tau}{2}\right).$$

Since $\sigma(\frac{\tau}{2})\neq 0$, it follows that $-Ce^{-\eta_1\frac{\tau}{2}}=1$, so that $C=-e^{\eta_1\frac{\tau}{2}}$. Substituting back gives

$$\sigma(z+\tau)=-e^{\eta_1\frac{\tau}{2}}e^{\eta_1 z}\sigma(z)=-e^{\eta_1(z+\frac{\tau}{2})}\sigma(z),$$

which is the first quasi-periodicity formula.
Similarly, replacing τ with 1 and using $\eta_2=\zeta(z+1)-\zeta(z)$ gives the second formula

$$\sigma(z+1)=-e^{\eta_2(z+\frac{1}{2})}\sigma(z).$$

Step 4: It remains to show that η_1 and η_2 fulfil the relation $2\pi i=\eta_2\tau-\eta_1$. For that, choose $\gamma\in(-1,0)$ and let $P=P_0+\gamma=\{\lambda_1+\lambda_2\tau \mid \gamma\leq\lambda_1,\lambda_2<\gamma+1\}$ be a period parallelogram for the lattice $L=[1,\tau]$ with boundary $C=\delta P$. Then C is a simply closed curve, assumed with positive orientation. Since $\zeta(z)$ has a pole at every lattice point (including 0) by Step 1, the only pole of $\zeta(z)$ in P is 0 (note that $0\in P$ since $-1<\gamma<0$ so $0<\gamma+1<1$), and it does not lie on C. As the function $\sigma(z)$ is holomorphic on $\mathbb{C}$, its derivative $\sigma'(z)$ is holomorphic on $\mathbb{C}$ as well, and so the quotient $\frac{\sigma'(z)}{\sigma(z)}$ is meromorphic on $\mathbb{C}$. Thus, all the assumptions for Cauchy's argument principle 1.0.8 are satisfies, and we can apply it to conclude that

$$\int_C \zeta(z)\,dz=\int_C\frac{\sigma'(z)}{\sigma(z)}dz=2\pi i\cdot(\#(\text{zeros of }\sigma\text{ in }P)-\#(\text{poles of }\sigma\text{ in }P)).$$

Since the only pole of $\zeta(z)$ in P is at $z = 0$, the only zero of $\sigma(z)$ in P is also at $z = 0$. Turning to the poles of $\sigma(z)$, we consider the zeros of $\frac{1}{\sigma(z)}$, which are determined by the factors $\frac{\omega}{\omega - z}$ for $\omega \in L\backslash\{0\}$. These never vanish for $z \notin L$, so $\sigma(z)$ has no poles in P other than at the lattice points. Therefore,

$$\int_C \zeta(z)\ dz = 2\pi i.$$

Now let C_i, $i = 1, 2, 3, 4$, be the bottom, right, top and left boundaries of the parallelogram C respectively, all with induced positive orientation. Then

$$\begin{aligned} 2\pi i &= \int_C \zeta(z)\ dz = \int_{C_1} \zeta(z)\ dz + \int_{C_2} \zeta(z)\ dz + \int_{C_3} \zeta(z)\ dz + \int_{C_4} \zeta(z)\ dz \\ &= \int_{\gamma+\gamma\tau}^{\gamma+1+\gamma\tau} \zeta(z)\ dz + \int_{\gamma+1+\gamma\tau}^{\gamma+1+(\gamma+1)\tau} \zeta(z)\ dz + \int_{\gamma+1+(\gamma+1)\tau}^{\gamma+(\gamma+1)\tau} \zeta(z)\ dz + \int_{\gamma+(\gamma+1)\tau}^{\gamma+\gamma\tau} \zeta(z)\ dz \end{aligned}$$

Using the same idea as in Proposition 2.3.9, namely, by considering the integrals over the bottom and top boundaries of C, and the identity $\eta_1 = \zeta(z + \tau) - \zeta(z)$, we obtain

$$\begin{aligned} \int_{C_1} \zeta(z)\ dz + \int_{C_3} \zeta(z)\ dz &= \int_{\gamma+\gamma\tau}^{\gamma+1+\gamma\tau} \zeta(z)\ dz + \int_{\gamma+1+(\gamma+1)\tau}^{\gamma+(\gamma+1)\tau} \zeta(z)\ dz \\ &= \int_{\gamma}^{\gamma+1} \zeta(u+\gamma\tau)\ du - \int_{\gamma}^{\gamma+1} \zeta(u+(\gamma+1)\tau)\ du \\ &= \int_{\gamma}^{\gamma+1} \zeta(u+\gamma\tau)\ du - \int_{\gamma}^{\gamma+1} \zeta(u+\gamma\tau+\tau)\ du \\ &= \int_{\gamma}^{\gamma+1} \zeta(u+\gamma\tau)\ du - \int_{\gamma}^{\gamma+1} \zeta(u+\gamma\tau) + \eta_1\ du \\ &= -\int_{\gamma}^{\gamma+1} \eta_1 du = -\eta_1, \end{aligned}$$

with the change of variables $u = z - a\tau$ with $a = \gamma, \gamma + 1$ in the second equality.
Similarly, by considering the integrals over the right and left boundaries of C, and the identity $\eta_2 = \zeta(z + 1) - \zeta(z)$, we get

$$\begin{aligned} \int_{C_2} \zeta(z)\ dz + \int_{C_4} \zeta(z)\ dz &= \int_{\gamma+1+\gamma\tau}^{\gamma+1+(\gamma+1)\tau} \zeta(z)\ dz + \int_{\gamma+(\gamma+1)\tau}^{\gamma+\gamma\tau} \zeta(z)\ dz \\ &= \int_{\gamma}^{\gamma+1} \zeta(\gamma+u\tau+1)\tau\ du - \int_{\gamma}^{\gamma+1} \zeta(\gamma+u\tau)\tau\ du \\ &= \int_{\gamma}^{\gamma+1} (\zeta(\gamma+u\tau)+\eta_2)\tau\ du - \int_{\gamma}^{\gamma+1} \zeta(\gamma+u\tau)\tau\ du \\ &= \int_{\gamma}^{\gamma+1} \eta_2\tau\ du = \eta_2\tau, \end{aligned}$$

with the change of variables $z = \gamma + u\tau + 1$ for the first and $z = \gamma + u\tau$ for the second integral. Combining these results yields $2\pi i = \eta_2\tau - \eta_1$, as desired. □

In such way as the numbers 1 and τ are called the periods of the Weierstrass $\wp$-function, the numbers η_1 and η_2 are called the *quasiperiods* of the Weierstrass σ-function.

Although the σ-function is not periodic, we aim to express it as a q-product expansion, which will help us connect it to the Weber functions and the Dedekind η-function. To do so, we need the following theorem:

Proposition 7.2.3. *Let $\tau \in \mathbb{H}$ and let $L = [1, \tau]$ be the corresponding lattice in $\mathbb{C}$. For $z, \omega \in \mathbb{C}\backslash L$, the Weierstrass σ-function and the Weierstrass $\wp$-function satisfy*

$$\wp(z) - \wp(\omega) = -\frac{\sigma(z+\omega)\sigma(z-\omega)}{\sigma^2(z)\sigma^2(\omega)}.$$

Proof. Let $z, \omega \in \mathbb{C}\backslash L$, and set

$$f(z) = -\frac{\sigma(z+\omega)\sigma(z-\omega)}{\sigma^2(z)\sigma^2(\omega)}.$$

We break down the proof of this proposition into three steps:
Step 1: We show that $f(z)$ is an even elliptic function for L, this will then imply that $f(z)$ is a rational function in $\wp(z)$ by Lemma 3.1.1 (ii).
Since the Weierstrass σ-function is odd as seen earlier, it follows that $f(z)$ is even:

$$f(-z) = -\frac{\sigma(-z+\omega)\sigma(-z-\omega)}{\sigma^2(-z)\sigma^2(\omega)} = -\frac{\sigma(z-\omega)\sigma(z+\omega)}{\sigma^2(z)\sigma^2(\omega)} = f(z).$$

To verify periodicity, it suffices to show that $f(z+1) = f(z+\tau) = f(z)$, since $L = [1, \tau]$. Using the quasi-periodicity relations from Proposition 7.2.2, we obtain

$$\begin{aligned} f(z+1) &= -\frac{\sigma(z+\omega+1)\sigma(z-\omega+1)}{\sigma^2(z+1)\sigma^2(\omega)} \\ &= -\frac{e^{\eta_2(z+\omega+\frac{1}{2})}\sigma(z+\omega)e^{\eta_2(z-\omega+\frac{1}{2})}\sigma(z-\omega)}{e^{2\eta_2(z+\frac{1}{2})}\sigma^2(z)\sigma^2(\omega)} \\ &= -\frac{\sigma(z+\omega)\sigma(z-\omega)}{\sigma^2(z)\sigma^2(\omega)} = f(z), \end{aligned}$$

and similarly,

$$\begin{aligned} f(z+\tau) &= -\frac{\sigma(z+\omega+\tau)\sigma(z-\omega+\tau)}{\sigma^2(z+\tau)\sigma^2(\omega)} \\ &= -\frac{e^{\eta_1(z+\omega+\frac{\tau}{2})}\sigma(z+\omega)e^{\eta_1(z-\omega+\frac{\tau}{2})}\sigma(z-\omega)}{e^{2\eta_1(z+\frac{\tau}{2})}\sigma^2(z)\sigma^2(\omega)} \\ &= -\frac{\sigma(z+\omega)\sigma(z-\omega)}{\sigma^2(z)\sigma^2(\omega)} = f(z). \end{aligned}$$

Therefore, f is doubly periodic with respect to L.
As $\sigma(z)$ is holomorphic on $\mathbb{C}$ and vanishes precisely at the lattice points L, any poles of

$f(z)$ arise only from zeros of $\sigma(z)$ in the denominator. Thus, $f(z)$ is meromorphic on $\mathbb{C}$.
Step 2: We show that the Laurent series expansion of $f(z)$ at $z = 0$ starts with $\frac{1}{z^2}$.
Since we established in *Step 1* that $f(z)$ is meromorphic on $\mathbb{C}$ with poles only at the lattice points L, it is meromorphic in a neighbourhood of $z = 0$, and hence admits a Laurent expansion there. To determine the leading term, we write

$$\begin{aligned} f(z) &= \frac{1}{\sigma^2(z)} \left(-\frac{\sigma(z+\omega)\sigma(z-\omega)}{\sigma^2(\omega)} \right) \\ &= \frac{1}{z^2} \left(\prod_{\omega \in L \setminus \{0\}} \left(1 - \frac{z}{\omega}\right) e^{\frac{z}{\omega} + \frac{1}{2}(\frac{z}{\omega})^2} \right)^{-2} \left(-\frac{\sigma(z+\omega)\sigma(z-\omega)}{\sigma^2(\omega)} \right). \end{aligned}$$

Both factors in the parentheses are holomorphic near $z = 0$. Indeed, this holds for the first factor, since $\sigma(z)$ is holomorphic near $z = 0$ and we exclude the initial z-term. For the second factor, the nominator is holomorphic as $\omega \notin L$, and the denominator $\sigma(\omega)^2$ is non-zero by the same assumption, hence the whole expression is holomorphic near 0. Hence both factors admit Taylor expansions, so in particular Laurent expansions involving only non-negative powers of z. Their constant terms are found by setting $z = 0$. The first factor evaluates to 1 and the second one is

$$-\frac{\sigma(0+\omega)\sigma(0-\omega)}{\sigma(\omega)^2} = -\frac{\sigma(\omega)(-\sigma(\omega))}{\sigma(\omega)^2} = -\frac{-\sigma(\omega)^2}{\sigma(\omega)^2} = 1.$$

It follows that the Laurent expansion of $f(z)$ at $z = 0$ indeed starts with the term $\frac{1}{z^2}$.
Step 3: We conclude $f(z) = \wp(z) + C$ for some constant C and deduce the formula.
Since $f(z)$ is meromorphic on $\mathbb{C}$ with poles only at lattice points L by *Step* 1, it is holomorphic on $\mathbb{C}\backslash L$. Moreover, $f(z)$ is an elliptic function for L by *Step* 1, so by Proposition 3.1.2, it can be expressed as a polynomial in $\wp(z)$, that is, there exists $A(x) \in \mathbb{C}[x]$, such that $f(z) = A(\wp(z))$. By *Step* 2, the Laurent expansion of $f(z)$ at $z = 0$ starts with $\frac{1}{z^2}$, which matches the leading term of the Laurent expansion of $\wp(z)$ (Theorem 2.3.18). Hence, the polynomial $A(x)$ must be linear of the form $A(x) = x + C$, so that $f(z) = \wp(z) + C$ for some constant $C \in \mathbb{C}$. To determine C, we evaluate at $z = \omega$. Since $\sigma(0) = 0$ by definition, we get

$$\wp(\omega) + C = f(\omega) = -\frac{\sigma(\omega+\omega)\sigma(\omega-\omega)}{\sigma^2(\omega)\sigma^2(\omega)} = -\frac{\sigma(2\omega)\sigma(0)}{\sigma^4(\omega)} = 0.$$

Therefore, $C = -\wp(\omega)$, giving the desired formula $f(z) = \wp(z) - \wp(\omega)$. □

While one-variable q-product expansions (Section 4.1) reflect the periodic behaviour of functions with respect to the lattice $L = [1, \tau]$, the two-variable case generalizes this structure to functions that are typically no longer periodic with respect to L. Instead, the focus shifts to quasi-periodicity. This is naturally reflected in their q-product expansion in two variables, involving both $q_\tau = e^{2\pi i \tau}$ and $q_z = e^{2\pi i z}$, which encode both the zeros of the function and their quasi-periodic transformations under lattice translations.
A central example is the Weierstrass σ-function, whose quasi-periodicity we established in Proposition 7.2.2, and which admits the following two-variable q-product expansion:

Proposition 7.2.4. *Let $\tau \in \mathbb{H}$ and $z \in \mathbb{C}$. The Weierstrass σ-function has the following two-variable q-product expansion:*

$$\sigma(z) = \frac{1}{2\pi i} e^{\eta_2 \frac{z^2}{2}} (q_z^{\frac{1}{2}} - q_z^{-\frac{1}{2}}) \prod_{n=1}^{\infty} \frac{(1 - q_\tau^n q_z)(1 - \frac{q_\tau^n}{q_z})}{(1 - q_\tau^n)^2},$$

where $q_\tau = e^{2\pi i \tau}$ and $q_z = e^{2\pi i z}$.

Proof. Denote by $f(z)$ the right-hand side of the above equation. We prove the proposition in four steps:
Step 1: We show that the zeros of $f(z)$ and $\sigma(z)$ are precisely the lattice points in L. Since the quotient of holomorphic functions is holomorphic whenever the denominator is non-zero, it will then follow that $\frac{\sigma(z)}{f(z)}$ is holomorphic on $\mathbb{C}\backslash L$.
By definition, the Weierstrass σ-function has simple zeros at the points of L (including $z = 0$). The zeros of $f(z)$ occur in two ways:

- $q_z^{\frac{1}{2}} = q_z^{-\frac{1}{2}}$, which gives $e^{\pi i z} = e^{-\pi i z}$, or equivalently, $e^{2\pi i z} = 1$, so that $z \in \mathbb{Z} \subseteq L$.
- $q_\tau^n q_z^{\pm 1} = 1$, which means $e^{2\pi i n\tau \pm 2\pi i z} = e^{2\pi i (n\tau \pm z)} = 1$, so that $n\tau \pm z \in \mathbb{Z}$ and hence $z = m \pm n\tau$ for some $m \in \mathbb{Z}$, and since $n \in \mathbb{Z}$, we have $z \in L$.

This case distinction includes the lattice point $z = 0$, which is also a zero of $f(z)$.
Conversely, let $z = m + n\tau \in L$. If $n = 0$, then

$$q_z^{\frac{1}{2}} - q_z^{-\frac{1}{2}} = e^{\pi i m} - e^{-\pi i m} = (-1)^m - (-1)^{-m} = 0,$$

by Euler's identity. If $n > 0$, then

$$\frac{q_\tau^n}{q_z} = e^{2\pi i (n\tau - z)} = e^{-2\pi i m} = (-1)^{-2m} = 1,$$

and if $n < 0$, then

$$q_\tau^{-n} q_z = e^{2\pi i (z - n\tau)} = e^{2\pi i m} = (-1)^{2m} = 1.$$

Hence every lattice point $z \in L$ corresponds to a zero of $f(z)$, which matches the simple zeros of $\sigma(z)$. It follows that the quotient $\frac{\sigma(z)}{f(z)}$ is holomorphic on $\mathbb{C}\backslash L$.
Step 2: Next, we show that $\frac{\sigma(z)}{f(z)}$ is L-periodic. Since every lattice $L \subseteq \mathbb{C}$ is homothetic to a lattice of the form $[1, \tau]$ with $\tau \in \mathbb{H}$, we may assume $L = [1, \tau]$. Therefore it suffices

to show that $\frac{\sigma(z)}{f(z)}$ has periods 1 and τ. We begin by computing $f(z+1)$:

$$\begin{aligned}
f(z+1) &= \frac{1}{2\pi i} e^{\eta_2 \frac{(z+1)^2}{2}} (q_{z+1}^{\frac{1}{2}} - q_{z+1}^{-\frac{1}{2}}) \prod_{n=1}^{\infty} \frac{(1-q_\tau^n q_{z+1})(1-q_\tau^n q_{z+1}^{-1})}{(1-q_\tau^n)^2} \\
&= \frac{1}{2\pi i} e^{\eta_2 \frac{(z+1)^2}{2}} (e^{\pi i(z+1)} - e^{-\pi i(z+1)}) \prod_{n=1}^{\infty} \frac{(1-q_\tau^n e^{2\pi i(z+1)})(1-q_\tau^n e^{-2\pi i(z+1)})}{(1-q_\tau^n)^2} \\
&= \frac{1}{2\pi i} e^{\eta_2 \frac{z^2+2z+1}{2}} (e^{\pi i z} e^{\pi i} - e^{-\pi i z} e^{-\pi i}) \prod_{n=1}^{\infty} \frac{(1-q_\tau^n e^{2\pi i z} e^{2\pi i})(1-q_\tau^n e^{-2\pi i z} e^{-2\pi i})}{(1-q_\tau^n)^2} \\
&= e^{\eta_2 \frac{2z+1}{2}} \frac{1}{2\pi i} e^{\eta_2 \frac{z^2}{2}} (e^{\pi i z}(-1) - e^{-\pi i z}(-1)) \prod_{n=1}^{\infty} \frac{(1-q_\tau^n q_z 1)(1-q_\tau^n q_z^{-1} 1)}{(1-q_\tau^n)^2} \\
&= (-1) e^{\eta_2 (z+\frac{1}{2})} \frac{1}{2\pi i} e^{\eta_2 \frac{z^2}{2}} (q_z^{\frac{1}{2}} - q_z^{-\frac{1}{2}}) \prod_{n=1}^{\infty} \frac{(1-q_\tau^n q_z)(1-q_\tau^n q_z^{-1})}{(1-q_\tau^n)^2} \\
&= -e^{\eta_2 (z+\frac{1}{2})} f(z).
\end{aligned}$$

As $\sigma(z+1) = -e^{\eta_2(z+\frac{1}{2})}\sigma(z)$ by Proposition 7.2.2, we conclude that

$$\frac{\sigma(z+1)}{f(z+1)} = \frac{-e^{\eta_2(z+\frac{1}{2})}\sigma(z)}{-e^{\eta_2(z+\frac{1}{2})} f(z)} = \frac{\sigma(z)}{f(z)}.$$

Now we compute $f(z+\tau)$. Note that $q_{z+\tau} = e^{2\pi i(z+\tau)} = e^{2\pi i z} e^{2\pi i \tau} = q_z q_\tau$, so we get

$$\begin{aligned}
f(z+\tau) &= \frac{1}{2\pi i} e^{\eta_2 \frac{(z+\tau)^2}{2}} (q_{z+\tau}^{\frac{1}{2}} - q_{z+\tau}^{-\frac{1}{2}}) \prod_{n=1}^{\infty} \frac{(1-q_\tau^n q_{z+\tau})(1-q_\tau^n q_{z+\tau}^{-1})}{(1-q_\tau^n)^2} \\
&= e^{\eta_2 \frac{2z\tau+\tau^2}{2}} \frac{1}{2\pi i} e^{\eta_2 \frac{z^2}{2}} (q_z^{\frac{1}{2}} q_\tau^{\frac{1}{2}} - q_z^{-\frac{1}{2}} q_\tau^{-\frac{1}{2}}) \frac{\prod_{n=1}^{\infty}(1-q_\tau^{n+1} q_z)(1-q_\tau^{n-1} q_z^{-1})}{\prod_{n=1}^{\infty}(1-q_\tau^n)^2}.
\end{aligned}$$

Using the Legendre relation $\eta_2\tau - \eta_1 = 2\pi i$ gives

$$\begin{aligned}
e^{\eta_2 \frac{2z\tau+\tau^2}{2}} &= e^{\eta_2 \tau \frac{(2z+\tau)}{2}} = e^{(\eta_1 + 2\pi i)\frac{(2z+\tau)}{2}} = e^{\eta_1(z+\frac{\tau}{2})} e^{2\pi i(z+\frac{\tau}{2})} \\
&= e^{\eta_1(z+\frac{\tau}{2})} e^{2\pi i z} e^{\pi i \tau} = e^{\eta_1(z+\frac{\tau}{2})} q_z q_\tau^{\frac{1}{2}},
\end{aligned}$$

and rearranging the terms in the product yields

$$\begin{aligned}
\prod_{n=1}^{\infty}(1-q_\tau^{n+1}q_z)(1-q_\tau^{n-1}q_z^{-1}) &= \prod_{n=1}^{\infty}(1-q_\tau^{n+1}q_z) \prod_{n=1}^{\infty}(1-q_\tau^{n-1}q_z^{-1}) \\
&= \prod_{m=2}^{\infty}(1-q_\tau^m q_z) \prod_{p=0}^{\infty}(1-q_\tau^p q_z^{-1}) \\
&= \left(\frac{1}{1-q_\tau q_z}\prod_{m=1}^{\infty}(1-q_\tau^m q_z)\right)\left((1-q_z^{-1})\prod_{p=1}^{\infty}(1-q_\tau^p q_z^{-1})\right) \\
&= \frac{1-q_z^{-1}}{1-q_\tau q_z}\prod_{n=1}^{\infty}(1-q_\tau^n q_z)(1-q_\tau^n q_z^{-1}).
\end{aligned} \tag{7.1}$$

Combining these two facts gives

$$f(z+\tau) = e^{\eta_1(z+\frac{\tau}{2})} q_z q_\tau^{\frac{1}{2}} \frac{1}{2\pi i} e^{\eta_2 \frac{z^2}{2}} (q_z^{\frac{1}{2}} q_\tau^{\frac{1}{2}} - q_z^{-\frac{1}{2}} q_\tau^{-\frac{1}{2}}) \frac{1-q_z^{-1}}{1-q_\tau q_z} \prod_{n=1}^{\infty} \frac{(1-q_\tau^n q_z)(1-q_\tau^n q_z^{-1})}{(1-q_\tau^n)^2}$$

$$= q_z q_\tau^{\frac{1}{2}} \frac{1-q_z^{-1}}{1-q_\tau q_z} \cdot \frac{q_z^{\frac{1}{2}} q_\tau^{\frac{1}{2}} - q_z^{-\frac{1}{2}} q_\tau^{-\frac{1}{2}}}{q_z^{\frac{1}{2}} - q_z^{-\frac{1}{2}}} e^{\eta_1(z+\frac{\tau}{2})} f(z).$$

It remains to simplify the first factor:

$$q_z q_\tau^{\frac{1}{2}} \frac{1-q_z^{-1}}{1-q_\tau q_z} \cdot \frac{q_z^{\frac{1}{2}} q_\tau^{\frac{1}{2}} - q_z^{-\frac{1}{2}} q_\tau^{-\frac{1}{2}}}{q_z^{\frac{1}{2}} - q_z^{-\frac{1}{2}}} = \frac{q_z - 1}{1-q_\tau q_z} \cdot \frac{q_z q_\tau - 1}{q_z - 1} = -1.$$

Thus, we obtain

$$f(z+\tau) = -e^{\eta_1(z+\frac{\tau}{2})} f(z)$$

and since $\sigma(z+\tau) = -e^{\eta_1(z+\frac{\tau}{2})}\sigma(z)$ by Proposition 7.2.2, we again conclude that

$$\frac{\sigma(z+\tau)}{f(z+\tau)} = \frac{\sigma(z)}{f(z)}.$$

Hence, $\frac{\sigma(z)}{f(z)}$ is invariant under shifts by 1 and τ, and therefore L-periodic.

Step 3: Now, we show that $\frac{\sigma(z)}{f(z)}$ is holomorphic at $z = 0$ and assumes the value 1 there. By *Step 1*, both $\sigma(z)$ and $f(z)$ have a simple zero at $z = 0$, so their quotient $\frac{\sigma(z)}{f(z)}$ is well-defined at 0. We write

$$\frac{\sigma(z)}{f(z)} = 2\pi i \frac{z}{q_z^{\frac{1}{2}} - q_z^{-\frac{1}{2}}} \frac{\prod_{\omega \in L\setminus\{0\}} (1-\frac{z}{\omega})\, e^{\frac{z}{\omega}+\frac{1}{2}(\frac{z}{\omega})^2}}{e^{\eta_2 \frac{z^2}{2}} \prod_{n=1}^{\infty} \frac{(1-q_\tau^n q_z)(1-\frac{q_\tau^n}{q_z})}{(1-q_\tau^n)^2}},$$

so by inserting $z = 0$, all factors in the products and the exponential evaluate to 1. Turning to the first fraction, both the numerator and denominator vanish at $z = 0$, but are holomorphic near 0. Since the derivative of the denominator does not vanish at $z = 0$, we may use L'Hôpital's rule (1.0.2) to compute the limit:

$$2\pi i \lim_{z\to 0} \frac{z}{e^{\pi i z} - e^{-\pi i z}} = 2\pi i \lim_{z\to 0} \frac{1}{\pi i (e^{\pi i z} + e^{-\pi i z})} = \frac{2\pi i}{2\pi i} = 1.$$

Hence, $\lim_{z\to 0} \frac{\sigma(z)}{f(z)} = \lim_{z\to 0} \frac{\sigma'(z)}{f'(z)}$ exists, and the function $\frac{\sigma(z)}{f(z)}$ extends holomorphically to $z = 0$ with the value 1, as claimed.

Step 4: Finally, we conclude that $\sigma(z) = f(z)$. Since $\frac{\sigma(z)}{f(z)}$ is holomorphic on $\mathbb{C}\setminus L$ by *Step 1* and both σ and f have simple zeros at the same lattice points, all singularities of the quotient are removable. Indeed, near any $\omega \in L$, we can write $\sigma(z) = (z-\omega)\sigma_1(z)$ and $f(z) = (z-\omega)f_1(z)$, where σ_1 and f_1 are holomorphic and non-vanishing near ω by the Taylor expansion of σ and f at ω, so their quotient $\frac{\sigma(z)}{f(z)} = \frac{\sigma_1(z)}{f_1(z)}$ is holomorphic near ω. It follows that $\frac{\sigma(z)}{f(z)}$ extends to a holomorphic function to all of $\mathbb{C}$ and hence is meromorphic on $\mathbb{C}$. By *Step* 2, this function is L-periodic and hence an elliptic function for L. It follows that it is constant by Liouville's Theorem 1.0.6. Since $\frac{\sigma(z)}{f(z)}$ assumes the constant value 1 at $z = 0$ by *Step 3*, we conclude $\sigma(z) = f(z)$. □

7.3 Algebraic computation of γ_2

We now arrive at the final step of our algebraic construction. Having developed the q-product expansions of the Weber functions and the Weierstrass σ-function and clarified their interrelations, we can now explicitly construct γ_2. This construction forms the missing link to the arithmetic of the j-invariant and leads to the proof that the coefficients of its q-expansion are integers.

Lemma 7.3.1. *The following formulas, involving the Weierstrass σ-function, the Weber functions, the Dedekind η-function, and Legendre's relation, hold*

$$\begin{aligned}\sigma\left(\frac{1}{2}\right) &= \frac{1}{2\pi} e^{\frac{\eta_2}{8}} \frac{\mathfrak{f}_2(\tau)^2}{\eta(\tau)^2},\\ \sigma\left(\frac{\tau}{2}\right) &= \frac{i}{2\pi} e^{\eta_2 \frac{\tau^2}{8}} q^{-\frac{1}{8}} \frac{\mathfrak{f}_1(\tau)^2}{\eta(\tau)^2},\\ \sigma\left(\frac{\tau+1}{2}\right) &= \frac{i}{2\pi} e^{\eta_2 \frac{(\tau+1)^2}{8}} q^{-\frac{1}{8}} \frac{\mathfrak{f}(\tau)^2}{\eta(\tau)^2}.\end{aligned}$$

Proof. The main tool for this proof is the q-product expansion of the σ-function from Proposition 7.2.4. We compute the formulas one by one.
For $\sigma(\frac{1}{2})$, we begin by rewriting the product

$$\begin{aligned}\prod_{n=1}^{\infty}(1+q_\tau^n)^2 &= \prod_{n=1}^{\infty}\frac{(1+q_\tau^n)^2(1-q_\tau^n)^2}{(1-q_\tau^n)^2}\\ &= \prod_{n=1}^{\infty}\frac{((1+q_\tau^n)(1-q_\tau^n))^2}{(1-q_\tau^n)^2} = \prod_{n=1}^{\infty}\frac{(1-q_\tau^{2n})^2}{(1-q_\tau^n)^2}\\ &= \frac{q_\tau^{-\frac{1}{6}}\left(q_\tau^{\frac{1}{12}}\prod_{n=1}^{\infty}(1-q_\tau^{2n})\right)^2}{q_\tau^{-\frac{1}{12}}\left(q_\tau^{\frac{1}{24}}\prod_{n=1}^{\infty}(1-q_\tau^{n})\right)^2} = \frac{q_\tau^{-\frac{1}{6}}\left(q_{2\tau}^{\frac{1}{24}}\prod_{n=1}^{\infty}(1-q_{2\tau}^{n})\right)^2}{q_\tau^{-\frac{1}{12}}\left(q_\tau^{\frac{1}{24}}\prod_{n=1}^{\infty}(1-q_\tau^{n})\right)^2}\\ &= \frac{q_\tau^{-\frac{1}{6}}\eta(2\tau)^2}{q_\tau^{-\frac{1}{12}}\eta(\tau)^2} = q_\tau^{-\frac{1}{12}}\frac{\mathfrak{f}_2(\tau)^2}{2}.\end{aligned}$$

At $z=\frac{1}{2}$, we have $q_z = e^{i\pi} = -1$. Substituting $q = q_\tau$ in the q-product expansion of

$\sigma(z)$, and using the above calculation gives

$$\begin{aligned}
\sigma\left(\frac{1}{2}\right) &= \frac{1}{2\pi i} e^{\frac{\eta_2}{8}} ((-1)^{\frac{1}{2}} - (-1)^{-\frac{1}{2}}) \prod_{n=1}^{\infty} \frac{(1+q^n)(1+q^n)}{(1-q^n)^2} \\
&= \frac{1}{2\pi i} e^{\frac{\eta_2}{8}} (i - (-i)) \frac{\prod_{n=1}^{\infty}(1+q^n)^2}{\prod_{n=1}^{\infty}(1-q^n)^2} \\
&= \frac{1}{2\pi i} e^{\frac{\eta_2}{8}} 2i \frac{q^{-\frac{1}{12}} \frac{\mathfrak{f}_2(\tau)^2}{2}}{q^{-\frac{1}{12}}\eta(\tau)^2} \\
&= \frac{1}{2\pi} e^{\frac{\eta_2}{8}} \frac{\mathfrak{f}_2(\tau)^2}{\eta(\tau)^2}.
\end{aligned}$$

For $\sigma(\frac{\tau}{2})$, we again start by rewriting the product

$$\begin{aligned}
\prod_{n=1}^{\infty}(1-q_\tau^{n+\frac{1}{2}})(1-q_\tau^{n-\frac{1}{2}}) &= \frac{1}{1-q_\tau^{\frac{1}{2}}} \prod_{n=1}^{\infty}(1-q_\tau^{n-\frac{1}{2}})^2 \\
&= \frac{q_\tau^{\frac{1}{24}}}{1-q_\tau^{\frac{1}{2}}} \left(q_\tau^{-\frac{1}{48}} \prod_{n=1}^{\infty}(1-q_\tau^{n-\frac{1}{2}}) \right)^2 \\
&= \frac{q_\tau^{\frac{1}{24}}}{1-q_\tau^{\frac{1}{2}}} \mathfrak{f}_1(\tau)^2,
\end{aligned}$$

where in the first equality we used the same trick as in equation (7.1).
At $z = \frac{\tau}{2}$, we have $q_z = e^{i\pi\tau} = q_\tau^{\frac{1}{2}}$. Substituting again $q = q_\tau$, we get

$$\begin{aligned}
\sigma\left(\frac{\tau}{2}\right) &= \frac{1}{2\pi i} e^{\eta_2 \frac{\tau^2}{8}} (q^{\frac{1}{4}} - q^{-\frac{1}{4}}) \prod_{n=1}^{\infty} \frac{(1-q^{n+\frac{1}{2}})(1-q^{n-\frac{1}{2}})}{(1-q^n)^2} \\
&= \frac{1}{2\pi i} e^{\eta_2 \frac{\tau^2}{8}} (q^{\frac{1}{4}} - q^{-\frac{1}{4}}) \frac{\prod_{n=1}^{\infty}(1-q^{n+\frac{1}{2}})(1-q^{n-\frac{1}{2}})}{\prod_{n=1}^{\infty}(1-q^n)^2} \\
&= \frac{1}{2\pi i} e^{\eta_2 \frac{\tau^2}{8}} \frac{q^{\frac{1}{4}} - q^{-\frac{1}{4}}}{1-q^{\frac{1}{2}}} \cdot \frac{q^{\frac{1}{24}} \mathfrak{f}_1(\tau)^2}{q^{-\frac{1}{12}}\eta(\tau)^2} \\
&= -\frac{1}{2\pi i} e^{\eta_2 \frac{\tau^2}{8}} q^{-\frac{1}{8}} \frac{\mathfrak{f}_1(\tau)^2}{\eta(\tau)^2} \\
&= \frac{i}{2\pi} e^{\eta_2 \frac{\tau^2}{8}} q^{-\frac{1}{8}} \frac{\mathfrak{f}_1(\tau)^2}{\eta(\tau)^2}
\end{aligned}$$

where we used $i^{-1} = -i$ and

$$\frac{q^{\frac{1}{4}} - q^{-\frac{1}{4}}}{1-q^{\frac{1}{2}}} \cdot \frac{q^{\frac{1}{24}}}{q^{-\frac{1}{12}}} = \frac{-q^{-\frac{1}{4}}(1-q^{\frac{1}{2}})}{1-q^{\frac{1}{2}}} \cdot \frac{q^{-\frac{5}{24}} q^{\frac{1}{4}}}{q^{-\frac{1}{3}} q^{\frac{1}{4}}} = -q^{-\frac{1}{4}} \frac{1-q^{\frac{1}{2}}}{1-q^{\frac{1}{2}}} \cdot q^{\frac{1}{8}} = -q^{-\frac{1}{8}}.$$

Finally, for $\sigma(\frac{1+\tau}{2})$, we similarly rewrite the product

$$\begin{aligned}\prod_{n=1}^{\infty}(1+q_\tau^{n+\frac{1}{2}})(1+q_\tau^{n-\frac{1}{2}}) &= \frac{1}{1+q_\tau^{\frac{1}{2}}}\prod_{n=1}^{\infty}(1-q_\tau^{n-\frac{1}{2}})^2 \\ &= \frac{q_\tau^{\frac{1}{24}}}{1+q_\tau^{\frac{1}{2}}}\left(q_\tau^{-\frac{1}{48}}\prod_{n=1}^{\infty}(1+q_\tau^{n-\frac{1}{2}})\right)^2 \\ &= \frac{q_\tau^{\frac{1}{24}}}{1+q_\tau^{\frac{1}{2}}}\mathfrak{f}(\tau)^2.\end{aligned}$$

At $z=\frac{1+\tau}{2}$ we have $q_z = e^{\pi i(\tau+1)} = q_\tau^{\frac{1}{2}}e^{i\pi} = -q_\tau^{\frac{1}{2}}$, and substituting again $q=q_\tau$ yields

$$\begin{aligned}\sigma\left(\frac{1+\tau}{2}\right) &= \frac{1}{2\pi i}e^{\eta_2\frac{(1+\tau)^2}{8}}((-q_\tau^{\frac{1}{2}})^{\frac{1}{2}} - (-q_\tau^{\frac{1}{2}})^{-\frac{1}{2}})\prod_{n=1}^{\infty}\frac{(1+q^{n+\frac{1}{2}})(1+q^{n-\frac{1}{2}})}{(1-q^n)^2} \\ &= \frac{1}{2\pi i}e^{\eta_2\frac{(1+\tau)^2}{8}}(iq_\tau^{\frac{1}{4}} - (-iq_\tau^{-\frac{1}{4}}))\frac{\prod_{n=1}^{\infty}(1+q^{n+\frac{1}{2}})(1+q^{n-\frac{1}{2}})}{\prod_{n=1}^{\infty}(1-q^n)^2} \\ &= \frac{1}{2\pi i}e^{\eta_2\frac{(1+\tau)^2}{8}}\frac{i(q_\tau^{\frac{1}{4}}+q_\tau^{-\frac{1}{4}})}{1+q_\tau^{\frac{1}{2}}}\cdot\frac{q^{\frac{1}{24}}\mathfrak{f}(\tau)^2}{q^{-\frac{1}{12}}\eta(\tau)^2} \\ &= \frac{1}{2\pi}e^{\eta_2\frac{(1+\tau)^2}{8}}\frac{q_\tau^{\frac{1}{4}}+q_\tau^{-\frac{1}{4}}}{1+q_\tau^{\frac{1}{2}}}\cdot\frac{q^{\frac{1}{24}}\mathfrak{f}(\tau)^2}{q^{-\frac{1}{12}}\eta(\tau)^2} \\ &= \frac{1}{2\pi}e^{\eta_2\frac{(1+\tau)^2}{8}}q^{-\frac{1}{8}}\frac{\mathfrak{f}(\tau)^2}{\eta(\tau)^2},\end{aligned}$$

where in the last equality we used

$$\frac{q^{\frac{1}{4}}+q^{-\frac{1}{4}}}{1+q^{\frac{1}{2}}}\cdot\frac{q^{\frac{1}{24}}}{q^{-\frac{1}{12}}} = \frac{q^{-\frac{1}{4}}(q^{\frac{1}{2}}+1)}{1+q^{\frac{1}{2}}}\cdot\frac{q^{-\frac{5}{24}}q^{\frac{1}{4}}}{q^{-\frac{1}{3}}q^{\frac{1}{4}}} = q^{-\frac{1}{4}}\frac{1+q^{\frac{1}{2}}}{1+q^{\frac{1}{2}}}\cdot q^{\frac{1}{8}} = q^{-\frac{1}{8}}.$$

This completes the formulas for $\sigma(\frac{1}{2}), \sigma(\frac{\tau}{2})$ and $\sigma(\frac{\tau+1}{2})$. □

The next theorem summarizes the computations carried out in this chapter, providing explicit expressions for the γ_2-function, and in particular for the j-function.
Moreover, it allows us to finally conclude that the q-expansion $j(\tau)$ has integer coefficients, thereby establishing the remaining part of Corollary 4.2.2.

Theorem 7.3.2. *Let $\tau\in\mathbb{H}$. Then $\Delta(\tau) = (2\pi)^{12}\eta(\tau)^{24}$ and*

$$\gamma_2(\tau) = \frac{\mathfrak{f}(\tau)^{24}-16}{\mathfrak{f}(\tau)^8} = \frac{\mathfrak{f}_1(\tau)^{24}+16}{\mathfrak{f}_1(\tau)^8} = \frac{\mathfrak{f}_2(\tau)^{24}+16}{\mathfrak{f}_2(\tau)^8}.$$

Proof. For the first part, we relate the Dedekind η-function and the Weber functions to the Weierstrass $\wp$-function. Let $\wp(z)$ denote the $\wp$-function for the lattice $L = [1, \tau]$, and recall the half-periods $\frac{1}{2}, \frac{\tau}{2}$ and $\frac{\tau+1}{2}$ of L from Lemma 2.3.21. Set $e_1 = \wp(\frac{1}{2}), e_2 = \wp(\frac{\tau}{2})$ and $e_3 = \wp(\frac{1+\tau}{2})$. We prove the following differences:

$$\begin{aligned} e_1 - e_2 &= \pi^2 \eta(\tau)^4 \mathfrak{f}(\tau)^8 \\ e_1 - e_3 &= \pi^2 \eta(\tau)^4 \mathfrak{f}_1(\tau)^8 \\ e_3 - e_2 &= \pi^2 \eta(\tau)^4 \mathfrak{f}_2(\tau)^8 \end{aligned} \tag{7.2}$$

using the Weierstrass σ-function and its properties.
By Proposition 7.2.3, the $\wp$-function can be expressed in terms of the σ-function as

$$\wp(z) - \wp(\omega) = -\frac{\sigma(z+\omega)\sigma(z-\omega)}{\sigma^2(z)\sigma^2(\omega)}$$

for $\omega, z \in \mathbb{C} \backslash L$. We apply this identity to the three pairs of half-periods.
With $z = \frac{1}{2}$ and $\omega = \frac{\tau}{2}$, we have

$$\begin{aligned} e_1 - e_2 = \wp\left(\frac{1}{2}\right) - \wp\left(\frac{\tau}{2}\right) &= -\frac{\sigma(\frac{1+\tau}{2})\sigma(\frac{1-\tau}{2})}{\sigma^2(\frac{1}{2})\sigma^2(\frac{\tau}{2})} = -\frac{\sigma(\frac{1+\tau}{2})\sigma(-\frac{1+\tau}{2}+1)}{\sigma^2(\frac{1}{2})\sigma^2(\frac{\tau}{2})} \\ &= e^{\eta_2(-\frac{1+\tau}{2}+\frac{1}{2})}\frac{\sigma(\frac{1+\tau}{2})\sigma(-\frac{1+\tau}{2})}{\sigma^2(\frac{1}{2})\sigma^2(\frac{\tau}{2})} = -e^{-\eta_2\frac{\tau}{2}}\frac{\sigma^2(\frac{1+\tau}{2})}{\sigma^2(\frac{1}{2})\sigma^2(\frac{\tau}{2})}, \end{aligned}$$

where we used Proposition 7.2.2, and the oddness of $\sigma(z)$ in the last step. Using the formulas from Lemma 7.3.1, we get

$$\begin{aligned} -e^{-\eta_2\frac{\tau}{2}}\frac{\sigma^2(\frac{1+\tau}{2})}{\sigma^2(\frac{1}{2})\sigma^2(\frac{\tau}{2})} &= -e^{-\eta_2\frac{\tau}{2}}\frac{\frac{1}{4\pi^2}e^{\eta_2\frac{(1+\tau)^2}{4}}q^{-\frac{1}{4}}\frac{\mathfrak{f}(\tau)^4}{\eta(\tau)^4}}{\frac{1}{4\pi^2}e^{\frac{\eta_2}{4}}\frac{\mathfrak{f}_2(\tau)^4}{\eta(\tau)^4}\cdot\frac{-1}{4\pi^2}e^{\eta_2\frac{\tau^2}{4}}q^{-\frac{1}{4}}\frac{\mathfrak{f}_1(\tau)^4}{\eta(\tau)^4}} \\ &= -\frac{\frac{1}{4\pi^2}\frac{\mathfrak{f}(\tau)^4}{\eta(\tau)^4}}{\frac{1}{4\pi^2}\frac{\mathfrak{f}_2(\tau)^4}{\eta(\tau)^4}\cdot\frac{-1}{4\pi^2}\frac{\mathfrak{f}_1(\tau)^4}{\eta(\tau)^4}} = 4\pi^2\frac{\eta(\tau)^4\mathfrak{f}(\tau)^4}{\mathfrak{f}_1(\tau)^4\mathfrak{f}_2(\tau)^4}, \end{aligned}$$

as the factor $q^{-\frac{1}{4}}$ cancels and

$$-e^{-\eta_2\frac{\tau}{2}}\frac{e^{\eta_2\frac{(1+\tau)^2}{4}}}{e^{\frac{\eta_2}{4}}\cdot e^{\eta_2\frac{\tau^2}{4}}} = -e^{-\eta_2\frac{\tau}{2}}\frac{e^{\frac{\eta_2}{4}}e^{\eta_2\frac{\tau}{2}}e^{\eta_2\frac{\tau^2}{4}}}{e^{\frac{\eta_2}{4}}\cdot e^{\eta_2\frac{\tau^2}{4}}} = -e^{-\eta_2\frac{\tau}{2}}e^{\eta_2\frac{\tau}{2}} = 1.$$

Using $\mathfrak{f}(\tau)\mathfrak{f}_1(\tau)\mathfrak{f}_2(\tau) = \sqrt{2}$ from Corollary 7.1.4, we conclude

$$e_1 - e_2 = 4\pi^2\frac{\eta(\tau)^4\mathfrak{f}(\tau)^4}{\mathfrak{f}_1(\tau)^4\mathfrak{f}_2(\tau)^4} = 4\pi^2\frac{\eta(\tau)^4\mathfrak{f}(\tau)^4}{\frac{4}{\mathfrak{f}(\tau)^4}} = \pi^2\eta(\tau)^4\mathfrak{f}(\tau)^8.$$

Similarly, with $z = \frac{1}{2}$ and $\omega = \frac{1+\tau}{2}$, we compute

$$\begin{aligned}
e_1 - e_3 = \wp\left(\frac{1}{2}\right) - \wp\left(\frac{1+\tau}{2}\right) &= -\frac{\sigma(1+\frac{\tau}{2})\sigma(-\frac{\tau}{2})}{\sigma^2(\frac{1}{2})\sigma^2(\frac{1+\tau}{2})} \\
&= e^{\eta_2 \frac{\tau+1}{2}} \frac{\sigma(\frac{\tau}{2})\sigma(-\frac{\tau}{2})}{\sigma^2(\frac{1}{2})\sigma^2(\frac{1+\tau}{2})} = -e^{\eta_2 \frac{\tau+1}{2}} \frac{\sigma^2(\frac{\tau}{2})}{\sigma^2(\frac{1}{2})\sigma^2(\frac{1+\tau}{2})} \\
&= -e^{\eta_2 \frac{\tau+1}{2}} \frac{\frac{-1}{4\pi^2} e^{\eta_2 \frac{\tau^2}{4}} q^{-\frac{1}{4}} \frac{\mathfrak{f}_1(\tau)^4}{\eta(\tau)^4}}{\frac{1}{4\pi^2} e^{\frac{\eta_2}{4}} \frac{\mathfrak{f}_2(\tau)^4}{\eta(\tau)^4} \cdot \frac{1}{4\pi^2} e^{\eta_2 \frac{(1+\tau)^2}{4}} q^{-\frac{1}{4}} \frac{\mathfrak{f}(\tau)^4}{\eta(\tau)^4}} \\
&= -\frac{\frac{-1}{4\pi^2} \frac{\mathfrak{f}_1(\tau)^4}{\eta(\tau)^4}}{\frac{1}{4\pi^2} \frac{\mathfrak{f}_2(\tau)^4}{\eta(\tau)^4} \cdot \frac{1}{4\pi^2} \frac{\mathfrak{f}(\tau)^4}{\eta(\tau)^4}} = 4\pi^2 \frac{\eta(\tau)^4 \mathfrak{f}_1(\tau)}{\mathfrak{f}(\tau)^4 \mathfrak{f}_2(\tau)^4} \\
&= 4\pi^2 \frac{\eta(\tau)^4 \mathfrak{f}_1(\tau)^4}{\frac{4}{\mathfrak{f}_1(\tau)^4}} = \pi^2 \eta(\tau)^4 \mathfrak{f}_1(\tau)^8,
\end{aligned}$$

by Proposition 7.2.2, Lemma 7.3.1, Corollary 7.1.4 and as

$$e^{\eta_2 \frac{\tau+1}{2}} \frac{e^{\eta_2 \frac{\tau^2}{4}}}{e^{\frac{\eta_2}{4}} e^{\eta_2 \frac{(1+\tau)^2}{4}}} = \frac{e^{\eta_2 \frac{\tau}{2}} e^{\frac{\eta_2}{2}} e^{\eta_2 \frac{\tau^2}{4}}}{e^{\frac{\eta_2}{4}} e^{\frac{\eta_2}{4}} e^{\eta_2 \frac{\tau}{2}} e^{\eta_2 \frac{\tau^2}{4}}} = 1.$$

Finally, with $z = \frac{1+\tau}{2}$ and $\omega = \frac{\tau}{2}$, we have

$$\begin{aligned}
e_3 - e_2 = \wp\left(\frac{1+\tau}{2}\right) - \wp\left(\frac{\tau}{2}\right) &= -\frac{\sigma(\tau+\frac{1}{2})\sigma(\frac{1}{2})}{\sigma^2(\frac{1+\tau}{2})\sigma^2(\frac{\tau}{2})} = e^{\eta_1 \frac{\tau+1}{2}} \frac{\sigma^2(\frac{1}{2})}{\sigma^2(\frac{1+\tau}{2})\sigma^2(\frac{\tau}{2})} \\
&= e^{\eta_1 \frac{\tau+1}{2}} \frac{\frac{1}{4\pi^2} e^{\frac{\eta_2}{4}} \frac{\mathfrak{f}_2(\tau)^4}{\eta(\tau)^4}}{\frac{1}{4\pi^2} e^{\eta_2 \frac{(1+\tau)^2}{4}} q^{-\frac{1}{4}} \frac{\mathfrak{f}(\tau)^4}{\eta(\tau)^4} \cdot \frac{-1}{4\pi^2} e^{\eta_2 \frac{\tau^2}{4}} q^{-\frac{1}{4}} \frac{\mathfrak{f}_1(\tau)^4}{\eta(\tau)^4}} \\
&= e^{(\eta_1 - \eta_2\tau)\frac{\tau+1}{2}} \frac{\frac{1}{4\pi^2} \frac{\mathfrak{f}_2(\tau)^4}{\eta(\tau)^4}}{\frac{1}{4\pi^2} q^{-\frac{1}{2}} \frac{\mathfrak{f}(\tau)^4}{\eta(\tau)^4} \cdot \frac{-1}{4\pi^2} \frac{\mathfrak{f}_1(\tau)^4}{\eta(\tau)^4}} \\
&= -4\pi^2 e^{(\eta_1 - \eta_2\tau)\frac{\tau+1}{2}} q^{\frac{1}{2}} \frac{\eta(\tau)^4 \mathfrak{f}_2(\tau)^4}{\mathfrak{f}(\tau)^4 \mathfrak{f}_1(\tau)^4} \\
&= -4\pi^2 e^{-2\pi i \frac{\tau+1}{2}} e^{\pi i} \frac{\eta(\tau)^4 \mathfrak{f}_2(\tau)^4}{\frac{4}{\mathfrak{f}_2(\tau)^4}} \\
&= \pi^2 e^{-\pi i \tau} e^{-\pi i} \eta(\tau)^4 \mathfrak{f}_2(\tau)^8 \\
&= \pi^2 \eta(\tau)^4 \mathfrak{f}_2(\tau)^8,
\end{aligned}$$

again by Proposition 7.2.2, Lemma 7.3.1, Corollary 7.1.4, using $\eta_2\tau - \eta_1 = 2\pi i$ and $e^{i\pi} = -1$, and as

$$e^{\eta_1 \frac{\tau+1}{2}} \frac{e^{\frac{\eta_2}{4}}}{e^{\eta_2 \frac{(1+\tau)^2}{4}} e^{\eta_2 \frac{\tau^2}{4}}} = e^{\eta_1 \frac{\tau+1}{2}} \frac{e^{\frac{\eta_2}{4}}}{e^{\frac{\eta_2}{4}} e^{\eta_2 \frac{\tau}{2}} e^{\eta_2 \frac{\tau^2}{4}} e^{\eta_2 \frac{\tau^2}{4}}} = e^{\eta_1 \frac{\tau+1}{2}} \frac{1}{e^{\eta_2 \frac{\tau}{2}} e^{\eta_2 \frac{\tau^2}{2}}} = e^{(\eta_1 - \eta_2\tau)\frac{\tau+1}{2}}.$$

Now, using these differences, we can express the discriminant $\Delta(L) = \Delta(\tau)$ of the lattice $L = [1, \tau]$ in terms of the Dedekind η-function by applying the connection between the half-periods of a lattice and its discriminant explored in the proof of Theorem 2.3.22:

$$\begin{aligned}\Delta(\tau) &= 16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2 \\ &= 16(\pi^2\eta(\tau)^4\mathfrak{f}(\tau)^8)^2(\pi^2\eta(\tau)^4\mathfrak{f}_1(\tau)^8)^2(\pi^2\eta(\tau)^4\mathfrak{f}_2(\tau)^8)^2 \\ &= 2^4\pi^{12}\eta(\tau)^{24}\mathfrak{f}(\tau)^{16}\mathfrak{f}_1(\tau)^{16}\mathfrak{f}_2(\tau)^{16} \\ &= (2\pi)^{12}\eta(\tau)^{24},\end{aligned}$$

where the last equality follows from Corollary 7.1.4.
For the second part, note that $\eta(\tau)$ is strictly positive for purely imaginary $\tau \in \mathbb{H}$. Indeed, for $\tau = iy$, we have

$$\eta(iy) = e^{\frac{2\pi i^2 y}{24}} \prod_{n=1}^{\infty}(1 - e^{\frac{2\pi i^2 yn}{24}}) = e^{\frac{-\pi y}{12}} \prod_{n=1}^{\infty}(1 - e^{-\frac{\pi yn}{12}}) \in \mathbb{R}_{>0}.$$

It follows that the expression $\Delta(\tau) = (2\pi)^{12}\eta(\tau)^{24}$ is not only real, as already established in Lemma 6.1.3, but also strictly positive for purely imaginary τ. Hence, its cube root is well-defined and given explicitly by

$$\sqrt[3]{\Delta(\tau)} = (2\pi)^4\eta(\tau)^8.$$

By definition of $\gamma_2(\tau)$ in Section 6.1, this gives

$$\gamma_2(\tau) = \sqrt[3]{j(\tau)} = 12\frac{g_2(\tau)}{\sqrt[3]{\Delta(\tau)}} = 12\frac{g_2(\tau)}{(2\pi)^4\eta(\tau)^8} = \frac{3g_2(\tau)}{4\pi^4\eta(\tau)^8}.$$

Now, we express $g_2(\tau)$ in terms of the Dedekind η-fuction and Weber functions. The idea is to first relate $g_2(\tau)$ to the e_i's and then apply the above differences (7.2).
Recall from Theorem 2.3.22, that the e_i's are roots of the polynomial $4x^3 - g_2(\tau)x - g_3(\tau)$ and satisfy $e_1e_2 + e_1e_3 + e_2e_3 = -\frac{g_2(\tau)}{4}$ and $e_1 + e_2 + e_3 = 0$. We compute

$$\begin{aligned}0 &= 4(e_1 + e_2 + e_3)^2 \\ &= 4(e_1^2 + e_2^2 + e_3^2) + 8(e_1e_2 + e_1e_3 + e_2e_3) \\ &= 4((e_2 - e_1)^2 - (e_2 - e_3)(e_3 - e_1)) + 12(e_1e_2 + e_1e_3 + e_2e_3) \\ &= 4((e_2 - e_1)^2 - (e_2 - e_3)(e_3 - e_1)) + 12\left(-\frac{g_2(\tau)}{4}\right) \\ &= 4((e_2 - e_1)^2 - (e_2 - e_3)(e_3 - e_1)) - 3g_2(\tau),\end{aligned}$$

which yields $3g_2(\tau) = 4((e_2 - e_1)^2 - (e_2 - e_3)(e_3 - e_1))$. Using the differences (7.2) gives

$$\begin{aligned}3g_2(\tau) &= 4((-\pi^2\eta(\tau)^4\mathfrak{f}(\tau)^8)^2 - \pi^2\eta(\tau)^4\mathfrak{f}_2(\tau)^8\pi^2\eta(\tau)^4\mathfrak{f}_1(\tau)^8) \\ &= 4\pi^4\eta(\tau)^8(\mathfrak{f}(\tau)^{16} - \mathfrak{f}_2(\tau)^8\mathfrak{f}_1(\tau)^8).\end{aligned}$$

Hence, substituting this into the formula for $\gamma_2(\tau)$ yields

$$\begin{aligned}\gamma_2(\tau) &= \frac{4\pi^4\eta(\tau)^8(\mathfrak{f}(\tau)^{16} - \mathfrak{f}_2(\tau)^8\mathfrak{f}_1(\tau)^8)}{4\pi^4\eta(\tau)^8} \\ &= \mathfrak{f}(\tau)^{16} - \mathfrak{f}_2(\tau)^8\mathfrak{f}_1(\tau)^8 \\ &= \mathfrak{f}(\tau)^{16} - \frac{16}{\mathfrak{f}(\tau)} \\ &= \frac{\mathfrak{f}(\tau)^{24} - 16}{\mathfrak{f}(\tau)^8},\end{aligned}$$

where we used Corollary 7.1.4 in the third equality.
To obtain the remaining two formulas, note that the expression

$$4((e_2 - e_1)^2 - (e_2 - e_3)(e_3 - e_1)) = e_1^2 + e_2^2 + e_3^2 + 2(e_1e_2 + e_2e_3 + e_1e_3)$$

is symmetric in the e_i. By permuting the indices, we obtain two additional equations:

$$\begin{aligned}3g_2(\tau) &= 4((e_1 - e_3)^2 - (e_1 - e_2)(e_2 - e_3)) \\ 3g_2(\tau) &= 4((e_3 - e_2)^2 - (e_3 - e_1)(e_1 - e_2)).\end{aligned}$$

Again, using the differences (7.2) together with Corollary 7.1.4, we obtain

$$\begin{aligned}3g_2(\tau) &= 4((e_1 - e_3)^2 - (e_1 - e_2)(e_2 - e_3)) \\ &= 4((\pi^2\eta(\tau)^4\mathfrak{f}_1(\tau)^8)^2 - \pi^2\eta(\tau)^4\mathfrak{f}(\tau)^8(-\pi^2\eta(\tau)^4\mathfrak{f}_2(\tau)^8) \\ &= 4\pi^4\eta(\tau)^8(\mathfrak{f}_1(\tau)^{16} + \mathfrak{f}(\tau)^8\mathfrak{f}_2(\tau)^8) \\ &= 4\pi^4\eta(\tau)^8\left(\mathfrak{f}_1(\tau)^{16} + \frac{16}{\mathfrak{f}_1(\tau)}\right) \\ &= 4\pi^4\eta(\tau)^8\frac{\mathfrak{f}_1(\tau)^{24} + 16}{\mathfrak{f}_1(\tau)^8},\end{aligned}$$

and similarly,

$$\begin{aligned}3g_2(\tau) &= 4((e_3 - e_2)^2 - (e_3 - e_1)(e_1 - e_2)) \\ &= 4((\pi^2\eta(\tau)^4\mathfrak{f}_2(\tau)^8)^2 - (-\pi^2\eta(\tau)^4\mathfrak{f}_1(\tau)^8)\pi^2\eta(\tau)^4\mathfrak{f}(\tau)^8) \\ &= 4\pi^4\eta(\tau)^8(\mathfrak{f}_2(\tau)^{16} + \mathfrak{f}_1(\tau)^8\mathfrak{f}(\tau)^8) \\ &= 4\pi^4\eta(\tau)^8\left(\mathfrak{f}_2(\tau)^{16} + \frac{16}{\mathfrak{f}_2(\tau)}\right) \\ &= 4\pi^4\eta(\tau)^8\frac{\mathfrak{f}_2(\tau)^{24} + 16}{\mathfrak{f}_2(\tau)^8}.\end{aligned}$$

Substituting these expressions into $\gamma_2(\tau)$ yields the two remaining formulas:

$$\gamma_2(\tau) = \frac{\mathfrak{f}_1(\tau)^{24} + 16}{\mathfrak{f}_1(\tau)^8} = \frac{\mathfrak{f}_2(\tau)^{24} + 16}{\mathfrak{f}_2(\tau)^8}.$$

□

Corollary 7.3.3. *The q-expansion of the j-function has integer coefficients.*

Proof. By definition, $\gamma_2(\tau)$ is the unique real cube root of $j(\tau)$ for purely imaginary τ (see Section 6.1), so $\gamma_2(\tau) = \sqrt[3]{j(\tau)}$. Using the formulas from the previous theorem, we obtain

$$\begin{aligned} j(\tau) = \gamma_2(\tau)^3 &= \frac{\mathfrak{f}(\tau)^{24} - 16}{\mathfrak{f}(\tau)^8} \cdot \frac{\mathfrak{f}_1(\tau)^{24} + 16}{\mathfrak{f}_1(\tau)^8} \cdot \frac{\mathfrak{f}_2(\tau)^{24} + 16}{\mathfrak{f}_2(\tau)^8} \\ &= \frac{\mathfrak{f}(\tau)^{24}\mathfrak{f}_1(\tau)^{24}\mathfrak{f}_2(\tau)^{24} + 16P(\mathfrak{f}(\tau), \mathfrak{f}_1(\tau), \mathfrak{f}_2(\tau))}{\mathfrak{f}(\tau)^8\mathfrak{f}_1(\tau)^8\mathfrak{f}_2(\tau)^8}, \end{aligned}$$

where $P(\mathfrak{f}(\tau), \mathfrak{f}_1(\tau), \mathfrak{f}_2(\tau))$ is the polynomial

$$\begin{aligned} P(\mathfrak{f}(\tau), \mathfrak{f}_1(\tau), \mathfrak{f}_2(\tau)) = {} & \mathfrak{f}(\tau)^{24}\mathfrak{f}_1(\tau)^{24} + \mathfrak{f}(\tau)^{24}\mathfrak{f}_2(\tau)^{24} - \mathfrak{f}_1(\tau)^{24}\mathfrak{f}_2(\tau)^{24} \\ & + 16\mathfrak{f}(\tau)^{24} - 16\mathfrak{f}_1(\tau)^{24} - 16\mathfrak{f}_2(\tau)^{24} - 16 \end{aligned}$$

in the Weber functions $\mathfrak{f}(\tau), \mathfrak{f}_1(\tau)$ and $\mathfrak{f}_2(\tau)$ with integer coefficients. Using the relation $\mathfrak{f}(\tau)\mathfrak{f}_1(\tau)\mathfrak{f}_2(\tau) = \sqrt{2}$ from Corollary 7.1.4, we rewrite the nominator and denominator as powers of $\sqrt{2}$, giving

$$\begin{aligned} j(\tau) &= \frac{\sqrt{2}^{24} + 16P(\mathfrak{f}(\tau), \mathfrak{f}_1(\tau), \mathfrak{f}_2(\tau))}{\sqrt{2}^8} \\ &= 256 + P(\mathfrak{f}(\tau), \mathfrak{f}_1(\tau), \mathfrak{f}_2(\tau)). \end{aligned}$$

Substituting the three functions by their q-product expansions from Proposition 7.1.3,

$$\begin{aligned} \mathfrak{f}(\tau) &= q^{-\frac{1}{48}} \prod_{n=1}^{\infty}(1 + q^{n-\frac{1}{2}}) \\ \mathfrak{f}_1(\tau) &= q^{-\frac{1}{48}} \prod_{n=1}^{\infty}(1 - q^{n-\frac{1}{2}}) \\ \mathfrak{f}_2(\tau) &= \sqrt{2}\, q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1 + q^n), \end{aligned}$$

into the polynomial P yields a power series expansion in q with integer and rational exponents. The coefficients of this series are integers: indeed, both $\mathfrak{f}(\tau)$ and $\mathfrak{f}_1(\tau)$ have integer coefficients and so $\mathfrak{f}(\tau)^{24}$ and $\mathfrak{f}_1(\tau)^{24}$ do as well. In the case of $\mathfrak{f}_2(\tau)$, raising the prefactor $\sqrt{2}$ to the power of 24, allows also $\mathfrak{f}_2(\tau)^{24}$ to have integer coefficients. Therefore, combining these expansions through addition and multiplication preserves integrality, and the resulting power series has integer coefficients.
Now it remains to compute its leading power. The functions $\mathfrak{f}(\tau)$ and $\mathfrak{f}_1(\tau)$ both start with $q^{-\frac{1}{48}}$, while $\mathfrak{f}_2(\tau)$ starts with $q^{\frac{1}{24}}$. Consequently, both $\mathfrak{f}(\tau)^{24}\mathfrak{f}_2(\tau)^{24}$ and $\mathfrak{f}_1(\tau)^{24}\mathfrak{f}_2(\tau)^{24}$ start with $q^{\frac{1}{2}}$, while $\mathfrak{f}(\tau)^{24}\mathfrak{f}_1(\tau)^{24}$ starts with q^{-1}.

Finally, since we have already established in Section 4.2 that the j-function admits a q-expansion

$$j(\tau) = \sum_{n=-\infty}^{\infty} c_n q^n$$

with integer powers, the linear independence of the monomials $\{q^r \mid r \text{ rational}\}$ over $\mathbb{C}$ implies that all coefficients of actual rational powers of q must vanish, leaving only integer powers beginning with q^{-1}. Hence, the resulting power series has integer coefficients, which proves the theorem and completes the proof of Corollary 4.2.2. □

8 Conclusion

This final chapter brings together the results developed throughout this work and culminates in the main conclusion. Building on the formulas for $\gamma_2(\tau)$ derived in the previous chapter, we make the arithmetic of class number one fields fully explicit. These expressions, originally introduced to establish the algebraic properties of γ_2, prove particularly useful for the explicit computations carried out here. In doing so, the analytic and algebraic aspects of complex multiplication meet in concrete computations that reveal the remarkable near-integrality of $e^{\pi\sqrt{163}}$.
The chapter is organized into two sections. In the first, we employ the formulas for $\gamma_2(\tau)$ to numerically approximate its values and thereby obtain explicit results for $j(E)$. While this step is not strictly necessary - the integrality of $j(E)$ already follows from Corollary 5.6.4 - it requires only minimal additional effort and provides a concrete illustration of the theoretical results. The second section then combines these computations to demonstrate that $e^{\pi\sqrt{163}}$ lies extraordinarily close to an integer, thereby concluding the central line of reasoning that has guided this work.

The first section of this chapter follows [3, §12 B–C], with additional explanations and proofs, while the second section presents original conclusions and exposition.

8.1 Numerical computation of γ_2

We now reach the stage where our theoretical framework meets computation. With $\gamma_2(\tau)$ expressed via Weber functions and their transformation properties in hand, we can numerically approximate its values for each order of class number one, directly linking these algebraic results to the arithmetic of the corresponding j-invariants.

Recall from Corollary 5.7.6 that there are exactly thirteen orders in imaginary quadratic number fields of class number one, corresponding to the discriminants

$$D = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163.$$

According to Corollary 5.6.4, the j-invariants $j(E) = j(\tau)$ of elliptic curves E with complex multiplication by such orders are integers. Moreover, for the ten discriminants not divisible by 3, Corollary 6.2.4 shows that these values are perfect cubes. Since γ_2 is, by definition, the unique real cube root of the j-function, it follows that in these cases $\gamma_2(\tau_0) = \sqrt[3]{j(\tau_0)}$ is an integer, for a suitably chosen element of the order (as in Theorem 6.2.1). Rather than evaluating $\gamma_2(\tau_0)$ directly, we approximate it using the expressions in terms of the Weber functions derived in Theorem 7.3.2. Since $\gamma_2(\tau_0)$ is an integer, an approximation within half an integer then suffices to determine its value uniquely.

As mentioned in the previous chapter, the Dedekind η-function and the Weber functions satisfy only a weak form of modularity for the full modular group. We will now examine their transformation properties, which follow directly from Theorem 7.3.2.

Proposition 8.1.1. *Let $\zeta_n = e^{2\pi i/n}$ be a primitive n-th root of unity. Then we have*

$$\begin{aligned}\eta(\tau+1) &= \zeta_{24}\eta(\tau)\\ \eta\left(-\frac{1}{\tau}\right) &= \sqrt{-i\tau}\eta(\tau),\end{aligned}$$

where the square root is chosen to be positive on the imaginary axis. Moreover,

$$\begin{aligned}\mathfrak{f}(\tau+1) &= \zeta_{48}^{-1}\mathfrak{f}_1(\tau)\\ \mathfrak{f}_1(\tau+1) &= \zeta_{48}^{-1}\mathfrak{f}(\tau)\\ \mathfrak{f}_2(\tau+1) &= \zeta_{24}\mathfrak{f}_2(\tau),\end{aligned}$$

and

$$\begin{aligned}\mathfrak{f}\left(-\frac{1}{\tau}\right) &= \mathfrak{f}(\tau)\\ \mathfrak{f}_1\left(-\frac{1}{\tau}\right) &= \mathfrak{f}_2(\tau)\\ \mathfrak{f}_2\left(-\frac{1}{\tau}\right) &= \mathfrak{f}_1(\tau).\end{aligned}$$

Proof. We start with the transformation properties of the Dedekind η-function. The first formula follows immediately from the definition of $\eta(\tau)$. For the second formula, we consider the discriminant of a lattice L in $\mathbb{C}$, given by $\Delta(L) = g_2(L)^3 - 27g_3(L)^2$. In the proof of Theorem 2.5.5, we showed that for any non-zero $\lambda \in \mathbb{C}$, the functions g_2 and g_3 scale as $g_2(\lambda L) = \lambda^{-4}g_2(L)$ and $g_3(\lambda L) = \lambda^{-6}g_3(L)$, which implies that

$$\Delta(\lambda L) = \lambda^{-12}\Delta(L).$$

Now let $L = [1, \tau]$, so that $\Delta(L) = \Delta(\tau)$. By applying the above with $\lambda = \tau^{-1}$, we get

$$\Delta\left(-\frac{1}{\tau}\right) = \Delta\left(\left[1, -\frac{1}{\tau}\right]\right) = \Delta(\tau^{-1}[1,\tau]) = \tau^{12}\Delta([1,\tau]) = \tau^{12}\Delta(\tau).$$

Using the formula $\Delta(\tau) = (2\pi)^{12}\eta(\tau)^{24}$ from Theorem 7.3.2 and taking 24th roots on both sides yields

$$\eta\left(-\frac{1}{\tau}\right) = \zeta\sqrt{-i\tau}\eta(\tau),$$

for some 24th root of unity ζ. Observe that for purely imaginary τ, the quantities $\eta(\tau), \eta(-\frac{1}{\tau})$ and $\sqrt{-i\tau}$ are positive real numbers. Hence, both sides of the equation are real and positive, which forces $\zeta = 1$ and gives the second formula.

Turning to the Weber functions, we begin with the transformation under $\tau \mapsto \tau + 1$. Their definitions and the first transformation property of the η-function give

$$\begin{aligned}
\mathfrak{f}(\tau+1) &= \zeta_{48}^{-1}\frac{\eta(\frac{\tau+2}{2})}{\eta(\tau+1)} = \zeta_{48}^{-1}\frac{\eta(\frac{\tau}{2}+1)}{\eta(\tau+1)} = \zeta_{48}^{-1}\frac{\zeta_{24}\ \eta(\frac{\tau}{2})}{\zeta_{24}\ \eta(\tau)} = \zeta_{48}^{-1}\mathfrak{f}_1(\tau)\\
\mathfrak{f}_1(\tau+1) &= \frac{\eta(\frac{\tau+1}{2})}{\eta(\tau+1)} = \frac{\eta(\frac{\tau+1}{2})}{\zeta_{24}\eta(\tau)} = \zeta_{48}^{-1}\left(\zeta_{48}^{-1}\frac{\eta(\frac{\tau+1}{2})}{\eta(\tau)}\right) = \zeta_{48}^{-1}\mathfrak{f}(\tau)\\
\mathfrak{f}_2(\tau+1) &= \sqrt{2}\ \frac{\eta(2\tau+2)}{\eta(\tau+1)} = \sqrt{2}\ \frac{\zeta_{24}^2\eta(2\tau)}{\zeta_{24}\eta(\tau)} = \zeta_{24}\mathfrak{f}_2(\tau).
\end{aligned}$$

For the transformation behaviour under $\tau \mapsto -\frac{1}{\tau}$, their definitions together with the second transformation property of the η-function yield

$$\mathfrak{f}_1\left(-\frac{1}{\tau}\right) = \frac{\eta(-\frac{1}{2\tau})}{\eta(-\frac{1}{\tau})} = \frac{\sqrt{-2i\tau}\eta(2\tau)}{\sqrt{-i\tau}\eta(\tau)} = \sqrt{2}\ \frac{\eta(2\tau)}{\eta(\tau)} = \mathfrak{f}_2(\tau).$$

Replacing τ with $-\frac{1}{\tau}$ in this computation gives $\mathfrak{f}_2(-\frac{1}{\tau}) = \mathfrak{f}_1(\tau)$. Finally, combining these two formulas and using Corollary 7.1.4, we obtain

$$\mathfrak{f}\left(-\frac{1}{\tau}\right) = \frac{\sqrt{2}}{\mathfrak{f}_1(-\frac{1}{\tau})\mathfrak{f}_2(-\frac{1}{\tau})} = \frac{\sqrt{2}}{\mathfrak{f}_2(\tau)\mathfrak{f}_1(\tau)} = \mathfrak{f}(\tau).$$

□

In preparation for the numerical evaluation, denote by $\lfloor \bullet \rceil$ the *nearest integer function*, defined as follows: for a real number $x \notin \mathbb{Z} + \frac{1}{2}$, the value $\lfloor x \rceil$ is the integer closest to x, and if $x \in \mathbb{Z} + \frac{1}{2}$, it is defined to be the integer greater than x.

We now proceed to state the theorem that provides an explicit numerical approximation for $\gamma_2(\tau_0)$. As already mentioned at the beginning of this section, τ_0 is an appropriately chosen element of an order $\mathcal{O}$ of discriminant D not divisible by 3 in an imaginary quadratic number field. More precisely, Theorem 6.2.1 helps us identify the correct choice of τ_0 associated to $\mathcal{O}$:

$$\tau_0 = \begin{cases} \sqrt{d} & \text{if } D = 4d \equiv 0 \bmod 4 \\ \frac{3+\sqrt{d}}{2} & \text{if } D = d \equiv 1 \bmod 4. \end{cases}$$

To numerically evaluate $\gamma_2(\tau_0)$, we work with the real parameter $|q|^2 = e^{-4\pi \operatorname{Im}(\tau_0)}$ in place of the complex quantity $q = e^{2\pi i \tau_0}$. This is convenient because, for odd discriminants, one has $q = -e^{-\pi\sqrt{|d|}}$, so fractional powers such as $q^{-\frac{1}{6}}$ become multivalued, whereas $|q|^2 \in (0,1)$ is single-valued and preserves the exponential decay of the q-series. Moreover, the identities relating $\gamma_2(\tau_0)$ to Weber functions involve powers of q^2, so $|q|^2$ is the natural parameter governing convergence. Since all analytic estimates used later depend only on the magnitudes $|q^n|$, replacing q by $|q|^2$ does not affect the validity of the approximation.

Theorem 8.1.2. *Let $\mathcal{O}$ be an order in an imaginary quadratic number field K of discriminant D with $3 \nmid D$, and write $\mathcal{O} = [1, \tau_0]$. Then*

$$\gamma_2(\tau_0) = \begin{cases} \lfloor 256 q^{\frac{2}{3}} + q^{-\frac{1}{3}} \rceil & \text{if } \tau_0 = \sqrt{d} \\ \lfloor 256 |q|^{\frac{2}{3}} - |q|^{-\frac{1}{3}} \rceil & \text{if } \tau_0 = \frac{3+\sqrt{d}}{2}, \end{cases}$$

where $|q| = |e^{2\pi i \tau_0}| = e^{-2\pi \operatorname{Im}(\tau_0)}$, and $\lfloor \bullet \rceil$ denotes the nearest integer function.

For clarity, note that the expression $\lfloor 256|q|^{\frac{2}{3}} - |q|^{-\frac{1}{3}} \rceil$ arises by rewriting

$$\lfloor 256(|q|^2)^{\frac{1}{3}} - (|q|^2)^{-\frac{1}{6}} \rceil$$

in terms of $|q|$. The latter form makes the dependence on the real parameter $|q|^2 = e^{-4\pi \operatorname{Im}(\tau_0)}$ explicit and reflects the change of variables used in the proof.

Proof. We begin with the case $\tau_0 = \sqrt{d}$, which occurs when the discriminant is even, i.e. when $D = 4d \equiv 0 \bmod 4$ as in Theorem 6.2.1. In this case, $d = -1, -2, -4$ or -7. (Note that we exclude $d = -3$ here, since this corresponds to the discriminant $D = -12$, which is divisible by 3 and thus excluded by our assumption $3 \nmid D$.) Using Theorem 7.3.2, we express $\gamma_2(\tau)$ in terms of the Weber function $\mathfrak{f}_2(\tau)$ as

$$\gamma_2(\sqrt{d}) = \mathfrak{f}_2(\sqrt{d})^{16} + \frac{16}{\mathfrak{f}_2(\sqrt{d})^8}.$$

In order to estimate $\mathfrak{f}_2(\sqrt{d})$, recall its q-product expansion $\mathfrak{f}_2(\sqrt{d}) = \sqrt{2}\, q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1+q^n)$ given by Proposition 7.1.3, where $q = e^{2\pi i \tau_0}$. Note that in this case, the parameter $q = e^{2\pi i \tau_0} = e^{-2\pi\sqrt{|d|}} \in \mathbb{R}_{>0}$ is already real and positive. Therefore, as explained above, no substitution by $|q|^2$ in the computation is needed. To estimate the infinite product, we use the inequality $1 + x \leq e^x$ for $x \in \mathbb{R}$ and the geometric series formula:

$$1 < \prod_{n=1}^{\infty}(1+q^n) < \prod_{n=1}^{\infty} e^{q^n} = e^{\sum_{n=1}^{\infty} q^n} = e^{\frac{1}{1-q} - q^0} = e^{\frac{q}{1-q}}.$$

Since $q = e^{-2\pi\sqrt{|d|}} \leq e^{-2\pi} \approx 0.0019$, we estimate the exponent by

$$\frac{q}{1-q} \leq \frac{q}{1-e^{-2\pi}} < 1.002q.$$

Combining these facts, we obtain the inequalities

$$\sqrt{2}\, q^{\frac{1}{24}} < \mathfrak{f}_2(\sqrt{d}) < \sqrt{2}\, q^{\frac{1}{24}} e^{1.002q},$$

which lead to the following bounds for the powers of $\mathfrak{f}_2(\sqrt{d})$:

$$256 q^{\frac{2}{3}} < \mathfrak{f}_2(\sqrt{d})^{16} < 256 q^{\frac{2}{3}} e^{16.032q}$$
$$16 q^{\frac{1}{3}} < \mathfrak{f}_2(\sqrt{d})^{8} < 16 q^{\frac{1}{3}} e^{8.016q}.$$

This yields upper and lower bounds for $\gamma_2(\sqrt{d})$:

$$256q^{\frac{2}{3}} + q^{-\frac{1}{3}}e^{-8.016q} < \gamma_2(\sqrt{d}) < 256q^{\frac{2}{3}}e^{16.032q} + q^{-\frac{1}{3}}.$$

To evaluate the sharpness of these bounds, consider their difference

$$\begin{aligned} E &= 256q^{\frac{2}{3}}e^{16.032q} + q^{-\frac{1}{3}} - (256q^{\frac{2}{3}} + q^{-\frac{1}{3}}e^{-8.016q}) \\ &= 256q^{\frac{2}{3}}(e^{16.032q} - 1) + q^{-\frac{1}{3}}(1 - e^{-8.016q}). \end{aligned}$$

Using the inequality $1 - e^{-x} < \frac{x}{1-x}$ for $0 < x < 1$, we estimate

$$\begin{aligned} E &< 256q^{\frac{2}{3}}(e^{16.032q} - 1) + q^{-\frac{1}{3}}\frac{8.016q}{1 - 8.016q} \\ &= 256q^{\frac{2}{3}}(e^{16.032q} - 1) + \frac{8.016q^{\frac{2}{3}}}{1 - 8.016q}, \end{aligned}$$

which is an increasing function in q. Then $q \leq e^{-2\pi} \approx 0.0019$ implies

$$E < 0.25.$$

Since $3 \nmid D$, the j-invariant $j(\sqrt{d})$ of the corresponding elliptic curve is an integer and a perfect cube (Corollary 6.2.4). By definition of γ_2, we have $\gamma_2(\sqrt{d})^3 = j(\sqrt{d})$, and hence $\gamma_2(\sqrt{d})$ itself is an integer. Therefore, because the total width of the estimate is less than $\frac{1}{2}$, the above computation implies that $\lfloor x \rceil = \gamma_2(\sqrt{d})$ for all x lying between the upper and lower bound of $\gamma_2(\sqrt{d})$. In particular, the value $256q^{\frac{2}{3}} + q^{-\frac{1}{3}}$ lies between these bounds, proving the first statement.

Now we turn to the case $\tau_0 = \frac{3+\sqrt{d}}{2}$, which arises when the discriminant is odd, i.e. when $D = d \equiv 1 \bmod 4$ by Theorem 6.2.1. In this case, $d = -7, -11, -19, -43, -67$ or -163. (Note that we exclude $d = -3$ and $d = -27$, since these correspond to the discriminants $D = -3$ and $D = -27$, which are divisible by 3 and thus excluded by our assumption $3 \nmid D$.) As before, we use the Theorem 7.3.2 to write

$$\gamma_2(\tau_0) = \mathfrak{f}_2(\tau_0)^{16} + \frac{16}{\mathfrak{f}_2(\tau_0)^8}.$$

However, the more complicated form of τ_0 makes a direct estimation of $\mathfrak{f}_2(\tau_0)$ less convenient. We simplify this by shifting the evaluation to $2\tau_0$ via the relation

$$\mathfrak{f}_2(\tau_0) = \frac{\sqrt{2}}{\mathfrak{f}_1(2\tau_0)}$$

from Theorem 7.1.4, where the expansions now involve integral powers. By applying the transformation properties from Proposition 8.1.1 to $\mathfrak{f}_1(2\tau_0)$, we obtain

$$\begin{aligned} \mathfrak{f}_1(2\tau_0) &= \mathfrak{f}_1(3 + \sqrt{d}) = \zeta_{48}^{-1}\mathfrak{f}(2 + \sqrt{d}) \\ &= \zeta_{48}^{-2}\mathfrak{f}_1(1 + \sqrt{d}) = \zeta_{48}^{-3}\mathfrak{f}(\sqrt{d}) = \zeta_{16}^{-1}\mathfrak{f}(\sqrt{d}), \end{aligned}$$

where ζ_n denotes a primitive n-th root of unity. Hence,

$$\mathfrak{f}_2(\tau_0) = \frac{\sqrt{2}\,\zeta_{16}}{\mathfrak{f}(\sqrt{d})},$$

and therefore

$$\gamma_2(\tau_0) = \frac{256}{\mathfrak{f}(\sqrt{d})^{16}} - \mathfrak{f}(\sqrt{d})^8.$$

We now proceed analogously to the first case by estimating $\mathfrak{f}(\sqrt{d})$ via its q-product expansion $\mathfrak{f}(\sqrt{d}) = q^{-\frac{1}{48}}\prod_{n=1}^{\infty}(1+q^{n-\frac{1}{2}})$, where, as discussed above, we evaluate all infinite products and powers using the parameter $|q|^2 = e^{-4\pi\,\mathrm{Im}(\tau_0)} \in \mathbb{R}_{>0}$ to ensure well-defined numerical approximations. Using $1 + x \le e^x$ for $x \in \mathbb{R}$, we get

$$1 < \prod_{n=1}^{\infty}(1+(|q|^2)^{n-\frac{1}{2}}) < \prod_{n=1}^{\infty}(1+(|q|^2)^n) < \prod_{n=1}^{\infty} e^{|q|^{2n}} = e^{\frac{|q|^2}{1-|q|^2}} < e^{1.002|q|^2},$$

where we estimated $|q|^2 = e^{-4\pi\,\mathrm{Im}(\tau_0)} = e^{-2\pi\sqrt{|d|}} \le e^{-2\pi}$, as before. Thus,

$$|q|^{-\frac{1}{24}} = (|q|^2)^{-\frac{1}{48}} < \mathfrak{f}(\sqrt{d}) < (|q|^2)^{-\frac{1}{48}} e^{1.002|q|^2} = |q|^{-\frac{1}{24}} e^{1.002|q|^2},$$

and raising to powers yields

$$\begin{aligned} |q|^{-\frac{1}{3}} = (|q|^2)^{-\frac{1}{6}} &< \mathfrak{f}(\sqrt{d})^8 < (|q|^2)^{-\frac{1}{6}} e^{8.016|q|^2} = |q|^{-\frac{1}{3}} e^{8.016|q|^2} \\ |q|^{-\frac{2}{3}} = (|q|^2)^{-\frac{1}{3}} &< \mathfrak{f}(\sqrt{d})^{16} < (|q|^2)^{-\frac{1}{3}} e^{16.032|q|^2} = |q|^{-\frac{2}{3}} e^{16.032|q|^2}. \end{aligned}$$

We obtain the following bounds for $\gamma_2(\tau_0)$ in terms of the real parameter $|q|^2$:

$$256|q|^{\frac{2}{3}} e^{-16.032|q|^2} - |q|^{-\frac{1}{3}} e^{8.016|q|^2} < \gamma_2(\tau_0) < 256|q|^{\frac{2}{3}} - |q|^{-\frac{1}{3}}.$$

To evaluate the sharpness of this estimate, consider their difference

$$\begin{aligned} E &= 256|q|^{\frac{2}{3}} - |q|^{-\frac{1}{3}} - (256|q|^{\frac{2}{3}} e^{-16.032|q|^2} - |q|^{-\frac{1}{3}} e^{8.016|q|^2}) \\ &= 256q^{\frac{2}{3}}(1 - e^{-16.032|q|^2}) - |q|^{-\frac{1}{3}}(1 - e^{8.016|q|^2}), \end{aligned}$$

and using the inequality $1 - e^{-x} < \frac{x}{1-x}$ for $0 < x < 1$, we find

$$\begin{aligned} E &< 256|q|^{\frac{2}{3}} \frac{16.032|q|^2}{1 - 16.032|q|^2} - |q|^{-\frac{1}{3}}(1 - e^{8.016|q|^2}) \\ &= \frac{4104.192|q|^{\frac{4}{3}}}{1 - 16.032|q|^2} - |q|^{-\frac{1}{3}}(1 - e^{8.016|q|^2}), \end{aligned}$$

which is an increasing function in $|q|$, and since $|q| \le e^{-2\pi} \approx 0.0019$, this again implies

$$E < 0.25.$$

By the same argument as before, since $\gamma_2(\tau_0)$ is an integer and the total width of the estimate is less than $\frac{1}{2}$, we conclude that $\lfloor x \rceil = \gamma_2(\tau_0)$ for all x lying between the upper and lower bound of $\gamma_2(\tau_0)$. In particular, the value $256|q|^{\frac{2}{3}} - |q|^{-\frac{1}{3}}$ lies between these bounds, completing the proof of the second statement. □

With these formulas in hand, it is now straightforward to compute $\gamma_2(\tau_0)$ for the ten imaginary quadratic orders of class number one with $3 \nmid D$. In these cases, $\gamma_2(\tau_0)$ is an integer (cf. Corollary 6.2.4), so the defining relation $\gamma_2(\tau_0)^3 = j(\tau_0)$ determines the corresponding values of $j(\tau_0)$ unambiguously. The results are summarized in the following table:

D	τ_0	q resp. $\lvert q\rvert$	$\gamma_2(\tau_0)$ (est.)	$\gamma_2(\tau_0)$	$j(\tau_0)$
-4	i	$e^{-2\pi}$	12.0027	12	12^3
-7	$\frac{3+\sqrt{-7}}{2}$	$e^{-\pi\sqrt{7}}$	-14.9647	-15	-15^3
-8	$\sqrt{-2}$	$e^{-2\pi\sqrt{2}}$	20.0199	20	20^3
-11	$\frac{3+\sqrt{-11}}{2}$	$e^{-\pi\sqrt{11}}$	-31.9922	-32	-32^3
-16	$2i$	$e^{-4\pi}$	66.0018	66	66^3
-19	$\frac{3+\sqrt{-19}}{2}$	$e^{-\pi\sqrt{19}}$	-95.9991	-96	-96^3
-28	$\sqrt{-7}$	$e^{-2\pi\sqrt{7}}$	255.0001	255	255^3
-43	$\frac{3+\sqrt{-43}}{2}$	$e^{-\pi\sqrt{43}}$	-959.9999	-960	-960^3
-67	$\frac{3+\sqrt{-67}}{2}$	$e^{-\pi\sqrt{67}}$	-5279.9999	-5280	-5280^3
-163	$\frac{3+\sqrt{-163}}{2}$	$e^{-\pi\sqrt{163}}$	-640319.9999	-640320	-640320^3

Table 8.1: j-invariants of imaginary quadratic orders of class number one with $3 \nmid D$.

Remark 8.1.3. *Numerically, it can be observed that for large discriminants, using the original complex parameter $q^{2\pi i\tau_0}$ in the approximate expression for $\gamma_2(\tau_0)$ may yield a value whose absolute magnitude is very close to the correct one, but with the opposite sign. This reflects the fact that the dominant contribution comes from the term $q^{-\frac{1}{3}}$, whose sign depends on the complex argument of q. As $\mathrm{Im}(\tau_0)$ increases (i.e. as $|D|$ becomes large), the smaller term $q^{\frac{2}{3}}$ becomes negligible, and the approximation becomes nearly symmetric in absolute value. Using the real and positive parameter $|q|^2$ avoids this ambiguity, ensuring that the computed values have the correct sign while preserving the exponential decay that controls numerical accuracy.*

For completeness, we also give the j-invariants of the three imaginary quadratic orders with discriminant divisible by 3:

D	τ_0	$j(\tau_0)$
-3	$\frac{1+\sqrt{-3}}{2}$	0
-12	$\sqrt{-3}$	$54000 = 2^4 \cdot 3^3 \cdot 5^3$
-27	$\frac{1+3\sqrt{-3}}{2}$	$-12288000 = -2^{15} \cdot 3 \cdot 5^3$

Table 8.2: j-invariants of imaginary quadratic orders of class number one with $3 \mid D$.

As predicted in Corollary 6.2.4, the last two entries are not perfect cubes, unlike the values of $j(\tau_0)$ for the orders with discriminant not divisible by 3, listed in Table 8.1.

8.2 $e^{\pi\sqrt{163}}$ is almost an integer

Having developed the necessary constructions and clarified their interrelations, we are now ready to bring everything together and focus on the order of discriminant $D = -163$ to conclude that $e^{\pi\sqrt{163}}$ is astonishingly close to an integer - a result that can bemade even more precise using the numerical approximations of γ_2 from the previous section.

Consider the order $\mathcal{O}$ of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$, $d < 0$, of discriminant $D = -163$. Since every order is a $\mathbb{Z}$-module of rank 2, hence a lattice in $\mathbb{C}$ under the embedding $K \hookrightarrow \mathbb{C}$, it can be written in the form $\mathcal{O} = [1, \omega]$ by Remark 3.3.2. This order is maximal by Theorem 5.7.5, so $\mathcal{O} = \mathcal{O}_K$. Since $-163 \equiv 1 \bmod 4$, we have $D = d$, and it follows that $\mathcal{O}_K = [1, \frac{1+\sqrt{-163}}{2}]$, again by Remark 3.3.2. By Corollary 5.7.6, $\mathcal{O}_K$ has class number one.

Let $\tau = \frac{1+\sqrt{-163}}{2} \in \mathbb{H}$ and set $L = \mathcal{O}_K = [1, \tau]$. By Corollary 2.5.14, which establishes a one-to-one correspondence between homothety classes of lattices in $\mathbb{C}$ and isomorphism classes of elliptic curves over $\mathbb{C}$, the associated elliptic curve E_L is defined over $\mathbb{C}$. Since $L = \mathcal{O}_K$, it follows naturally that $\mathrm{End}(E_L) \cong \mathcal{O}_K$ (see Section 3.5), i.e. E_L has complex multiplication by $\mathcal{O}_K$. Since the order $\mathcal{O}_K$ has class number one, Corollary 5.6.4 guarantees that $j(E_L) = j(\tau) \in \mathbb{Z}$.
Now, by Corollary 4.2.2, the j-function admits the q-expansion

$$j(\tau) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} a_n q^n$$

with integer coefficients a_n. Using the corresponding parameter

$$q = e^{2\pi i\tau} = e^{2\pi i\frac{1+\sqrt{-163}}{2}} = e^{\pi i}e^{\pi i\sqrt{-163}} = -e^{-\pi\sqrt{163}},$$

we obtain

$$j(\tau) = -e^{\pi\sqrt{163}} + 744 + \sum_{n=1}^{\infty} a_n(-e^{-\pi\sqrt{163}})^n,$$

and hence

$$e^{\pi\sqrt{163}} = -j(\tau) + 744 + \sum_{n=1}^{\infty} a_n(-e^{-\pi\sqrt{163}})^n.$$

Since $e^{-\pi\sqrt{163}} \approx 3.8 \cdot 10^{-18}$ and all coefficients $a_n \in \mathbb{Z}$, the series converges exponentially. Using $a_1 = 196884$ as calculated in the proof of Corollary 4.2.2, the first term contributes roughly

$$|a_1|(4 \cdot 10^{-18}) \approx 7.9 \cdot 10^{-13},$$

and the higher-order terms are even smaller, so that

$$\left|\sum_{n=1}^{\infty} a_n(-e^{-\pi\sqrt{163}})^n\right| < 8 \cdot 10^{-13}.$$

Consequently,

$$e^{\pi\sqrt{163}} = -j(\tau) + 744 + \epsilon,$$

with $\epsilon < 8 \cdot 10^{-13}$. Since $j(\tau) \in \mathbb{Z}$, it follows that $e^{\pi\sqrt{163}}$ differs from an integer by less than 10^{-13}, making it astonishingly close to an integer.

As mentioned earlier, the integrality of $j(\tau)$ follows from the theoretical framework; using the numerical approximations in the previous section, in particular Table 8.1, we can now make this conclusion more explicit and precise.
To work with a representative compatible with the modular transformation properties (cf. Section 6.2), rather than evaluating the j-function at $\frac{1+\sqrt{-163}}{2}$, we consider the $\mathrm{SL}_2(\mathbb{Z})$-equivalent point

$$\tau_0 = \tau + 1 = \frac{3 + \sqrt{-163}}{2}.$$

Since τ and τ_0 lie in the same $\mathrm{SL}_2(\mathbb{Z})$-orbit, Lemma 2.5.10 implies $j(\tau) = j(\tau_0)$, so we may compute the value of the j-function at τ_0 instead. Using the parameter $q = e^{2\pi i\tau_0} = e^{3\pi i}e^{\pi i\sqrt{-163}} = -e^{-\pi\sqrt{163}}$, Table 8.1 provides the value $j(\tau_0) = -640320^3$. Inserting this into the previous result, we obtain

$$\begin{aligned} e^{\pi\sqrt{163}} &= -j(\tau_0) + 744 + \epsilon \\ &= 640320^3 + 744 + \epsilon \\ &= 262537412640768744 + \epsilon, \end{aligned}$$

where $\epsilon < 8 \cdot 10^{-13}$, as estimated above.
This shows that $e^{\pi\sqrt{163}}$ differs from the integer 262537412640768744 by less than a trillionth - a remarkable phenomenon resulting from the interplay between algebraic number theory, modular functions, and the arithmetic of elliptic curves with complex multiplication, so that it is, in fact, almost an integer.

Bibliography

[1] Lars V. Ahlfors. *Complex Analysis*. McGraw-Hill, third edition, 1979.

[2] John B. Conway. *Functions of One Complex Variable*. Springer, second edition, 1978.

[3] David A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley and Sons, 1989.

[4] Richard M. Foote David S. Dummit. *Abstract Algebra*. Wiley, third edition, 2003.

[5] Martin Gardner. Mathematical games: Six sensational discoveries that somehow or another have escaped public attention. *Scientific American*, Vol. 232, No. 4:p. 126–133, April 1975. Accessed: 26.09.2025.

[6] Paul Garrett. Product expansion of sin x. (Lecture notes), `https://www-users.cse.umn.edu/~garrett/m/complex/`, University of Minnesota, January 2021. Accessed: 10.09.2025.

[7] Serge Lang. *Algebra*. Springer, third edition, 2002.

[8] Jürgen Neukirch. *Algebraic Number Theory*. Springer, first edition, 1999.

[9] Srinivasa Ramanujan. Modular equations and approximations to π. *Quarterly Journal of Mathematics*, Vol. 45:p. 350–372, 1914.

[10] Walter Rudin. *Principles of Mathematical Analysis*. McGraw-Hill, third edition, 1976.

[11] Reinhard Schertz. Weber's class invariants revisited. *Journal de Théorie des Nombres de Bordeaux*, Vol. 14, No. 1:p. 325–343, 2002.

[12] Jean-Pierre Serre. Le problème des groupes de congruence pour sl2. *Ann. of Mathematics*, Vol. 92, No. 3:p. 489–527, 1970.

[13] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer, 1994.

[14] Andrew Sutherland. Elliptic curves. (Lecture notes), `https://ocw.mit.edu/courses/18-783-elliptic-curves-spring-2021/pages/lecture-notes-and-worksheets/`, MIT Mathematics 18.783, Spring 2021. Accessed: 20.10.2025.