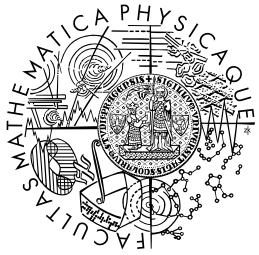

FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

BACHELOR THESIS

Ondrej Bínovský

Imaginary quadratic fields with class number 1

Department of Algebra

Supervisor of the bachelor thesis:	Mgr. Vítězslav Kala, Ph.D.
Study programme:	Mathematics
Study branch:	Mathematical Methods of Information Security

Prague 2021

I declare that I carried out this bachelor thesis independently, and only with the cited sources, literature and other professional sources.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In ..... date ..... signature of the author

I would like to thank Vítězslav Kala for his help and the time he dedicated to me, and Jan Nekovář for a useful discussion. I am grateful to my mother Martina for her support.

Title: Imaginary quadratic fields with class number 1

Author: Ondrej Bínovský

Department: Department of Algebra

Supervisor: Mgr. Vítězslav Kala, Ph.D., Department of Algebra

Abstract: We give an exposition of Heegner's and Siegel's proofs that there are exactly 9 imaginary quadratic fields with class number equal to 1. In particular, we discuss Weber's original method of determining the class invariants of an imaginary quadratic field. Finally, we give an elementary proof of a sufficient condition, due to Alice Gee, for a value of a modular function to be a class invariant.

Keywords: imaginary quadratic fields, class number problem, modular functions, class invariants, complex multiplication

Contents

Introduction **2**

1 Preliminaries **7**
1.1 Notation 7
1.2 Imaginary quadratic fields 7
1.3 Elliptic functions 10

2 Modular functions **14**
2.1 The modular group 14
2.2 Modular functions 15
2.3 Modular functions of higher level 15
2.4 Transformation equations 18
2.5 Examples of modular functions 20

3 Class invariants **22**
3.1 Integrality of the j-invariant 22
3.2 Weber's determination of class invariants 24
3.3 A sufficient criterion for class invariants 31
3.4 Heegner's proof 36

4 Siegel's proof **40**
4.1 The Dirichlet-Kronecker formula 40
4.2 Class number 1 and an inert conductor f 50
4.3 Specialization to $f = 5$ 55
4.4 Modular functions of level 5 57
4.5 The diophantine equation 64

Bibliography **69**

Introduction

Unique factorization

The Fundamental Theorem of Arithmetic states that the ring $\mathbb{Z}$ is a unique factorization domain, meaning that except for zero and the units of $\mathbb{Z}$, every element of $\mathbb{Z}$ can be written as a product of irreducible elements of $\mathbb{Z}$ in exactly one way, apart from reordering of the factors and multiplication by units.

Let K be a number field, that is, a finite extension of $\mathbb{Q}$. The subring $\mathcal{O}_K$ of K, consisting of those elements of K that satisfy a monic polynomial equation over $\mathbb{Z}$, plays the same role as $\mathbb{Z}$ when viewed as a subring of $\mathbb{Q}$. We can now ask the question whether the ring $\mathcal{O}_K$ is a unique factorization domain.

It turns out that this is in general not the case. Nonetheless, the ideals of $\mathcal{O}_K$ still enjoy the property of unique factorization. By this we mean that every ideal of $\mathcal{O}_K$ can be expressed as a product of prime ideals in exactly one way, apart from reordering of the factors.

The failure of the unique factorization of the elements of $\mathcal{O}_K$ is measured by the ideal class group $\mathrm{Cl_K}$ of K which is defined as follows. Define an equivalence relation on the set of all nonzero ideals of $\mathcal{O}_K$ by saying that two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent if $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$ for some nonzero $\alpha, \beta \in \mathcal{O}_K$. Then it can be shown that the equivalence classes of this relation form an abelian group with multiplication coming from multiplication of ideals, the identity element being the equivalence class of principal ideals.

The ring $\mathcal{O}_K$ is a unique factorization domain if and only if the group $\mathrm{Cl_K}$ is trivial. The order of Cl_K is called the class number of K, and it is denoted by h_K. The class number h_K is always finite.

For a given number field K it is relatively easy to compute its class number. However, it is very hard to determine the general properties of h_K as a function of K. For example, it is not known whether there exists infinitely many number fields K such that $h_K = 1$.

Let us now restrict our attention on the number fields of degree 2 over $\mathbb{Q}$. These come in two types: either having two embeddings into $\mathbb{R}$, or none. In the former case, they are called real quadratic fields, and in the latter, imaginary quadratic fields. It is conjectured that there are infinitely many real quadratic fields with class number one.

By contrast, there are only 9 imaginary quadratic fields with class number one. More precisely, there are given by

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

This was first proved by Kurt Heegner [Hee52] in 1952 (150 years after it was surmised by Gauss in [GC86]). It is perhaps surprising that his proof (and also similar ones due to Baran, Chen, Kenku, and Siegel) involves little arithmetic of quadratic fields themselves. The formulation of this problem actually gives no indication of the crucial tools and objects used in its solution, which are class field theory, complex multiplication of elliptic curves, modular functions, and rational points on modular curves.

The object of this work is an exposition of the main ideas of Heegner's proof. This was done before in [Cox11], [Kez], [Boo], [Sha14], [Sch10], [Bir11], [Mey70], [Deu68], and [Sta69]. We have followed Stark's paper [Sta69] which is exceptional in that it does not use any unproved assertions from class field theory. Stark points out that Heegner's proof actually does not even require any algebraic number theory.

Kurt Heegner

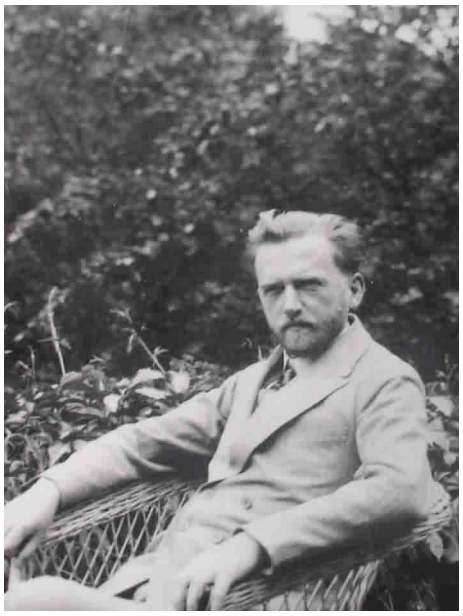

Photo of Kurt Heegner taken at the terrace of mother's house in Berlin in the 1930s. Taken from [cva] where it is attributed to Fritz Heegner.

Heegner's solution of the class number one problem was at first thought to be incorrect because of the unclear way his paper was written, apparent dependence on an unproved result of Weber, and perhaps even unwillingness of other mathematicians to read an article by a nonprofessional mathematician. Stark writes in the first appendix to [Sta11] that

> "I believe I am the modern rediscoverer of Heegner's paper. I came across it in Math Reviews somewhere in academic 1962-63 while working on my PhD thesis. The last sentence of the review [of the Heegner's paper] is a thesis killer!"

He further states that

> "Fortunately for me and my thesis, my thesis advisor, DH Lehmer, vaguely remembered that Heegner was incorrect, but that he was going to attend a conference in Boulder in the summer of 1963 and verify with the experts that was the case. He returned and confirmed once again that "the experts" said Heegner's proof was incorrect. Lehmer

did not tell me who "the experts" were and I never found out. However, two of my three main suspects in the whole affair were at the Boulder meeting."

J.-P. Serre write in his article [Ser85, p. 8], titled $\Delta = b^2 - 4ac$, that

> "The next progress came in 1952 when K. Heegner published a proof that [the tenth imaginary quadratic field with class number 1] does not exist. However, this proof used properties of modular functions which he stated without enough justification. People could not understand his work, and did not believe it (I tried myself once to follow his arguments, but got nowhere ..). Hence, the question of the existence of [the tenth imaginary quadratic field with class number 1] was still considered as open."

S. Chowla in his chapter in the Seminar on Complex Multiplication [BCH66, VI-2] writes, without giving any reason or argument, that

> "It should also be remarked here that a recent claim by Kurt Heegner, (M.Z. 1954) to have solved this problem, seems unjustified."

The website of the *Foundation for German communication and related technolgies* [cva] states that

> "Kurt Heegner was born on 16 December 1893 and he died in 1965. In the year 1920 he received his Ph.D. at Jena University on: Über den Zwischenkreisröhrensender. Particularly in the 1920s and 1930s he published quite some papers on valve oscillators. He even jointly prepared a paper with Watanabe of Japan."

This website also describes Heegner's work in electronics, especially in oscillators, giving a list of his patents. It states that he was mainly a private tutor (Privat Dozent) in Mathematics, and detailing Heegner's struggles to obtain revenue from his patents. The website further cites certain Bechmann (according to the website, Germany's leading experts on quartz resonators) as saying: "*Herr Dr. Heegner redete unklar und unverständlich wie immer . . .* ".

Birch [Bir04, 3.] says of Heegner that "*Heegner was a fine mathematician, with a rather low-grade post in a gymnasium in East Berlin*", and that

> "In his famous, very eccentrically written, paper he begins with a historical introduction concerning the congruence number problem, then he quotes various things from Weber and proves some highly surprising theorems showing that the congruence number problem is soluble for certain families of [positive integers]; and then he suddenly (correctly but over succinctly) solves the classical class number one problem. Unhappily, in 1952 there was noone left who was sufficiently expert in Weber's Algebra to appreciate Heegner's achievement."

But Birch says also that

> "Heegner's paper was written in an amateurish and rather mystical style, so perhaps it was not surprising that at the time noone tried very hard to understand it."

In the report of the 2008 Oberwolfach conference on history of mathematics [DCS09, p. 1354], Patterson, Schappacher, and Opolka note

> "Heegner appears from the records as a not very socially adept but upright person. He was known around Steglitz where, especially in his later years his appearance became somewhat eccentric. He had a long white beard, a long white pigtail and clothes which had been once good but had become old and worn. He was apparently known as the 'Jesus of Steglitz' and, because of his character and his courage during the war, generally respected."

Here, Steglitz is the part of Berlin where Heegner have lived since 1932. After he became ill in 1950, he have lived in poverty, helped out by his sister Lotte. He died in 1965, "*alone and it may have been three days or so before he was found*", according to [DCS09, p. 1356].

Later, Birch, building on Heegner's ideas, introduced the important notion of Heegner points. These are points on modular curves obtained as images of quadratic irrationalities in the upper half-plane. By the Modularity Theorem, every elliptic curve over rational numbers is an image of a modular curve by a rational map, so we can consider the images of Heegner points on elliptic curves. These have sometimes infinite order, or are at least exceptionally large. Heegner points were used in Kolyvagin's work on the Birch–Swinnerton-Dyer conjecture. For more information on Heegner points see [Gro84].

To give an illustration, Heegner in his article proved that if $p \equiv -1 \pmod 8$ is a prime, then the equation $y^2 = -p(x^4 - 64)$ has infinitely many rational solutions. This implies that the elliptic curve $y^2 = x(x^2 + p^2)$ has rank 1. Using similar ideas, Satgé proved in [Sat87] that if $n/2$ is a prime and $n \equiv 4 \pmod 9$, then $n = x^3 + y^3$ for some $x, y \in \mathbb{Q}$.

For additional information on Heegner see Schappacher's presentations [Schb] and [Scha] from talks given in Paris and Madrid, respectively.

This work

In the mentioned article [Sta69], titled *On the "gap" in a theorem of Heegner*, Stark claims that, in fact, the only problem with Heegner's proof is reliance on a theorem in Weber's *Lehrbuch der Algebra* [Web08] whose proof is incomplete. Fortunately, this can remedied very easily, even using the original Weber's method, as Stark indeed does in his paper. We will look at Weber's methods in detail in Chapter 3.

The contested result of Weber concerns the Schläfli's modular function $\mathfrak{f}$. This function is defined by $\mathfrak{f}(\tau) = e^{-\pi i \tau/24} \prod_{n \geq 1}(1 + e^{\pi i \tau(2n-1)})$ for τ in the upper half-plane $\mathfrak{H}$. Let τ now be such that $K = \mathbb{Q}(\tau)$ is an imaginary quadratic field and $\tau \in \mathfrak{H}$. Weber "proves" that $\mathfrak{f}(\tau)^2 \in K(j(\tau))$, and conjectures that actually $\mathfrak{f}(\tau) \in K(j(\tau))$, under certain congruence conditions on the minimal polynomial of τ. (Here j is the modular invariant.) Heegner uses only the former result in his solution of the class number one problem. However, in his article, he also proves

other things (which are of independent interest), and there he uses the stronger result that $\mathfrak{f}(\tau) \in K(j(\tau))$.

Weber's conjecture was proved by Birch [Bir69b] in 1969. Note that Weber published his conjecture at the end of 19th century. However, it was Shimura who developed a fully satisfactory formalism for dealing with this type of questions. In his book *Introduction to the Arithmetic Theory of Automorphic Functions* [Shi94] he proved what is now known as the Shimura's reciprocity law.

Alice Gee in her PhD thesis [Gee99] deduced from the Shimura's reciprocity law an explicit criterion, which, given a modular function f and a point $\tau \in K \cap \mathfrak{H}$, allows us to decide whether $f(\tau) \in K(j(\tau))$ by a simple calculation.

In Chapter 3 we give a direct and elementary proof of Gee's criterion (under certain minor restriction on the point τ). Our proof is based on the formalism used by Lang [Lan87] in his proof of the Shimura's reciprocity law. We have also used a simple but important result from the appendix of [Ser90] (appearing also in [Che99] and [Bar10]) which restricts the image of the Galois representation of an elliptic curve (over $\mathbb{C}$) with complex multiplication.

This proof of Gee's criterion is author's contribution to the thesis. Note that there is no connection explicitly pointed out in the literature, between Gee's criterion and the approach taken in [Che99] and [Bar10]. While Gee uses Shimura's results, Baran and Chen use the so-called modular interpretation of the points on modular curves. We have just worked with function fields. The second contribution of the author is a systematic treatment of the Weber's transformation equations for modular functions, and subsequent exposition of Weber's method of determining a class invariant in two particular cases.

In Chapter 4 we give an exposition of the main ideas of Siegel's solution of the class number problem. Siegel's proof is a variation of Heegner's proof, but Siegel uses modular functions of level 5, while Heegner uses modular functions of level 24. Siegel's proof is also, in a certain respect, easier to understand. This is because we get the resulting diophantine equation directly from the relation between modular functions (that is, the modular curve). By contrast, in Heegner's proof we must perform additional contortions, real understanding of which would require far more work.

1. Preliminaries

1.1 Notation

Let A be a ring. We denote by $A^\times$ the group of units of A. We denote by $\mathrm{M}_2(A)$ the ring of 2-by-2 matrices with entries in A. We define $\mathrm{GL}_2(A) = \mathrm{M}_2(A)^\times$ and $\mathrm{SL}_2(A) = \{\alpha \in \mathrm{GL}_2(A) \colon \det(\alpha) = 1\}$. If $A \subset \mathbb{R}$ then we define $\mathrm{GL}_2^+(A) = \{\alpha \in \mathrm{GL}_2(A) \colon \det(\alpha) > 0\}$. We denote the 2-by-2 identity matrix by 1.

We define the upper half-plane by $\mathfrak{H} = \{\tau \in \mathbb{C} \colon \Im(\tau) > 0\}$ and we let $q = e^{2\pi i \tau}$ for $\tau \in \mathfrak{H}$. We denote the n-th root of unity $e^{2\pi i/n}$ by ζ_n. Let k be a field. We denote by $k((X))$ the field of formal Laurent series in the variable X.

1.2 Imaginary quadratic fields

An **imaginary quadratic field** K is an extension of $\mathbb{Q}$ of degree 2 having no embedding into $\mathbb{R}$. When K is viewed as a subfield of $\mathbb{C}$, then the latter condition is equivalent to requiring that $K \cap \mathbb{R} = \mathbb{Q}$. Next we define the **ring of integers** of K as

$$\mathcal{O}_K = \{\alpha \in K \colon \alpha^2 + s\alpha + t = 0 \text{ for some } s, t \in \mathbb{Z}\}.$$

In other words $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K, and so it is indeed a subring of K. For $\alpha \in K$ we define its **norm** by $N(\alpha) = \alpha\overline{\alpha}$ and its **trace** by $tr(\alpha) = \alpha + \overline{\alpha}$. For a detailed discussion of the rings of integers, norms, and traces see [Con, 2.,3.].

Proposition 1.2.1. *Let $K = \mathbb{Q}(\sqrt{-m})$ be an imaginary quadratic field, where m is a positive squarefree integer. Then $\mathcal{O}_K = \mathbb{Z}[\omega] = [\omega, 1]$, where*

$$\omega = \begin{cases} \sqrt{-m} & \text{if } m \not\equiv 3 \pmod 4, \\ \frac{1+\sqrt{-m}}{2} & m \equiv 3 \pmod 4. \end{cases}$$

Alternatively, we may take $\omega = \frac{m+\sqrt{-m}}{2}$ which works in both cases.

Proof. See [Con, 3., Theorem 3.4., p. 2]. □

Proposition 1.2.2. *Let K be an imaginary quadratic field. Write $K = \mathbb{Q}(\sqrt{-m})$ with m squarefree. Let $\mathcal{O}_K = \mathbb{Z}[\omega]$, where ω is as in Proposition 1.2.1. Let $f(X)$ be the minimal polynomial of ω over $\mathbb{Q}$, so that*

$$f(X) = \begin{cases} X^2 + m & \text{if } m \not\equiv 3 \pmod 4, \\ X^2 - X + \frac{1+m}{4} & m \equiv 3 \pmod 4. \end{cases}$$

Let $\overline{f}(X)$ be the reduction of $f(X)$ modulo p. Then

(1) If $\overline{f}(X)$ is irreducible in $(\mathbb{Z}/p\mathbb{Z})[X]$, then (p) is a prime ideal in $\mathcal{O}_K$, and we say that p is inert in K.

(2) If $\overline{f}(X) = (X - c)(X - c')$, where $c, c' \in \mathbb{Z}/p\mathbb{Z}$ are distinct, then $(p) = \mathfrak{p}\overline{\mathfrak{p}}$, where $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are distinct prime ideals, and we say that p splits in K.

(3) If $f(X) = (X - c)^2$, where $c \in \mathbb{Z}/p\mathbb{Z}$, then $(p) = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$, and we say that p is ramified in K.

Proof. See [Con, 8., Theorem 8.3., p. 20]. □

Proposition 1.2.3. *Let K be an imaginary quadratic field such that $h_K = 1$. Write $K = \mathbb{Q}(\sqrt{-m})$ with m squarefree.*
(1) Let p be a prime which splits or ramifies in K. Then $p \geq m/4$.
(2) If $m > 8$ then $m \equiv 3 \pmod 8$.
(3) If $m \geq 16$ then m is a prime.

Proof. Let p be a prime which splits or ramifies in K. Then $(p) = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_1, \mathfrak{p}_2$ are prime ideals in $\mathcal{O}_K$. Since $h_K = 1$, every ideal in $\mathcal{O}_K$ is principal, so $\mathfrak{p}_1 = (\pi_1)$ and $\mathfrak{p}_2 = (\pi_2)$ for some $\pi_1, \pi_2 \in \mathcal{O}_K$. We have either $\pi_1 = \overline{\pi_2}$ or $\pi_1 = \pi_2$, according to whether p splits or ramifies. In any case we have $N(\pi_1) = N(\pi_2)$. From $(p) = (\pi_1\pi_2)$ we see that $p = \pi_1\pi_2 u$, where u is a unit in $\mathcal{O}_K$. Taking norms we obtain $p^2 = N(\pi_1)N(\pi_2) = N(\pi_2)^2$ or $p = N(\pi_1)$. Let $\omega = \frac{m+\sqrt{-m}}{2}$, so $\mathcal{O}_K = [\omega, 1]$. Write $\pi_1 = a + b\omega$, where $a, b \in \mathbb{Z}$. We have

$$\begin{aligned} p = N(\pi_1) &= (a + b\omega)(a + b\overline{\omega}) = a^2 + (\omega + \overline{\omega})ab + \omega\overline{\omega}b^2, \\ &= a^2 + mab + \frac{m^2 + m}{4}b^2 = \left(a + \frac{mb}{2}\right)^2 + \frac{m}{4}b^2, \end{aligned}$$

and, since $b \neq 0$, (1) follows. By (1) the prime 2 is inert in K if $m > 8$. Since the polynomial $X^2 + m$ is always reducible modulo 2, by Proposition 1.2.2 we must have $m \equiv 3 \pmod 4$, and moreover the polynomial $X^2 - X + \frac{1+m}{4}$ must be irreducible modulo 2. This means that $m \equiv 3 \pmod 8$. Finally, if m is composite, then m has a prime divisor p such that $p < \sqrt{m}$. Proposition 1.2.2 tells us that p ramifies, so we have $p \geq m/4$. Therefore $\sqrt{m} > m/4$, proving (3). □

Corollary 1.2.4. *The notation being as in Proposition 1.2.3, we have $\left(\frac{m}{p}\right) = -1$ for all primes $2 < p < m/4$.*

Proposition 1.2.5. *Let K be an imaginary quadratic field. Then the class number h_K is equal to the number of triples $(a, b, c) \in \mathbb{Z}^3$ satisfying the following properties:*
(1) a, b, c are relatively prime.
(2) $d_K = b^2 - 4ac$.
(3) $-a < b \leq a < c$ or $0 \leq b \leq a = c$.

Proof. See [Cox11, §2.,A., Theorem 2.13., p. 29]. □

Proposition 1.2.5 gives us an algorithm for computing the class number. The following proposition provides an "explicit formula" for the class number of an imaginary quadratic field. It is apparently hopeless to get a lower bound from this formula.

Proposition 1.2.6. *Let $K = \mathbb{Q}(\sqrt{-p})$ with a prime p such that $p \equiv 3 \pmod 8$. Then*

$$h_K = \frac{1}{3} \sum_{0<n<p/2} \left(\frac{n}{p}\right).$$

Proof. See [Zag81, §9, Satz 4, p. 82]. Zagier also considers the other cases modulo 8. The proof is rather involved; one needs to compute the value of certain L-series at 1 in two ways. □

By a **lattice** Λ we mean a set of the shape

$$\Lambda = [\omega_1, \omega_2] = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\},$$

where ω_1, ω_2 are complex numbers whose ratio is not real. We call (ω_1, ω_2) a **basis** for Λ. Two lattices Λ and Λ' are said to be **homothetic** if $\Lambda' = \mu\Lambda$ for some $\mu \in \mathbb{C}^\times$.

Proposition 1.2.7. *Let $\Lambda = [\omega_1, \omega_2]$ and $\Lambda' = [\omega_1', \omega_2']$ be lattices. Assume that $\omega_1/\omega_2 \in \mathfrak{H}$ and $\omega_1'/\omega_2' \in \mathfrak{H}$. Then $\Lambda = \Lambda'$ if and only if*

$$\begin{pmatrix}\omega_1'\\ \omega_2'\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} \qquad \text{for some} \quad \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Proof. Easy. See [DS05, 1.3, Lemma 1.3.1., p. 25]. □

Consider a lattice Λ and let

$$\mathcal{O}_\Lambda = \{\lambda \in \mathbb{C} : \lambda\Lambda \subset \Lambda\}.$$

The set $\mathcal{O}_\Lambda$ is called **the order of the lattice** Λ. It is clear that homothetic lattices have the same orders. Consequently we may restrict ourselves to lattices of the form $[\tau, 1]$, where usually $\tau \in \mathfrak{H}$. We use the following notation: $\Lambda_\tau = [\tau, 1]$ and $\mathcal{O}_\tau = \mathcal{O}_{\Lambda_\tau}$.

Proposition 1.2.8. *Let $\tau, \omega \in \mathfrak{H}$. The lattices Λ_τ and Λ_ω are homothetic if and only if $\tau = \gamma\omega$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Let $\tau, \omega \in \mathbb{C}$. Then $\Lambda_\tau = \Lambda_\omega$ if and only if $\tau \pm \omega \in \mathbb{Z}$.*

Proof. Easy calculation. □

Let us now investigate the structure of the orders $\mathcal{O}_\tau$. One can embed $\mathcal{O}_\tau$ into $\mathrm{M}_2(\mathbb{Z})$ as follows. Define a map by

$$\begin{aligned}\epsilon_\tau \colon \mathcal{O}_\tau &\longrightarrow \mathrm{M}_2(\mathbb{Z}),\\ \lambda &\longmapsto \epsilon_\tau(\lambda),\end{aligned}$$

where the matrix $\epsilon_\tau(\lambda)$ is determined by the action of λ on the basis $(\tau, 1)$ of the lattice Λ_τ, that is,

$$\lambda\begin{pmatrix}\tau\\ 1\end{pmatrix} = \epsilon_\tau(\lambda)\begin{pmatrix}\tau\\ 1\end{pmatrix}. \tag{1.1}$$

We say that $\tau \in \mathfrak{H}$ is a **CM point** if $\mathbb{Q}(\tau)$ is an imaginary quadratic field. If $A\tau^2 + B\tau + C = 0$, where A, B, C are integers such that $(A, B, C) = 1$, then we call this equation **the minimal equation** for τ.

Proposition 1.2.9. *Let $\tau \in \mathfrak{H}$ be a CM point with minimal equation*

$$A\tau^2 + B\tau + C = 0.$$

Then

$$\epsilon_\tau(\mathcal{O}_\tau) = \left\{ s\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + t\begin{pmatrix}0 & -C\\ A & B\end{pmatrix} : s, t \in \mathbb{Z}\right\}.$$

Proof. Let $\lambda \in \mathcal{O}_\tau$ and write $\epsilon_\tau(\lambda) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Eliminating λ from (1.1) yields

$$c\tau^2 + (d-a)\tau - b = 0. \tag{1.2}$$

Comparing (1.2) with $A\tau^2 + B\tau + C = 0$ and remembering that $(A, B, C) = 1$, we obtain

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & -tC \\ tA & a + tB \end{pmatrix}$$

for some $t \in \mathbb{Z}$. This is the desired result. □

The proof of Proposition 1.2.9 shows that if $\tau \in \mathfrak{H}$ is not a CM point, then necessarily $\mathcal{O}_\tau = \mathbb{Z}$. On the other hand, if τ is a CM point with minimal equation $A\tau^2 + B\tau + C = 0$, then writing $\alpha = \epsilon_\tau^{-1} \left(\begin{smallmatrix} 0 & -C \\ A & B \end{smallmatrix}\right)$ we see that $\mathcal{O}_\tau = [\alpha, 1]$. By the second part of Proposition 1.2.8 we have $\mathcal{O}_\tau = [\beta, 1]$ if and only if $\beta = \pm\alpha + s$, where $s \in \mathbb{Z}$.

Writing $\epsilon_\tau(\lambda) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in (1.1) we can express λ as follows

$$\lambda^2 - (a+d)\lambda + ad - bc = 0.$$

Therefore we always have $\mathcal{O}_\tau \subset \mathcal{O}_K$, where $K = \mathbb{Q}(\tau)$. Consider now an arbitrary subring $\mathcal{O}$ of $\mathcal{O}_K$. Then $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank 1 or 2. In the former case we have $\mathcal{O} = \mathbb{Z}$. In the latter case, the ring $\mathcal{O}$ is called a **quadratic order** (or simply an **order**) in K. proposition 1.2.9 shows that the order of a lattice is a quadratic order in the corresponding imaginary quadratic field. Conversely any quadratic order is an order of some lattice (for example itself).

Proposition 1.2.10. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K. Write $\mathcal{O}_K = [\omega, 1]$. Then there exists a unique positive integer f such that $\mathcal{O} = [f\omega, 1]$.*

Proof. See [Cox11, §7.,A., Lemma 7.2., p. 133]. □

The integer f of Proposition 1.2.10 is called **the conductor** of the order $\mathcal{O}$. If we view $\mathcal{O}_K$ and $\mathcal{O}$ as $\mathbb{Z}$-modules, then we have $(\mathcal{O}_K : \mathcal{O}_\tau) = f$.

Let $\tau \in \mathfrak{H}$ be a CM point. We define **the discriminant** D_τ of the order $\mathcal{O}_\tau$ by $D_\tau = (f\omega - f\overline{\omega})^2$. The second part of Proposition 1.2.8 shows that D_τ is well defined.

Proposition 1.2.11. *Let $A\tau^2 + B\tau + C = 0$ be the minimal equation for CM point $\tau \in \mathfrak{H}$. Then $D_\tau = B^2 - 4AC$.*

Proof. Let $\alpha = \epsilon_\tau^{-1} \left(\begin{smallmatrix} 0 & -C \\ A & B \end{smallmatrix}\right)$ so that $\mathcal{O}_\tau = [\alpha, 1]$. Now we use (1.1) with $\lambda = \alpha$ to obtain

$$\alpha^2 - B\alpha + AC = 0.$$

Therefore $D_\tau = (\alpha - \overline{\alpha})^2 = (\alpha + \overline{\alpha})^2 - 4\alpha\overline{\alpha} = B^2 - 4AC$. □

1.3 Elliptic functions

Let Λ be a lattice. We say that a meromorphic function f on $\mathbb{C}$ is an **elliptic function** with respect to the lattice Λ, if $f(z + \omega) = f(z)$ whenever $z \in \mathbb{C}$ and

$\omega \in \Lambda$. We define the **Weierstrass elliptic function** with respect to the lattice Λ by

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

The function $\wp_\Lambda$ is holomorphic on $\mathbb{C} \setminus \Lambda$ and has a pole of second order at every point of Λ. We define $G_{2n}(\Lambda) = \sum_{0 \neq \omega \in \Lambda} \omega^{-2n}$ for $n \geq 2$, and $g_2(\Lambda) = 60G_4(\Lambda)$, $g_3(\Lambda) = 140G_6(\Lambda)$.

Proposition 1.3.1. *Let Λ be a lattice.*

(1) The Laurent series expansion about origin of $\wp_\Lambda$ is

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

(2) The function $\wp_\Lambda$ satisfies the differential equation

$$\wp_\Lambda'^2 = 4\wp_\Lambda^3 - g_2(\Lambda)\wp_\Lambda - g_3(\Lambda).$$

(3) Let $\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2$. Then $\Delta(\Lambda) \neq 0$.

(4) The field of all elliptic functions with respect to Λ is equal to $\mathbb{C}(\wp_\Lambda, \wp_\Lambda')$. The field of all even elliptic functions with respect to Λ is equal to $\mathbb{C}(\wp_\Lambda)$.

(5) Let $n \geq 2$ be an integer. Then $G_{2n}(\Lambda)$ is a polynomial in $g_2(\Lambda)$ and $g_3(\Lambda)$ with rational coefficients.

(6) Let $z, w \in \mathbb{C}$. We have $\wp_\Lambda(z) = \wp_\Lambda(w)$ if and only if $z \equiv \pm w \pmod{\Lambda}$.

Proof. See [Cox11, §10., p. 181] or [Lan87, Chapter 1]. □

Proposition 1.3.2. *Let Λ be a lattice corresponding to an order $\mathcal{O}$ in an imaginary quadratic field K. Let L be a subfield of $\mathbb{C}$ containing $g_2(\Lambda)$ and $g_3(\Lambda)$. Then for every $\alpha \in \mathcal{O}$ we have $\wp_\Lambda(\alpha z) = R_\alpha(\wp_\Lambda(z))$, where R_α is a rational function with coefficients in $K \cdot L$.*

Proof. Let $\wp = \wp_\Lambda$ and $\wp_\alpha(z) = \wp_\Lambda(\alpha z)$. We know that an even elliptic function with respect to the lattice Λ is expressible rationally via $\wp$. Because $\mathcal{O}\Lambda \subset \Lambda$ and $\wp$ is even, there is a rational function $R_\alpha \in \mathbb{C}(X)$ such that $\wp_\alpha = R_\alpha(\wp)$. We know that the Laurent expansions of $\wp$ and $\wp_\alpha$ are of the form

$$\wp_\alpha(z) = \frac{1}{\alpha^2 z^2} + \sum_{n=1}^{\infty} (2n+1) P_{n+1}(g_2(\Lambda), g_3(\Lambda)) \alpha^{2n} z^{2n},$$
$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) P_{n+1}(g_2(\Lambda), g_3(\Lambda)) z^{2n},$$

where $P_{n+1}(X, Y) \in \mathbb{Q}[X.Y]$ for every $n \geq 1$. Therefore $\wp_\alpha \in (K \cdot L)((z))$ and $\wp \in L((z))$. Now let $\sigma \in \mathrm{Aut}(\mathbb{C}/K \cdot L)$. Then σ extends to an automorphism $\mathbb{C}((z)) \to \mathbb{C}((z))$ by acting on the coefficients of the formal Laurent series. Every such automorphism σ fixes $\wp$ and $\wp_\alpha$. Consequently, we have $R_\alpha^\sigma = R_\alpha$ for every $\sigma \in \mathrm{Aut}(\mathbb{C}/K \cdot L)$. Therefore the coefficients of R_α must lie in $K \cdot L$. □

In general, an **elliptic curve** is a smooth projective curve of genus 1. For us an elliptic curve E will we be the curve given by an equation of the form

$$y^2 = 4x^3 - g_2 x - g_3, \quad g_2, g_3 \in \mathbb{C}, \quad g_2^3 - 27g_3^2 \neq 0, \tag{1.3}$$

together with a point at infinity. In other words,

$$E = \{[x, y, z] \in \mathbb{P}^2(\mathbb{C})\colon y^2 z = 4x^3 - g_2 x z^2 - g_3 z^3\}.$$

We see from this, that the point at infinity of E is $[0, 1, 0]$. Let Λ be a lattice and let E_Λ be the curve defined by the equation

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

Proposition 1.3.1 shows that E_Λ is an elliptic curve and there is a bijection

$$\begin{aligned} \Phi\colon \mathbb{C}/\Lambda &\longrightarrow E_\Lambda \\ z + \Lambda &\longmapsto \begin{cases} [\wp_\Lambda(z), \wp'_\Lambda(z), 1] & \text{if } z \notin \Lambda, \\ [0, 1, 0] & \text{if } z \in \Lambda. \end{cases} \end{aligned} \tag{1.4}$$

Conversely, if E, g_2, g_3 are as in (3.25), then there exists a lattice Λ such that $g_2 = g_2(\Lambda)$ and $g_3 = g_3(\Lambda)$ and we have a bijection $\Phi\colon \mathbb{C}/\Lambda \to E$ as in (1.4). This is the content of the Uniformization Theorem for elliptic curves. See [Sil09, VI.5.].

It is well known that an elliptic curve can be given the structure of an abelian group in such a way that the group operations are rational maps of the curve. If the elliptic curve E_Λ is considered as a group, then the bijection Φ of (1.4) becomes an isomorphism of groups.

We let $E[N]$ be the subgroup of an elliptic curve E consisting of points of E whose order is finite and divides N. We have

$$E_\Lambda[N] \cong \frac{\frac{1}{N}\Lambda}{\Lambda} \cong \frac{\mathbb{Z}}{N\mathbb{Z}} \times \frac{\mathbb{Z}}{N\mathbb{Z}}.$$

The j-invariant of an elliptic curve $E\colon y^2 = 4x^3 - g_2 x - g_3$ is defined as

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

Let $\tau \in \mathfrak{H}$ and $\Lambda_\tau = [\tau, 1]$ and let $E_\tau = E_{\Lambda_\tau}$ be the corresponding elliptic curve. We set

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

Thus the j-invariant can be viewed as a function on the upper-half plane, lattices, or elliptic curves.

Proposition 1.3.3. *Let Λ_1 and Λ_2 be lattices. Then Λ_1 and Λ_2 are homothetic if and only if $j(\Lambda_1) = j(\Lambda_2)$. Similarly, if E_1 and E_2 are elliptic curves, then E_1 and E_2 are isomorphic if and only if $j(E_1) = j(E_2)$.*

Proof. see [Cox11, §14., A., 14.4.]. □

Let Λ be a lattice. Then the complex torus $\mathbb{C}/\Lambda_\tau$ is both a Riemann surface and an abelian group. Therefore we can consider holomorphic homomorphisms between such tori. If Λ_1 and Λ_2 are lattices, then the holomorphic homomorphism from Λ_1 to Λ_2 are given by multiplication by λ such that $\lambda\Lambda_1 \subseteq \Lambda_2$. Isomorphism occurs if and only if $\lambda\Lambda_1 = \Lambda_2$. For proofs see for example [Sil09, VI.4.].

Holomorphic homomorphisms and isomorphisms of complex tori correspond to isogenies and isomorphisms of elliptic curves. Let λ be such that $\lambda\Lambda_\tau \subseteq \Lambda_z$ and let $[\lambda]\colon \Lambda_\tau \longrightarrow \mathbb{C}/\Lambda_z\colon w + \Lambda_\tau \longmapsto \lambda + \Lambda_z$. Then we have the commutative diagram

$$\begin{array}{ccc} \mathbb{C}/\Lambda_\tau & \xrightarrow{\sim} & E_\tau \\ \downarrow{\scriptstyle [\lambda]} & & \downarrow{\scriptstyle R_\lambda} \\ \mathbb{C}/\Lambda_z & \xrightarrow{\sim} & E_z \end{array}$$

where R_λ is the corresponding isogeny (that is, a homomorphism which is a rational map). Conversely, for an isogeny we get a multiplication map of lattices.

Suppose now that E_τ has an endomorphism which is not multiplication by an integer. Then for some $\lambda \notin \mathbb{Z}$ we have $\lambda\Lambda_\tau \subseteq \Lambda_\tau$, or

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

where $a, b, c, d \in \mathbb{Z}$. Thus

$$c\tau^2 + (d-a)\tau - b = 0, \qquad \tau \in \mathfrak{H},$$

meaning that $\mathbb{Q}(\tau)$ is an imaginary quadratic field. Note that λ is an algebraic integer. By Section 1.2 we have $\mathrm{End}(E_\tau) \cong \mathcal{O}$ for some order $\mathcal{O}$ in $\mathbb{Q}(\tau)$. By the Uniformization Theorem the same is true for any elliptic curve over $\mathbb{C}$ with a nontrivial endomorphism.

Theorem 1.3.4. *Let E be an elliptic curve with complex multiplication by a quadratic order $\mathcal{O}$. Then $j(E)$ is an algebraic number of degree at most $h(\mathcal{O})$.*

Proof. We may assume that $E = E_\tau$ for some $\tau \in \mathfrak{H}$. Suppose that

$$E_\tau \colon y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$$

has CM by $\mathcal{O}$. Let σ be any automorphism of $\mathbb{C}$. Then the elliptic curve

$$E_\tau^\sigma \colon y^2 = 4x^3 - g_2(\tau)^\sigma x - g_3(\tau)^\sigma$$

has also CM by $\mathcal{O}$, because the map

$$\begin{aligned} \mathrm{End}(E_\tau) &\longrightarrow \mathrm{End}(E_\tau^\sigma) \\ \phi &\mapsto \sigma \circ \phi \circ \sigma^{-1} \end{aligned}$$

is an isomorphism. By the Uniformization Theorem we can find $\omega \in \mathfrak{H}$ such that $E_\tau^\sigma \cong E_\omega$. The corresponding lattices Λ_τ and Λ_ω are proper ideals of the order $\mathcal{O}$. They are homothetic if and only if $j(E_\tau) = j(E_\omega)$. We have $j(E_\omega) = j(E_\tau^\sigma) = j(E_\tau)^\sigma$. There are exactly $h(\mathcal{O})$ classes of proper ideals of $\mathcal{O}$, implying that there are exactly $h(\mathcal{O})$ distinct values of the corresponding j-invariants. Therefore $j(E_\tau)$ has at most $h(\mathcal{O})$ conjugates. □

It can be shown that the degree of $j(E)$ is *exactly* $h(\mathcal{O})$ if E has CM by the order $\mathcal{O}$. In fact, the value $j(E_\tau)$ generates the Hilbert class field of the imaginary quadratic field $\mathbb{Q}(\tau)$. See for example [Deu58, 10.,11.].

2. Modular functions

In this chapter we describe the basic theory of modular functions. The references are [Lan87, 6.], [Shi94, 6.], and [DS05, 7.].

2.1 The modular group

The group $\mathrm{GL}_2^+(\mathbb{R})$ acts on the upper half-plane $\mathfrak{H}$ as follows. Let $\tau \in \mathfrak{H}$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{R})$. Then the action of γ is given by

$$(\gamma, \tau) \longmapsto \gamma\tau, \quad \text{where} \quad \gamma\tau = \frac{a\tau + b}{c\tau + d}.$$

The formula $\Im(\gamma\tau) = \det(\gamma)/|c\tau + d|^2$ shows that $\gamma\tau \in \mathfrak{H}$, so that this action is well defined.

The subgroup $\mathrm{SL}_2(\mathbb{Z})$ of $\mathrm{GL}_2^+(\mathbb{R})$ is called the **modular group**. Let Γ be a subgroup of $\mathrm{GL}_2^+(\mathbb{R})$. We define the **stabilizer** of a point $\tau \in \mathfrak{H}$ in the subgroup Γ by $\Gamma_\tau = \{\gamma \in \Gamma \colon \gamma\tau = \tau\}$. Let

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

Proposition 2.1.1. *(1)* $\mathrm{SL}_2(\mathbb{Z})$ *is generated by the matrices* T *and* S.
(2) We have $\mathrm{SL}_2(\mathbb{Z})_i = \langle S \rangle$ *and* $\mathrm{SL}_2(\mathbb{Z})_{\zeta_3} = \langle ST \rangle$.
(3) We have $\mathrm{SL}_2(\mathbb{Z})_\tau = \{\pm 1\}$ *for* $\tau \in \mathfrak{H}, \notin \mathrm{SL}_2(\mathbb{Z})i, \notin \mathrm{SL}_2(\mathbb{Z})\zeta_3$.
(4) Let $\mathcal{F} = \{\tau \in \mathfrak{H} \colon |\Re(\tau)| < 1/2$ *and* $|\tau| > 1\}$. *Then for every* $\tau \in \mathfrak{H}$ *there exist* $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ *such that* $\gamma\tau$ *lies in* $\overline{\mathcal{F}}$, *the closure of* $\mathcal{F}$ *in* $\mathfrak{H}$. *No two points of* $\mathcal{F}$ *are equivalent, and if* $\tau_1, \tau_2 \in \overline{\overline{\mathcal{F}}}$ *are such that* $\tau_1 = \gamma\tau_2$ *for some* $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, *then either* $\gamma = \pm T$ *and* $\tau_1 - \tau_2 = \pm 1$, *or* $\gamma = \pm S$ *and* $|\tau_1| = |\tau_2| = 1$.

Let N be a positive integer. We define $\Gamma(N)$ to be the kernel of the natural map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. The group $\Gamma(N)$ is called the **principal congruence subgroup** of level N. A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is called a **congruence subgroup** if $\Gamma(N) \subset \Gamma$ for some N.

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. We let $\Gamma\backslash\mathfrak{H} = \{\Gamma\tau \colon \tau \in \mathfrak{H}\}$. Quotients of this form are called **modular curves**, and they are denoted by $Y(\Gamma)$. A modular curve $Y(\Gamma)$ can be given the structure of a Riemann surface. We may compactify $Y(\Gamma)$ by adding a finite number of points which are called **cusps** of $Y(\Gamma)$ (or of Γ). The resulting compact Riemann surface is denoted by $X(\Gamma)$ (and is also called a modular curve).

We define $X(N) = X(\Gamma(N))$. The meromorphic functions on $X(N)$ are called **modular functions of level** N. One may apply the general theory of compact Riemann surfaces to conclude that the field of modular functions of level N has transcendence degree 1 over $\mathbb{C}$, thus determining a smooth projective algebraic curve over $\mathbb{C}$. This justifies the latter part of the name modular curve.

The arithmetic interest in modular curves comes from the fact that the equations of modular curves can be defined over $\mathbb{Q}$ (or possibly over a finite extension

of $\mathbb{Q}$). Therefore it makes sense to consider rational points on modular curves. Further, modular curves serve as a *moduli space* for elliptic curves, meaning that there is a bijection between the points of a modular curve and certain isomorphism classes of elliptic curves.

However, we shall not use modular curves here. In the next two sections we will consider modular functions as meromorphic functions on $\mathfrak{H}$ which are invariant under the action of some congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

2.2 Modular functions

We first define modular functions. Let f be a meromorphic function on $\mathfrak{H}$. Suppose that f is invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathfrak{H}$, that is, $f(\gamma\tau) = f(\tau)$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and all $\tau \in \mathfrak{H}$. Then, in particular, $f(\tau+1) = f(\tau)$ for every $\tau \in \mathfrak{H}$. Therefore we may write $f(\tau) = \tilde{f}(q)$, where $q = e^{2\pi i\tau}$ and $\tilde{f}$ is meromorphic inside the unit disc, except possibly at the origin. Let the Laurent series expansion about the origin of the function $\tilde{f}$ be $\tilde{f}(q) = \sum_{n\geq -\infty} a_n q^n$. We say that f is a **modular function** (or more precisely a **modular function of level** 1) if the Laurent series expansion of the associated function $\tilde{f}$ contains only a finite number of polar terms, that is $\tilde{f}(q) = \sum_{n\geq n_0} a_n q^n$, where $n_0 \in \mathbb{Z}$.

We call $\sum_{n\geq n_0} a_n q^n$ the **Fourier expansion** of the modular function f, and the coefficients a_n the **Fourier coefficients** of f.

Proposition 2.2.1. *The map*

$$\begin{aligned} &\mathfrak{H} \longrightarrow \{\textit{lattices}\} \longrightarrow \{\textit{elliptic curves over } \mathbb{C}\} \\ &\tau \longmapsto \Lambda_\tau \longmapsto E_\tau \end{aligned}$$

induces a bijection

$$\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H} \longleftrightarrow \frac{\{\textit{lattices}\}}{\textit{homothety}} \longleftrightarrow \frac{\{\textit{elliptic curves over } \mathbb{C}\}}{\textit{isomorphism over } \mathbb{C}}.$$

Proposition 2.2.2. *(1) The Fourier coefficients of j are integers.*

(2) The map $\tau \mapsto j(\tau)$ induces a bijection $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H} \to \mathbb{C}$. In other words, the function j maps $\mathfrak{H}$ onto $\mathbb{C}$, and we have $j(\tau_1) = j(\tau_2)$ for some $\tau_1, \tau_2 \in \mathfrak{H}$ if and only if $\tau_1 = \gamma\tau_2$, where $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

(3) Every modular function is a rational function in j.

(4) Every modular function that is holomorphic on $\mathfrak{H}$ is a polynomial in j.

(5) If a modular function is holomorphic on $\mathfrak{H}$ and also holomorphic at infinity, then it is constant.

2.3 Modular functions of higher level

Definition 2.3.1. *A function $f\colon \mathfrak{H} \to \mathbb{C}$ is called modular of level N if*

(1) *f is meromorphic on $\mathfrak{H}$,*

(2) *$f(A\tau) = f(\tau)$ for every $A \in \Gamma(N)$,*

(3) *The function $f \circ \gamma$ is meromorphic at infinity for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.*

Definition 2.3.2. *Let N be a positive integer, and let r and s be integers not both divisible by N. We define*

$$f_N^{(r,s)}(\tau) = \frac{g_2(\tau)}{g_3(\tau)} \wp_\tau \left(\frac{r\tau + s}{N} \right).$$

The functions $f_N^{(r,s)}$ are called the Fricke functions (after Robert Fricke). It is easy to see that the function $f_N^{(r,s)}$ depends only on the residue of (r, s) modulo N.

Proposition 2.3.3. *Let $\tau \in \mathfrak{H}$ be not congruent to i or ζ_3 modulo $\mathrm{SL}_2(\mathbb{Z})$. Suppose that $f_N^{(r_1,s_1)}(\tau) = f_N^{(r_2,s_2)}(\tau)$. Then $(r_1, s_1) \equiv \pm(r_2, s_2) \pmod N$.*

Proposition 2.3.4. *The functions $f_N^{(r,s)}$ are modular of level N. The modular group acts on them as a group of permutations: $f_N^{(r,s)}(\gamma\tau) = f_N^{(r,s)\gamma}(\tau)$ for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.*

Proposition 2.3.5. *Let N be a positive integer. There is a natural exact sequence*

$$1 \longrightarrow \Gamma(N) \longrightarrow \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \longrightarrow 1.$$

Proof. See for example [DS05, Exercise 1.2.2., p. 21] or [Lan87, §1.,p. 61]. □

Proposition 2.3.6. *Let N be a positive integer and let $Q = q^{1/N}$. We have for $\tau \in \mathfrak{H}$*

$$f_N^{(r,s)}(\tau) = P(q) \left(\frac{1}{12} + \frac{Q^r \zeta_N^s}{(1 - Q^r \zeta_N^s)^2} + \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} n q^{mn} (Q^{-rn} \zeta_N^{-sn} + Q^{rn} \zeta_N^{sn} - 2) \right),$$

where P is a power series with integer coefficients.

Lemma 2.3.7. *Let $\alpha \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be such that $u\alpha = \varepsilon_u u$ for every $u \in s_N$, where $\varepsilon_u = \pm 1$. Then $\alpha = \pm 1$.*

Lemma 2.3.8. *Let $\tau \in \mathfrak{H}_1$, and let $\alpha \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be such that $f_N^{u\alpha}(\tau) = f_N^u(\tau)$ for all $u \in s_N$. Then $\alpha = \pm 1$.*

Lemma 2.3.9. *Let $\alpha \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be such that $f_N^{u\alpha} = f_N^u$ for all $u \in s_N$. Then $\alpha = \pm 1$.*

We define

$$F_{N,\mathbb{C}} = \mathbb{C}(j, f_N^{(r,s)} : (r, s) \in s_N),$$
$$F_N = \mathbb{Q}(j, f_N^{(r,s)} : (r, s) \in s_N).$$

Theorem 2.3.10. *The field extension $F_{N,\mathbb{C}}/\mathbb{C}(j)$ is Galois, and*

$$\mathrm{Gal}(F_{N,\mathbb{C}}/\mathbb{C}(j)) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}.$$

Moreover, the field $F_{N,\mathbb{C}}$ coincides with the field of all modular functions of level N.

Proof. Let $R_{N,\mathbb{C}}$ be the field of modular functions of level N, and consider the homomorphism

$$\begin{aligned} \theta\colon \mathrm{SL}_2(\mathbb{Z}) &\longrightarrow \mathrm{Aut}(R_{N,\mathbb{C}}), \\ \gamma &\longmapsto \theta(\gamma), \end{aligned}$$

where the automorphism $\theta(\gamma)$ acts on $R_{N,\mathbb{C}}$ by $f \mapsto f \circ \gamma$. To show that this is a well defined homomorphism, we must show that $f \circ \gamma$ is an element of $R_{N,\mathbb{C}}$. The group $\Gamma(N)$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$, so if $\alpha \in \Gamma(N)$, then there exists $\alpha' \in \Gamma(N)$ such that $\gamma\alpha = \alpha'\gamma$, and thus $f \circ \gamma \circ \alpha = f \circ \alpha' \circ \gamma = f \circ \gamma$. The other conditions for $f \in$ to be in $R_{N,\mathbb{C}}$ are satisfied automatically.

Now we determine the kernel of the homomorphism θ. By the definition of $R_{N,\mathbb{C}}$ we have $\pm 1\Gamma(N) \subset \ker\theta$. To prove the opposite inclusion, suppose that $\gamma \in \ker\theta$. Let $\overline{\gamma}$ be the image of γ in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. We know that $f_N^{(r,s)} \in R_{N,\mathbb{C}}$ and $f_N^{(r,s)} \circ \gamma = f_N^{(r,s)\overline{\gamma}}$ for all $(r,s) \in s_N$. We apply Lemma 2.3.9 to obtain $\overline{\gamma} = \pm 1$. Therefore $\ker\theta = \pm\Gamma(N)$, and there is an injection

$$\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\} \cong \mathrm{SL}_2(\mathbb{Z})/\pm\Gamma(N) \hookrightarrow \mathrm{Aut}(R_{N,\mathbb{C}}).$$

Let G_N denote the image $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ in $\mathrm{Aut}(R_{N,\mathbb{C}})$. Then G_N is a finite group of automorphisms of $R_{N,\mathbb{C}}$ whose fixed field is the field of modular functions of level N invariant under the full $\mathrm{SL}_2(\mathbb{Z})$, that is, the field $\mathbb{C}(j)$. Therefore the extension $R_{N,\mathbb{C}}/\mathbb{C}(j)$ is Galois and the corresponding Galois group is G_N (see [Mil18, Theorem 3.10 (c), p. 38]).

It remains to prove that $F_{N,\mathbb{C}} = R_{N,\mathbb{C}}$. By Lemma 2.3.9 every automorphism fixing the functions $f_N^{(r,s)}$ for all $(r,s) \in s_N$ must be induced by a matrix in $\pm\Gamma(N)$. Therefore the subgroup corresponding to the subextension $R_{N,\mathbb{C}}/F_{N,\mathbb{C}}$ is trivial, and so $F_{N,\mathbb{C}} = R_{N,\mathbb{C}}$ as asserted. □

Theorem 2.3.11. *The field extension $F_N/\mathbb{Q}(j)$ is Galois, and*

$$\mathrm{Gal}(F_N/\mathbb{Q}(j)) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}.$$

Proof. Every automorphism of the field $\mathbb{Q}(\zeta_N)$ extends to an automorphism of $\mathbb{Q}(\zeta_N)((q^{1/N}))$ by acting on the coefficients of the formal Laurent series. We know that $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$ (see [Mil18, Theorem 5.10, p. 63]). For $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ let σ_d denote the automorphism of $\mathbb{Q}(\zeta_N)$ determined by $\zeta_N^{\sigma_d} = \zeta_N^d$. Proposition 2.3.6 implies that the extension of σ_d to $\mathbb{Q}(\zeta_N)((q^{1/N}))$ (which we will denote by the same symbol) acts on the functions $\{f_N^{(r,s)} : (r,s) \in s_N\}$ by $(f_N^{(r,s)})^{\sigma_d} = f^{(r,ds)}$. Since the Fourier coefficients of j lie in $\mathbb{Q}$, the automorphism σ_d restricts to an automorphism $F_N \to F_N$ which we will again denote by σ_d. Consequently, we get an injection

$$\begin{aligned} (\mathbb{Z}/N\mathbb{Z})^\times &\hookrightarrow \mathrm{Aut}(F_N/\mathbb{Q}(j)), \\ d &\longmapsto \sigma_d. \end{aligned}$$

On the other hand, the group $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on $\{f_N^{(r,s)} : (r,s) \in s_N\}$ by $f_N^{(r,s)} \circ \gamma = f^{(r,s)\overline{\gamma}}$, where $\overline{\gamma} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and γ is a lift of $\overline{\gamma} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ to $\mathrm{SL}_2(\mathbb{Z})$.

We can now use the exact sequence of Proposition 2.3.5 to combine these two actions, obtaining an injection

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\} \hookrightarrow \mathrm{Aut}(F_N). \tag{2.1}$$

More precisely, if $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ then the matrix A can be uniquely represented as $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & a \end{smallmatrix}\right) \alpha$, where $a = \det A$ and $\alpha \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Hence the automorphism corresponding to the matrix A is $\sigma_a \circ \alpha$.

Let G_N be the image of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ in $\mathrm{Aut}(F_N)$ (see (2.1)). Then G_N is a finite group of automorphisms of F_N. The fixed field of G_N consists of those functions f in F_N which are invariant both under the action of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and the action of $(\mathbb{Z}/N\mathbb{Z})^\times$. The former condition requires f to be of level one. The latter requires f to lie in $\mathbb{Q}(j)$ by virtue of Proposition 2.2.2, (1). Therefore the fixed field of G_N is $\mathbb{Q}(j)$, implying that the extension $F_N/\mathbb{Q}(j)$ is Galois with Galois group $G_N \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ (see [Mil18, Theorem 5.10, p. 63]). □

Proposition 2.3.12. *We have $\mathbb{C} \cap F_N = \mathbb{Q}(\zeta_N)$. In particular ζ_N is an element of F_N.*

Proof. Let $k = \mathbb{C} \cap F_N$. We have $\mathbb{C}(j) \cdot F_N = F_{N,\mathbb{C}}$ because $F_{N,\mathbb{C}} = \mathbb{C}(j, f_N^{(r,s)} : (r,s) \in s_N)$. Note that $k(j) = \mathbb{C}(j) \cap F_N$. Therefore (see [Mil18, Proposition 3.18, p. 40])

$$\mathrm{Gal}(F_N/k(j)) \cong \mathrm{Gal}(F_{N,\mathbb{C}}/\mathbb{C}(j)) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}.$$

In particular $[F_N : k(j)] = \#\,\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$, and so

$$[k(j) : \mathbb{Q}(j)] = \#\,\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\,\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \#\,(\mathbb{Z}/N\mathbb{Z})^\times\,.$$

Consequently, $[k : \mathbb{Q}] = \#\,(\mathbb{Z}/N\mathbb{Z})^\times = [\mathbb{Q}(\zeta_N) : \mathbb{Q}]$. On the other hand, we have $k \subset \mathbb{Q}(\zeta_N)$ because $F_N \subset k((q^{1/N}))$. Thus $k = \mathbb{Q}(\zeta_N)$ as asserted. □

Proposition 2.3.13. *The field F_N consists of all modular functions of level N whose Fourier coefficients lie in the field $\mathbb{Q}(\zeta_N)$.*

Proof. Since the extension $F_{N,\mathbb{C}}/\mathbb{C}(j)$ is finite and separable there exists an element $g_N \in F_{N,\mathbb{C}}$ such that $F_{N,\mathbb{C}} = \mathbb{C}(j, g_N)$ (see [Mil18, Theorem 5.1, p. 59]). Moreover, we can choose the function g_N to be a linear combination of $f_N^{(r,s)}$ with rational coefficients, assuring that g_N has Fourier coefficients in $\mathbb{Q}(\zeta_N)$ (see [Mil18, Remark 5.2, p. 60]). Now let $h \in F_{N,\mathbb{C}}$ and suppose that the Fourier coefficients of h lie in ζ_N. We can write $h = R(j, g_N)$, where R is a rational function. All three functions h, j, and g_N have Fourier coefficients in $\mathbb{Q}(\zeta_N)$. Therefore comparing the coefficients of each power of $q^{1/N}$ in the relation $h = R(j, g_N)$, we obtain a system of linear equations with coefficients in $\mathbb{Q}(\zeta_N)$ whose solution are the coefficients of R. Thus R has coefficients in $\mathbb{Q}(\zeta_N)$, so $h \in \mathbb{Q}(\zeta_N, j, g_N) = F_N$ (see Proposition 2.3.12), and we are done. □

2.4 Transformation equations

We define

$$\mathcal{M}_m = \left\{ \begin{pmatrix} r & s \\ 0 & t \end{pmatrix} : r > 0, rt = m, 0 \le s < t \right\}.$$

The set $\mathcal{M}_m$ is a set of representatives for the left action of $\mathrm{SL}_2(\mathbb{Z})$ on the set of 2-by-2 matrices with integer entries and determinant equal to m. If f is a modular function, let $\Gamma(f)$ be the exact subgroup of $\mathrm{SL}_2(\mathbb{Z})$ under which the function f is invariant. Let α be a 2-by-2 matrix with positive determinant. We define

$$R_{\alpha,\Gamma(f)} = \{A\alpha B \colon A, B \in \Gamma(f)\}.$$

The group $\Gamma(f)$ acts on the set $R_{\alpha,\Gamma(f)}$ from right and left. We denote by

$$\Gamma(f)\backslash R_{\alpha,\Gamma(f)}$$

any set of representatives for the left action.

Theorem 2.4.1. *Let $f \in F_{N,\mathbb{C}}$ be such that $\mathbb{C}(j) \subset \mathbb{C}(f)$, and let $\alpha \in \mathcal{M}_m$. The minimal polynomial of the function $f \circ \alpha$ over the field $\mathbb{C}(f)$ is*

$$\prod_{M \in \Gamma(f)\backslash R_{\alpha,\Gamma(f)}} (X - f \circ M)\,. \tag{2.2}$$

Proof. From the definition of the set $R_{\alpha,\Gamma(f)}$ we see that the Galois group

$$\mathrm{Gal}(F_{mN,\mathbb{C}}/\mathbb{C}(f)) \cong \Gamma_N(f)$$

acts on the roots of the polynomial (2.2). We must show that it acts transitively. Let $M_1, M_2 \in R_{\alpha,\Gamma(f)}$. Write $M_1 = A_1\alpha B_1$ and $M_2 = A_2\alpha B_2$, where $A_1, A_2, B_1, B_2 \in \Gamma(f)$. We observe that the automorphism given by the matrix $\overline{B_1^{-1}B_2} \in \Gamma_N(f)$ maps the function $f \circ M_1 = f \circ \alpha \circ B_1$ to the function $f \circ M_2 = f \circ \alpha \circ B_2$. This concludes the proof. □

Lemma 2.4.2. *Let $f \in F_N$ and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Let $\sigma_d \in \mathrm{Gal}(F_N/\mathbb{Q}(j))$ be the automorphism induced by $d \in (\mathbb{Z}/N\mathbb{Z})^\times$. Let $D = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$. Let $\overline{\gamma}$ be the image of γ in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Let γ' be a lift of the matrix $D^{-1}\overline{\gamma}D$ to $\mathrm{SL}_2(\mathbb{Z})$. Then we have*

$$(f \circ \gamma)^{\sigma_d} = f^{\sigma_d} \circ \gamma'. \tag{2.3}$$

Proof. Since the field F_N is generated over $\mathbb{Q}(j)$ by the Fricke functions $f_N^{(r,s)}$, it is sufficient to prove the relation (2.3) for them. Let $(r,s) \in s_N$. By Proposition 2.3.4 and Theorem 2.3.11 we have

$$(f_N^{(r,s)} \circ \gamma)^{\sigma_d} = f_N^{(r,s)\overline{\gamma}D} = f_N^{(r,s)D\overline{\gamma'}} = (f_N^{(r,s)})^{\sigma_d} \circ \gamma'.$$

This completes the proof. □

Lemma 2.4.3. *Suppose that $f \in F_N$ has rational Fourier coefficients. Suppose that $(m,N) = 1$. Let $M \in \mathcal{M}_m$ be a diagonal matrix. Let $\overline{M}$ be the image of M in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Then the group $\Gamma_N(f)$ is stable under conjugation by $\overline{M}$. In other words, we have $\overline{M}^{-1}\Gamma_N(f)\overline{M} \subset \Gamma_N(f)$.*

Proof. Write $\overline{M} = \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$, where $a, b \in (\mathbb{Z}/N\mathbb{Z})^\times$. Since $\overline{M} = a\left(\begin{smallmatrix} 1 & 0 \\ 0 & a \end{smallmatrix}\right)^{-1}\left(\begin{smallmatrix} 1 & 0 \\ 0 & b \end{smallmatrix}\right)$, it is sufficient to prove the lemma for matrices of the type $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$ where $d \in (\mathbb{Z}/N\mathbb{Z})^\times$. Let $A \in \Gamma_N(f)$. As the matrix $A' = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)^{-1} A \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$ has determinant equal to 1, it is an element of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Furthermore, since the function f has rational Fourier coefficients, it is fixed, for every $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, by the automorphism σ_d in $\mathrm{Gal}(F_N/\mathbb{Q}(j))$ corresponding to the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$, (see Theorem 2.3.11). Therefore $A' \in \Gamma_N(f)$. □

Theorem 2.4.4. *Let $f \in F_N$ and $\alpha \in \mathcal{M}_m$. Assume that $(N, m) = 1$ and that both f and $f \circ \alpha$ have rational Fourier coefficients. The minimal polynomial of the function $f \circ \alpha$ over the field $\mathbb{Q}(f)$ is*

$$\prod_{M \in \Gamma(f) \backslash R_{\alpha,\Gamma(f)}} (X - f \circ M). \tag{2.4}$$

Proof. By Theorem 2.4.1 the polynomial (2.4) is the minimal polynomial of $f \circ \alpha$ over $\mathbb{C}(f)$. Therefore to show that it is defined over $\mathbb{Q}(f)$ we must show that the set

$$\{f \circ M : M \in R_{\alpha,\Gamma(f)}\}$$

is stable under the Galois action induced by $(\mathbb{Z}/mN\mathbb{Z})^\times$. Let $d \in (\mathbb{Z}/mN\mathbb{Z})^\times$, $D = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$, and let $\sigma_d \in \mathrm{Gal}(F_{mN}/\mathbb{Q}(j))$ be the corresponding automorphism. Take $M \in R_{\alpha,\Gamma(f)}$. Then $M = A\alpha B$ for some $A, B \in \Gamma(f)$. Since the function $f \circ \alpha$ has rational Fourier coefficients, Lemma 2.4.2 applies to it, and we obtain

$$\begin{aligned}(f \circ M)^{\sigma_d} &= (f \circ \alpha \circ B)^{\sigma_d} \\ &= (f \circ \alpha)^{\sigma_d} \circ B' \quad \text{where } B' \text{ is a lift of } D^{-1}BD \text{ to } \mathrm{SL}_2(\mathbb{Z}), \\ &= f \circ \alpha \circ B' \quad \text{because } f \circ \alpha \text{ has rational Fourier coefficients.}\end{aligned}$$

But according to Lemma 2.4.3 the matrix B' is an element of $\Gamma(f)$. Therefore $\alpha B' \in R_{\alpha,\Gamma(f)}$, and we are done. □

2.5 Examples of modular functions

Definition 2.5.1. *We define*

$$\gamma_2(\tau) = j(\tau)^{1/3},$$

the cube root being chosen in such a way that γ_2 has rational Fourier coefficients.

It is easy to see that the function γ_2 is well-defined because all zeros of the j-invariant have order 3. The function γ_2 is called the Weber modular function. For more details see [Cox11, §12,A, p. 249].

Proposition 2.5.2. *Let $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. We have*

$$\gamma_2 \circ S = \gamma_2, \quad \gamma_2 \circ T = \zeta_3^{-1}\gamma_2.$$

Proof. See [Cox11, §12,A, Proposition 12.3. p. 250]. □

Definition 2.5.3. *We define*

$$\eta(\tau) = \frac{1}{(2\pi)^{1/2}}\Delta(\tau)^{1/24},$$

the 24-th root being chosen in such a way that $\eta(\tau)$ is positive for $\tau \in \mathfrak{H}$ purely imaginary. The function η is called the Dedekind eta function.

Proposition 2.5.4. *Let $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. We have*

$$\eta(S\tau) = (-i\tau)^{1/2}\eta(\tau), \quad \eta(T\tau) = \zeta_{24}\eta(\tau).$$

Proof. See [Cox11, §12,B, Corollary 12.19, p. 259]. □

Definition 2.5.5. *We define*

$$\mathfrak{f} = \zeta_{48}^{-1}\frac{\eta \circ \left(\begin{smallmatrix} 1 & 1 \\ 0 & 2 \end{smallmatrix}\right)}{\eta}, \quad \mathfrak{f}_1 = \frac{\eta \circ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)}{\eta}, \quad \mathfrak{f}_2 = \sqrt{2}\frac{\eta \circ \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)}{\eta}.$$

These functions are called the Schläfli's modular functions (after Ludwig Schläfli). Note that they are holomorphic and nonzero on $\mathfrak{H}$.

Proposition 2.5.6. *Let* $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ *and* $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. *We have*

$$(\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2) \circ S = (\mathfrak{f}, \mathfrak{f}_2, \mathfrak{f}_1),$$
$$(\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2) \circ T = (\zeta_{48}^{-1}\mathfrak{f}_1, \zeta_{48}^{-1}\mathfrak{f}, \zeta_{48}^{2}\mathfrak{f}_2).$$

Proof. See [Cox11, §12,B, Corollary 12.19, p. 259]. □

Proposition 2.5.7. *We have*

$$\gamma_2 \circ \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \zeta_3^{ab-ac+cd-a^2cd}\gamma_2 \quad \textit{for } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Proof. See [Cox11, §12,A, Proposition 12.3. p. 250]. □

Proposition 2.5.8. *We have*

$$\mathfrak{f}^3 \circ \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \zeta_{16}^{2cd+2ad-ac-bd-2d^2}\mathfrak{f}^3 \quad \textit{for } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(\mathfrak{f}^{24}).$$

Proof. See [Web08, §40, p. 134]. □

Proposition 2.5.9. *We have*

$$\gamma_2 = \frac{\mathfrak{f}^{24} - 16}{\mathfrak{f}^8}.$$

Proof. See [Cox11, §12,B, Theorem 12.17., p. 257]. □

Proposition 2.5.10. *We have for* $\tau \in \mathfrak{H}$

$$\mathfrak{f}_1(2\tau)\mathfrak{f}_2(\tau) = \sqrt{2}.$$

Proof. See [Cox11, §12,B, Exercise 12.9]. □

Proposition 2.5.11. *Let* $\tau, \omega \in \mathfrak{H}$ *and* $a \in \{3, 24\}$. *We have* $\mathfrak{f}(\tau)^a = \mathfrak{f}(\omega)^a$ *if and only if* $\tau = A\omega$ *where* $A \in \Gamma(\mathfrak{f}^a)$.

Using the above general transformation formulas, we can easily compute the exact subgroups of $\mathrm{SL}_2(\mathbb{Z})$ under which the functions $\gamma_2, \mathfrak{f}^3$ and $\mathfrak{f}^{24}$ are invariant.

Proposition 2.5.12. *We have*

$$\Gamma(\gamma_2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix} \textit{ or } \begin{pmatrix} * & t \\ t & * \end{pmatrix} \textit{ for some } t \pmod 3 \right\}.$$

Proposition 2.5.13. *We have*

$$\Gamma(\mathfrak{f}^3) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(\mathfrak{f}^{24}) : a + d \equiv 0 \pmod{16} \textit{ or } b \equiv c \pmod{16} \right\}.$$

Proposition 2.5.14. *We have*

$$\Gamma(\mathfrak{f}^{24}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \textit{ or } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \pmod 2 \right\}.$$

3. Class invariants

3.1 Integrality of the j-invariant

In this section we prove that $j(\tau)$ is an algebraic integer whenever τ is a CM point. We give the classical analytic proof. There are also at least two different algebraic proofs, but they are more difficult. See [Rob73, III,3.], and especially [Sil11, II.,§6., p. 140]. We have followed [Lan87, 5,§2, Theorem 3 and 4, p. 55-57] and [Shi94, 4.6., p. 107].

Lemma 3.1.1. *Let f be a modular function of level one holomorphic on $\mathfrak{H}$. Write $f = \sum_{n=-N} a_n q^n$. Suppose that the Fourier coefficients a_n are algebraic integers. Then $f = P(j)$, where P is a polynomial whose coefficients are algebraic integers.*

Proof. By Proposition 2.2.2, (1) we have

$$j = \frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n,$$

where the coefficients c_n are integers. Subtracting a suitable multiple of a power of the j-invariant from the function f we obtain

$$f - a_{-N} j^N = \left(\frac{a_{-N}}{q^N} + \cdots\right) - a_{-N}\left(\frac{1}{q} + c_0 + \cdots\right)^N = \frac{d_{N-1}}{q^{N-1}} + \cdots,$$

where the coefficients d_n are algebraic integers. Continuing in this manner we eliminate all polar terms contained in the Fourier expansion of f. Thus there is a polynomial P, whose coefficients are algebraic integers, and such that the function $f - P(j)$ is holomorphic at infinity. Since f was assumed holomorphic on $\mathfrak{H}$, Proposition 2.2.2, (5) implies that $f - P(j) = c$ for some $c \in \mathbb{C}$. The number c must be algebraic because it is equal to the constant coefficient of the Fourier expansion of the function $f - P(j)$. □

Let $m > 1$ be an integer. There is only one orbit in $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{M}_m/\mathrm{SL}_2(\mathbb{Z})$, namely $\mathrm{SL}_2(\mathbb{Z})\left(\begin{smallmatrix} m & 0 \\ 0 & 1 \end{smallmatrix}\right)\mathrm{SL}_2(\mathbb{Z})$. Therefore for every $\alpha \in \mathcal{M}_m$ the minimal polynomial of the function $j\circ\alpha$ over the field $\mathbb{Q}(j)$ is the same as the minimal polynomial of $j \circ \left(\begin{smallmatrix} m & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Consequently, for a fixed m, there is only one modular polynomial for j of order m. We denote it by $\Phi_m^j(X, Y)$.

Proposition 3.1.2. *Let m be a positive integer. The polynomial $\Phi_m^j(X, Y)$ has integer coefficients.*

Proof. The set

$$\mathcal{S}_{m,1} = \left\{ \begin{pmatrix} r & s \\ 0 & t \end{pmatrix} : r > 0, rt = m, 0 \le s < t, (r, s, t) = 1 \right\}$$

is a set of representatives for $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{M}_m$. Therefore

$$\Phi_m^j(X, j) = \prod_{M \in \mathcal{S}_{m,1}} (X - j \circ M).$$

We see that the coefficients of the polynomial $\Phi_m^j(X,j)$ are the elementary symmetric polynomials in the functions $j \circ \left(\begin{smallmatrix} r & s \\ 0 & t \end{smallmatrix}\right) = \sum_{n=-1}^{\infty} \zeta_n^{rs} c_n q^{r^2 n}$, where the c_n are integers. This reveals to us that the Fourier coefficients of the coefficients of $\Phi_m^j(X,j)$ are algebraic integers. Thus Lemma 3.1.1 shows that $\Phi_m^j(X,Y)$ has algebraic coefficients. However, the function $j \circ \left(\begin{smallmatrix} m & 0 \\ 0 & 1 \end{smallmatrix}\right)$ has rational Fourier coefficients, and so by Theorem 2.4.4 the polynomial $\Phi_m^j(X,Y)$ has rational coefficients. Therefore they must be in fact integers. □

Proposition 3.1.3. *Suppose that m is not a square. Then the leading coefficient of the polynomial $\Phi_m^j(X,X)$ is ± 1.*

Proof. The leading coefficient of $\Phi_m^j(X,X)$ is equal to the coefficient of the lowest polar term in the Fourier expansion of $\Phi_m^j(j,j)$. On the other hand,

$$\Phi_m^j(j,j) = \prod_{M \in \mathcal{S}_{m,1}} (j - j \circ M),$$

and the polar part of the Fourier expansion of $j - j \circ \left(\begin{smallmatrix} r & s \\ 0 & t \end{smallmatrix}\right)$ is $q^{-1} - \zeta_n^{rs} q^{-r^2/n}$. Since m is not a square, cancellation cannot occur, and so the leading Fourier coefficient of $j - j \circ \left(\begin{smallmatrix} r & s \\ 0 & t \end{smallmatrix}\right)$ is a root of unity. Consequently the leading coefficient of $\Phi_m^j(X,X)$ is also a root of unity. By Proposition 3.1.2 it is an integer. Therefore it must be ± 1. □

Theorem 3.1.4. *Let τ be a CM point. Then $j(\tau)$ is an algebraic integer.*

Proof. Let $K = \mathbb{Q}(\tau)$. First, we prove the theorem in the case when $\mathcal{O}_\tau$ is the maximal order of K. Then one can choose an element μ of $\mathcal{O}_\tau$ such that its norm $N(\mu)$ is a squarefree integer $m > 1$. Indeed, if $K = \mathbb{Q}(i)$, then take $\mu = 1 + i$, and if $K = \mathbb{Q}(\sqrt{-m})$ with $m > 1$ squarefree, then take $\mu = \sqrt{-m}$. Since multiplication by elements of $\mathcal{O}_\tau$ preserves the lattice $[\tau, 1]$, we have

$$\mu \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \tau \\ 1 \end{pmatrix}, \tag{3.1}$$

where the matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ has integral entries. A little calculation shows that

$$\mu^2 - (a+d)\mu + ad - bc = 0.$$

In other words $\det M = m$. Moreover, because m is squarefree, the matrix M is primitive. Now (3.1) implies $M\tau = \tau$. Therefore $j(M\tau) = j(\tau)$, and consequently $\Phi_m^j(j(\tau), j(\tau)) = 0$. By the effect of Proposition 3.1.2 and Proposition 3.1.3 the polynomial $\Phi_m^j(X,X)$ has integer coefficients while the leading one is ± 1. This shows that $j(\tau)$ is an algebraic integer.

Now we resolve the case when $\mathcal{O}_\tau$ is not the maximal order of K. Let $\mathcal{O}_\omega$ be the maximal order of K. Then since $(\omega, 1)$ is a basis for K over $\mathbb{Q}$, there exists a matrix $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ such that $\tau = \alpha\omega$. We may assume that α has integral entries and that it is primitive. Accordingly we have $\Phi_n^j(j(\tau), j(\omega)) = 0$ and $n = \det \alpha$ is not a square. Therefore by Proposition 3.1.2 and Proposition 3.1.3 $j(\tau)$ is integral over $\mathbb{Z}[j(\omega)]$. But we already proved the theorem for maximal orders, so $j(\omega)$ is integral over $\mathbb{Z}$, implying the integrality of $j(\tau)$. □

3.2 Weber's determination of class invariants

In this section we show how to prove Weber's theorems on class invariants. We follow Weber's book *Lehrnuch der Algebra* [Web08] and Stark's article [Sta69]. From Section 2.4 we know that if both the modular functions f and $f \circ \alpha$ have rational coefficients Fourier and $\mathbb{Q}(j) \subset \mathbb{Q}(f)$, then the minimal polynomial of $f \circ \alpha$ over $\mathbb{Q}(f)$ is

$$\phi(X) = \prod_{M \in \Gamma(f) \backslash R_{\alpha,\Gamma(f)}} (X - f \circ M).$$

We will always take $\alpha = \left(\begin{smallmatrix} m & \\ & 1 \end{smallmatrix}\right)$. Write

$$\phi(X) = X^d - s_1(f)X^{d-1} + \cdots (-1)^d s_d(f),$$

where the coefficients s_i are rational functions in f. If f is holomorphic on $\mathfrak{H}$, then s_i are polynomials in f. This is the case for functions which we will be interested in. We may therefore consider the polynomial in two variables and with rational coefficients

$$\Phi_f(X, Y) = \phi(X) = X^d - s_1(Y)X^{d-1} + \cdots (-1)^d s_d(Y).$$

We have in particular

$$\phi_f(X, f(\tau)) = \prod_{M \in \Gamma(f) \backslash R_{\alpha,\Gamma(f)}} (X - f(M\tau)).$$

The important thing now is that $\Phi_f(f(\tau), f(\tau)) = 0$ for some τ if and only if $f(\tau) = f(M\tau)$ for some $M \in R_{\alpha,\Gamma(f)}$. For functions which we will be interested in, the latter statement is equivalent to $\tau = AM\tau$ for some $A \in \Gamma(f), M \in R_{\alpha,\Gamma(f)}$. What this injectivity means is that the function f is a uniformizer of a modular curve of genus 0, that is, it gives a bijection between the modular curve and the projective line.

For the modular functions γ_2 and $\mathfrak{f}^{24}$ the transformation polynomials can be described more explicitly. Let n, d be relatively prime positive integers. We define

$$\mathcal{S}(n, d) = \left\{ \begin{pmatrix} r & s \\ 0 & t \end{pmatrix} : r > 0, rt = n, (r, t, s) = 1, d \mid s, 0 \le s < dt \right\}.$$

Then our transformation polynomials for the matrix $\alpha = \left(\begin{smallmatrix} n & \\ & 1 \end{smallmatrix}\right)$ are

$$\phi_{\gamma_2}(X, \gamma_2(\tau)) = \prod_{M \in \mathcal{S}(n,3)} (X - f(M\tau)),$$
$$\phi_{\mathfrak{f}^{24}}(X, \mathfrak{f}^{24}(\tau)) = \prod_{M \in \mathcal{S}(n,16)} (X - f(M\tau)).$$

We give two proofs of Weber's theorem concerning $\mathfrak{f}^{24}$.

Theorem 3.2.1. *Let p be a positive integer and let $\theta_p = \sqrt{-p}$. Then $\mathfrak{f}(\theta_p)^{24} \in \mathbb{Q}(j(\theta_p))$.*

Proof. Let $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. The numbers

$$\mathfrak{f}(\theta_p)^{24}, \quad \mathfrak{f}(T\theta_p)^{24}, \quad \mathfrak{f}(TST\theta_p)^{24}$$

are the roots of the equation

$$(X-16)^3 - j(\theta_p)X = 0. \tag{3.2}$$

Note that $\left(\begin{smallmatrix} 0 & -p \\ 1 & 0 \end{smallmatrix}\right)\theta_p = \theta_p$. Since $\left(\begin{smallmatrix} 0 & -p \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$, we obtain another equation for $\mathfrak{f}(\tau)^{24}$, namely $\Phi_{\mathfrak{f}^{24}}(\mathfrak{f}(\theta_p), \mathfrak{f}(\theta_p)) = 0$, where $\alpha_p = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Let $M \in \mathcal{M}_p$ be a matrix fixing θ_p. Comparison of the relations $\left(\begin{smallmatrix} 0 & -p \\ 1 & 0 \end{smallmatrix}\right)\theta_p = \theta_p$ and $M\theta_p = \theta_p$ shows that there are integers s and u such that $M = \left(\begin{smallmatrix} s & -pu \\ u & s \end{smallmatrix}\right)$. Consequently $\det M = s^2 + pu^2$. But we assumed that $\det M = p$, so we must have $s = 0$ and $u = \pm 1$. Therefore there is only one matrix (modulo ± 1) in $\mathcal{M}_p$ fixing θ_p.

We contend that the numbers $\mathfrak{f}(T\theta_p)^{24}$ and $\mathfrak{f}(TST\theta_p)^{24}$ cannot be roots of the equation $\Phi_{\mathfrak{f}^{24}}(X, X) = 0$. To prove this, it is sufficient to demonstrate that there is no matrix N in $\Gamma(\mathfrak{f}^{24})\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\Gamma(\mathfrak{f}^{24})$ fixing $T\theta_p$ or $TST\theta_p$.

The relation $NT\theta_p = T\theta_p$ leads to

$$T^{-1}NT\theta_p = \theta_p. \tag{3.3}$$

Similarly, $NTST\theta_p = TST\theta_p$ implies

$$T^{-1}S^{-1}T^{-1}NTST\theta_p = \theta_p. \tag{3.4}$$

Since $N \in \Gamma(\mathfrak{f}^{24})\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\Gamma(\mathfrak{f}^{24})$, we have $N \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \pmod 2$. Therefore the matrices in (3.3) and (3.4) are congruent to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ modulo 2. However, we have just proved that the only matrix in $\mathcal{M}_m$ fixing θ_p is $\pm\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ which is a contradiction.

Consequently, the equations (3.2) and $\Phi_{\mathfrak{f}^{24}}(X, X) = 0$ have only the root $\mathfrak{f}(\theta_p)^{24}$ in common. Because they have both coefficients in $\mathbb{Q}(j(\theta_p))$ we must have $f(\theta_p)^{24} \in \mathbb{Q}(j(\theta_p))$. □

Lemma 3.2.2. *Let n be a positive integer such that $n \equiv -1 \pmod 3$. Suppose that the number $\omega \in \mathfrak{H}$ satisfies $\omega^2 + B\omega + C = 0$, where B, C are integers. If $\gamma_2(\omega) \neq 0$ is a root of the polynomial $\Phi_{\gamma_2}(X, X)$, then $B \equiv 0 \pmod 3$.*

Proof. If $\Phi_{\gamma_2}(\gamma_2(\omega), \gamma_2(\omega)) = 0$ and $\gamma_2(\omega) \neq 0$ then by our observations above there exists $\left(\begin{smallmatrix} r & s \\ 0 & t \end{smallmatrix}\right) \in \mathcal{S}(n, 3)$ such that $\gamma_2(\omega) = \gamma_2\left(\frac{r\omega+s}{t}\right)$. The transformation formula for γ_2 implies

$$\frac{a\omega + b}{c\omega + d} = \frac{r\omega + s}{t},$$

with $ad - bc = 1$, and

$$ab - ac + cd - a^2cd \equiv 0 \pmod 3. \tag{3.5}$$

This gives us a second quadratic equation

$$rc\omega^2 + (dr - ta + cs)\omega + (sd - bt) = 0$$

Comparing it with $\omega^2 + B\omega + c = 0$, we obtain

$$cr = u, \tag{3.6}$$

$$dr - ta + cs = Bu, \tag{3.7}$$

$$sd - bt = Cu, \tag{3.8}$$

where u is an integer. Since $(r,3)=1$, the number u is divisible by 3 if and only if c is.

Suppose that this were the case. The determinant condition implies $ad \equiv 1 \pmod 3$. In particular, the numbers a and d are not divisible by 3. Because s is divisible by 3, we see from (3.7) that $dr \equiv ta \pmod 3$. Therefore $ad \equiv rt = n \equiv -1 \pmod 3$, a contradiction.

Hence the numbers c, u are not divisible by 3. Multiplying the congruence (3.5) by c, we obtain

$$\begin{aligned} a(ad-1) - a + d - a^2 d &\equiv 0 \pmod 3, \\ a + d &\equiv 0 \pmod 3. \end{aligned}$$

Since $rt \equiv -1 \pmod 3$ we have also $t \equiv -r \pmod 3$. Consequently

$$Bu = dr - ta + cs \equiv r(a+d) + cs \equiv 0 \pmod 3.$$

But u is not divisible by 3 so $B \equiv 0 \pmod 3$. □

Theorem 3.2.3. *Suppose that the negative discriminant $D = -p$ is not divisible by 3. Then $\gamma_2\left(\sqrt{-p}\right) \in \mathbb{Q}\left(j(\sqrt{-p})\right)$.*

Proof. Let $\theta = \sqrt{-p}$.

Assume first that $p \equiv -1 \pmod 3$. We have $\theta^2 + p = 0$ so $\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\theta = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\theta$. The function γ_2 is invariant under $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \in \mathcal{S}(p,3)$. We cannot have $\theta \equiv e^{2\pi i/3} \pmod{\Gamma(\gamma_2)}$ because θ pertains to a discriminant not divisible by 3 and the discriminant corresponding to $e^{2\pi i/3}$ is -3. Therefore the number $z = \gamma_2(\theta/p) = \gamma_2(\theta)$ is a root of the equation $\Phi_{\gamma_2}(X,X) = 0$, where the matrix is $\left(\begin{smallmatrix} p & \\ & 1 \end{smallmatrix}\right)$.

The three roots of the polynomial

$$S(X) = X^3 - j(\theta)$$

are given by

$$\gamma_2(\theta), \quad e^{-2\pi i/3}\gamma_2(\theta) = \gamma_2(\theta+1), \quad e^{2\pi i/3}\gamma_2(\theta) = \gamma_2(\theta-1).$$

We claim that the numbers $\gamma_2(\theta+1), \gamma_2(\theta-1)$ cannot be roots of the polynomial $\Phi_{\gamma_2}(X,X)$. Since $\theta+1, \theta-1 \equiv \theta \pmod{\Gamma(\gamma_2)}$, the values

$$\gamma_2(\theta+1), \qquad \gamma_2(\theta-1)$$

do not vanish. The quadratic equations for $\theta+1$ and $\theta-1$ are

$$\begin{aligned} (\theta+1)^2 - 2(\theta+1) + p + 1 &= 0, \\ (\theta-1)^2 + 2(\theta-1) + p + 1 &= 0. \end{aligned}$$

By Lemma 3.2.2, the numbers $\gamma_2(\theta+1), \gamma_2(\theta-1)$ cannot be roots of the polynomial $\Phi_{\gamma_2}(X,X)$. Thus the polynomials $S(X)$ and $\Phi_{\gamma_2}(X,X)$ with coefficients in $\mathbb{Q}(j(\theta))$ have only the root $\gamma_2(\theta)$ in common. Therefore, by Euclidean algorithm, $\gamma_2(\theta) \in \mathbb{Q}(j(\theta))$.

On the other hand, when $p \equiv 1 \pmod 3$ we cannot use the transformation polynomial with $n = p$. In this case, however, we may set $n = p+4 \equiv -1 \pmod 3$. Since $\theta^2 + p = 0$ we also have

$$\begin{pmatrix} 1 & p+2 \\ 0 & p+4 \end{pmatrix} \theta = \frac{\theta + p + 2}{p+4} = \frac{\theta + 1}{\theta + 2} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \theta$$

and $\left(\begin{smallmatrix} 1 & p+2 \\ 0 & p+4 \end{smallmatrix}\right) \in \mathcal{S}(p+4, 3)$. We know that the function γ_2 is invariant under the transformation $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right)$. Therefore the number $\gamma_2 \left(\frac{\theta+p+2}{p+4}\right) = \gamma_2(\theta)$ is a root of the polynomial $\Phi_{\gamma_2}(X, X)$. Now we proceed as in the first part of the proof. □

Theorem 3.2.4. *Suppose that the negative discriminant $D = -p$ is not divisible by 3. Set $\tau = \frac{-3+\sqrt{-p}}{2}$. Then $\gamma_2(\tau) \in \mathbb{Q}(j(\tau))$.*

Proof. Set $N = \frac{9+p}{4}$. The quadratic equations for the numbers $\tau, \tau+1, \tau-1$ are

$$\tau^2 + 3\tau + N = 0, \tag{3.9}$$
$$(\tau+1)^2 + (\tau+1) + N = 0, \tag{3.10}$$
$$(\tau-1)^2 + 5(\tau-1) + N + 4 = 0. \tag{3.11}$$

If $N \equiv p \equiv 1 \pmod 3$ then we rewrite (3.9) as

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \tau = \frac{\tau+1}{\tau+2} = \frac{\tau+N-1}{N-2} = \begin{pmatrix} 1 & N-1 \\ 0 & N-2 \end{pmatrix} \tau.$$

Note that $N \geq 4$ and $\left(\begin{smallmatrix} 1 & N-1 \\ 0 & N-2 \end{smallmatrix}\right) \in \mathcal{S}(N-2, 3)$. The function γ_2 is invariant under $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right)$. Therefore by Theorem the number $\gamma_2(\tau) = \gamma_2 \left(\frac{\tau+N-1}{N-2}\right)$ is a root of the transformation equation $\Phi_{\gamma_2}(X, X)$ (with determinant $N-2$), since $N - 2 \equiv -1 \pmod 3$. By Lemma 3.2.2 we can exclude the roots $\tau+1$ and $\tau-1$. Now we complete the argument as in the proof of Theorem 3.2.3.

When $N \equiv p \equiv -1 \pmod 3$ then we write (3.9) as

$$\begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix} \tau = \frac{3\tau+2}{4\tau+3} = \frac{\tau+12N-18}{16N-27} = \begin{pmatrix} 1 & 12N-18 \\ 0 & 16N-27 \end{pmatrix} \tau.$$

In this case we observe that the function γ_2 is invariant under the transformation $\left(\begin{smallmatrix} 3 & 2 \\ 4 & 3 \end{smallmatrix}\right)$, and that $\left(\begin{smallmatrix} 1 & 12N-18 \\ 0 & 16N-27 \end{smallmatrix}\right) \in \mathcal{S}(16N-27, 3)$. Since $16N - 27 \equiv -1 \pmod 3$ we can use the transformation equation with $n = 16N - 27$ as in the first part of the proof. □

Theorem 3.2.5. *Let $D = -p \equiv 1 \pmod 4$ be a negative discriminant. Then*

$$\mathfrak{f}\left(\sqrt{-p}\right)^{24} \in \mathbb{Q}\left(j\left(\sqrt{-p}\right)\right).$$

Proof. Let $\theta = \sqrt{-p}$. Then $\theta^2 + p = 0$ so that

$$\frac{\theta}{p} = -\frac{1}{\theta}, \qquad \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \theta = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \theta.$$

Since $\mathfrak{f}^{24}$ is invariant under $\Gamma(\mathfrak{f}^{24})$, we have $\mathfrak{f}(M\theta)^{24} = \mathfrak{f}(\theta)^{24}$, where $M = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \in \mathcal{S}(p, 16)$. Now we the transformation equation $\Phi_{\mathfrak{f}^{24}}(X, X)$ with determinant $n = p$ to find that $\mathfrak{f}(\theta)^{24}$ is a root of

$$\Phi_{\mathfrak{f}^{24}}(X, X) = 0. \tag{3.12}$$

On the other hand, the roots of the cubic equation

$$(x - 16)^3 - j(\theta)\, x = 0 \tag{3.13}$$

are given by

$$x = \mathfrak{f}(\theta)^{24}, \quad \mathfrak{f}(\theta + 1)^{24}, \quad \mathfrak{f}\left(1 - \frac{1}{\theta}\right)^{24}.$$

The equations (3.12) and (3.13) share the root $\mathfrak{f}(\theta)^{24}$ and we will now demonstrate that this is their only common root, i.e. $\mathfrak{f}(\theta + 1)^{24}, \mathfrak{f}(1 - 1/\theta)^{24}$ are not roots of $\Phi_{\mathfrak{f}^{24}}(X, X) = 0$. For this purpose, we need the following lemma.

Lemma 3.2.6. *Let $\omega \in \mathfrak{H}$ satisfy the quadratic equation $A\omega^2 + B\omega + C = 0$ with integral coefficients. Suppose further that $(A, B, C) = 1$, and that B, C are divisible by 2. Then the number $\mathfrak{f}(\omega)^{24}$ cannot be a root of the equation $\Phi_{\mathfrak{f}^{24}}(X, X) = 0 = 0$, where $p \equiv 3 \pmod 4$ is the determinant.*

Proof. Assume on the contrary, that $\Phi_{\mathfrak{f}^{24}}(\mathfrak{f}(\omega)^{24}, \mathfrak{f}(\omega)^{24}) = 0$. According to the remarks below the definition of the polynomial $\Phi_{\mathfrak{f}^{24}}(X, X)$, we have

$$\mathfrak{f}(\omega)^{24} = \mathfrak{f}\left(\frac{r\omega + s}{t}\right)^{24}$$

with $rt = p$, and s divisible by 16. Since $\mathfrak{f}^{24}$ is injective modulo $\Gamma(\mathfrak{f}^{24})$ we have, for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(\mathfrak{f}^{24})$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\omega = \begin{pmatrix} r & s \\ 0 & t \end{pmatrix}\omega, \qquad \frac{a\omega + b}{c\omega + d} = \frac{r\omega + s}{t}.$$

In this way we get another quadratic equation for ω

$$cr\omega^2 + (cs + dr - at)\omega + ds - bt = 0.$$

If we now compare this equation with $A\omega^2 + B\omega + C = 0$, taking into account that $(A, B, C) = 1$, we receive

$$cr = Au, \tag{3.14}$$

$$cs + dr - at = Bu, \tag{3.15}$$

$$ds - bt = Cu, \tag{3.16}$$

where u is an integer. Since s is divisible by 16, C is even and t is odd, we infer from (3.16) that b is even. By the characterization of the group $\Gamma(\mathfrak{f}^{24})$, the number c must be also even and the numbers d, a must be odd. Because A is odd, we see from (3.14) that $2 \mid u$. Therefore appealing to (3.15), we now have $dr \equiv at \pmod 4$. But the numbers d, r, a, t are all odd, so that this is the same as $rt \equiv ad \pmod 4$. The determinant condition $ad - bc = 1$ implies that $ad \equiv 1 \pmod 4$. Hence $p = rt \equiv ad \equiv 1 \pmod 4$. This is a contradiction. □

The quadratic equations satisfied by the numbers $\theta+1$ and $1-1/\theta$ are

$$(\theta+1)^2-2p(\theta+1)+p+1=0,$$
$$p\left(1-\frac{1}{\theta}\right)^2-2p\left(1-\frac{1}{\theta}\right)+p+1=0.$$

Thus the requirements of Lemma 3.2.6 are fulfilled and therefore $\theta+1$ and $1-1/\theta$ cannot be roots of the equation $\Phi_{\mathfrak{f}^{24}}(X,X)=0$.

Consequently the equations (4.1.5) and (3.13) with coefficients in $\mathbb{Q}(j(\theta))$ have only the root $\mathfrak{f}(\theta)^{24}$ in common. Therefore using the Euclidean algorithm the number $\mathfrak{f}(\theta)^{24}$ may be expressed rationally in terms of $j(\theta)$, i.e. $\mathfrak{f}(\theta)^{24}\in\mathbb{Q}(j(\theta))$, and the theorem is hereby proved. □

Theorem 3.2.7. *Let $D=-p\equiv 5 \pmod 8$ be a negative discriminant. Then*

$$\mathfrak{f}\left(\sqrt{-p}\right)^6\in\mathbb{Q}\left(j\left(\sqrt{-p}\right)\right).$$

Proof. Set $\theta=\sqrt{-p}$. Then $\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\theta=\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)\theta$, where $\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\in\mathcal{S}(p,16)$. Therefore, reasoning as in the proof of the previous theorem, $\mathfrak{f}\left(\frac{\theta}{p}\right)^3=\mathfrak{f}(\theta)^3$ and $\Phi_{\mathfrak{f}^{24}}(\mathfrak{f}(\theta)^3,\mathfrak{f}(\theta)^3)=0$, determinant being p. Recall that $\mathfrak{f}(\theta+2)=e^{-\frac{\pi i}{12}}\mathfrak{f}(\theta)$. This means that the roots of the polynomial

$$S(X)=X^8-\mathfrak{f}(\theta)^{24}$$

are given by $x=\mathfrak{f}(\theta+2k)^3=e^{-\frac{\pi ik}{4}}\mathfrak{f}(\theta)^3$, for $k=0,\dots,7$. Next we investigate the common roots of the polynomials $S(x)$ and $\Phi_{\mathfrak{p}^{24}}(x,x)$. In other words, the question is, for which $0\le k\le 7$ it is true that

$$\Phi_{\mathfrak{f}^{24}}(\mathfrak{f}(\theta+2k)^3,\mathfrak{f}(\theta+2k)^3)=0. \tag{3.17}$$

Suppose that for some $0\le k\le 7$ the equation (3.17) is true. Let $\theta_k=\theta+2k$. Then by definition of the transformation equation we have

$$\mathfrak{f}(\theta_k)^3=\mathfrak{f}\left(\frac{r\theta_k+s}{t}\right)^3$$

with $\left(\begin{smallmatrix}r&s\\o&t\end{smallmatrix}\right)\in\mathcal{S}(p,16)$ so that $rt=p$ and $16\mid s$. By injectivity we obtain

$$\frac{a\theta_k+b}{c\theta_k+d}=\frac{r\theta_k+s}{t}, \tag{3.18}$$

where $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\Gamma(\mathfrak{f}^{24})$ has the following property

$$ac+bd+2d^2-2ad-2cd\equiv 0 \pmod{16}. \tag{3.19}$$

The relation (3.18) can be rewritten as

$$cr\theta_k^2+(cs+dr-at)\theta_k+ds-bt=0. \tag{3.20}$$

On the other hand, since $\theta^2+p=0$, the number $\theta_k=\theta+2k$ also satisfies

$$\theta_k^2-4k\theta_k+p+4k^2=0. \tag{3.21}$$

We claim that k must be divisible by 4. Comparing the coefficients of the equations (3.20) and (3.21) we get

$$cr = u, \tag{3.22}$$

$$cs + dr - at = 4ku, \tag{3.23}$$

$$ds - bt = (p + 4k^2)u. \tag{3.24}$$

where u is an integer. By the characterization of $\Gamma(\mathfrak{f}^{24})$ we have

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \text{ or } \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \pmod 2.$$

Suppose that the numbers a, d are both odd. Then, since s is divisible by 16, from (3.23) we have $dr \equiv at \pmod 4$. Because $rt = p \equiv 3 \pmod 4$ and, in this case, $ad \equiv 1 \pmod 4$, this leads to a contradiction. Therefore $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \pmod 2$. The determinant condition $ad - bc = 1$ implies $b \equiv -c \pmod 4$. Now we use (3.19) to deduce

$$\begin{aligned} ac + bd - 2cd &\equiv 0 \pmod 8, \\ c\frac{a}{2} + b\frac{d}{2} - cd &\equiv 0 \pmod 4, \\ c\frac{a}{2} - c\frac{d}{2} - cd &\equiv 0 \pmod 4, \\ a - d - 2d &\equiv 0 \pmod 8. \end{aligned}$$

Hence $a + d \equiv 0 \pmod 8$. Next $p = rt \equiv 3 \pmod 8$ whence $t \equiv 3r \pmod 8$. Consequently

$$dr - at \equiv dr - 3ar = r(a + d - 4a) \equiv 0 \pmod 8.$$

Now s is divisible by 16 and u is odd, therefore we infer from (3.23) that k is even. Combining (3.22) and (3.24) we obtain $-bt \equiv pcr \pmod 8$ or $-bc \equiv 1 \pmod 8$. Thus $b \equiv -c \pmod 8$ and $ad \equiv 0 \pmod 8$. But we also have $ac + bd \equiv 0 \pmod 4$ and $b \equiv -c \pmod 4$ so that $a \equiv d \equiv 0 \pmod 4$. By (3.19) we have

$$\begin{aligned} c\frac{a}{2} + b\frac{d}{2} - dc &\equiv 0 \pmod 8, \\ bc\frac{a}{2} + b^2\frac{d}{2} - dbc &\equiv 0 \pmod 8, \\ -\frac{a}{2} + \frac{d}{2} + d &\equiv 0 \pmod 8. \\ 3d - a &\equiv 0 \pmod{16}. \end{aligned}$$

Write $t = 3r + 8\ell$, where ℓ is an integer. Then

$$dr - at = r(d - 3a) - 8\ell a \equiv 0 \pmod{16}.$$

Subsequently, since u is odd, k is divisible by 4 and the claim is thereby proved.

This means that the number $\mathfrak{f}(\theta_k)^3 = \mathfrak{f}(\theta + 2k)^3$ can be a root of the equation $\Phi_{\mathfrak{f}^{24}}(x, x) = 0$ only for $k = 0, 4$. We know that $\mathfrak{f}(\theta)^3$ is a common root of the polynomials $S(X)$ and $\Phi_{\mathfrak{f}^{24}}(X, X)$ with coefficients in $\mathbb{Q}\left(\mathfrak{f}(\theta)^{24}\right)$. If this is their only common root, then $\mathfrak{f}(\theta)^3 \in \mathbb{Q}\left(\mathfrak{f}(\theta)^{24}\right) \subseteq \mathbb{Q}(j(\theta))$ and we are done. If not, then the common roots of $S(x)$ and $\Phi_{\mathfrak{f}^{24}}(X, X)$ are precisely the numbers $\mathfrak{f}(\theta)^3$ and $\mathfrak{f}(\theta + 8)^3 = -\mathfrak{f}(\theta)^3$. In consequence their greatest common divisor is $X^2 - \mathfrak{f}(\theta)^6$ so that $\mathfrak{f}(\theta)^6 \in \mathbb{Q}\left(\mathfrak{f}(\theta)^{24}\right) \subseteq \mathbb{Q}(j(\theta))$. □

Theorem 3.2.8. *Let $D = -p \equiv 5 \pmod 8$ be a negative discriminant not divisible by 3. Then $\mathfrak{f}\left(\sqrt{-p}\right)^2 \in \mathbb{Q}\left(j\left(\sqrt{-p}\right)\right)$.*

Proof. Let $\theta = \sqrt{-p}$. The premises of Theorems 3.2.3, 3.2.5, and 3.2.7 are fulfilled. Therefore the numbers

$$\gamma_2\left(\theta\right), \mathfrak{f}\left(\theta\right)^{24}, \mathfrak{f}\left(\theta\right)^6$$

lie in the field $\mathbb{Q}\left(j\left(\theta\right)\right)$. But $\gamma_2\left(\theta\right)$ does not vanish, and we have

$$\mathfrak{f}\left(\theta\right)^8 = \frac{\mathfrak{f}\left(\theta\right)^{24} - 16}{\gamma_2\left(\theta\right)}.$$

Therefore $\mathfrak{f}\left(\theta\right)^8 \in \mathbb{Q}\left(j\left(\theta\right)\right)$. Consequently $\mathfrak{f}\left(\theta\right)^2 = \mathfrak{f}\left(\theta\right)^8 / \mathfrak{f}\left(\theta\right)^6 \in \mathbb{Q}\left(j\left(\theta\right)\right)$. □

3.3 A sufficient criterion for class invariants

Let $\wp_\tau$ be the Weierstrass elliptic function corresponding to the lattice $\Lambda_\tau = [\tau, 1]$. Consider the elliptic curve

$$E_\tau \colon y^2 = 4x^3 - \frac{27j(\tau)}{j(\tau) - 12^3}x - \frac{27j(\tau)}{j(\tau) - 12^3}. \tag{3.25}$$

We have the following analytic isomorphism

$$\Phi_\tau \colon \mathbb{C}/\Lambda_\tau \longrightarrow E_\tau \colon z + \Lambda_\tau \longmapsto \begin{cases} (0,1,0), & \text{if } z \in \Lambda_\tau, \\ (\wp(z), \wp'(z), 1), & \text{otherwise.} \end{cases}$$

Consequently

$$E_\tau[N] \cong \frac{\frac{1}{N}\Lambda_\tau}{\Lambda_\tau} \cong \frac{\mathbb{Z}}{N\mathbb{Z}} \times \frac{\mathbb{Z}}{N\mathbb{Z}},$$

and

$$\begin{aligned} \mathrm{End}(E_\tau[N]) &\cong \mathrm{M}_2\left(\mathbb{Z}/N\mathbb{Z}\right), \\ \mathrm{Aut}(E_\tau[N]) &\cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}). \end{aligned}$$

The choice of basis

$$\begin{aligned} P_1 &= \Phi_\tau(\tau/N + \Lambda_\tau), \\ P_2 &= \Phi_\tau(1/N + \Lambda_\tau), \end{aligned} \tag{3.26}$$

for $E_\tau[N]$, gives us a representation

$$\rho_{N,\tau} \colon \mathrm{End}(E_\tau[N]) \longrightarrow \mathrm{M}_2\left(\mathbb{Z}/N\mathbb{Z}\right),$$

determined by the relation

$$\rho_{N,\tau}(\varphi)\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} P_1^\varphi \\ P_2^\varphi \end{pmatrix}.$$

We let

$$s_N = \frac{\{\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}\} \setminus \{(0,0)\}}{\pm 1}.$$

We have

$$x(rP_1 + sP_2) = \frac{g_2(\tau)}{g_3(\tau)} \wp_\tau \left(\frac{r\tau + s}{N} \right)$$

for $(r, s) \in s_N$. Conversely, the x-coordinate of every point in $E_\tau[N]$ arises in this way because the function $\wp_\tau$ is even.

Proposition 3.3.1. *Let R be an integral domain integrally closed in its field of fractions K. Let L be a Galois extension of K with group G. Let S be the integral closure of R in L. Let $\mathfrak{m}$ be a maximal ideal in R and $\mathfrak{M}$ a maximal ideal of S lying above m. Let*

$$D_{\mathfrak{M}} = \{\sigma \in G \colon \sigma\mathfrak{M} = \mathfrak{M}\}$$

be the decomposition group of $\mathfrak{M}$. Let $\overline{R} = R/\mathfrak{m}$ and $\overline{S} = S/\mathfrak{M}$. Suppose that the extension $\overline{S}/\overline{R}$ is separable. Then the extension $\overline{S}/\overline{R}$ is Galois, and there is a surjective homomorphism

$$G \longrightarrow \mathrm{Gal}(\overline{S}/\overline{R}) \colon \sigma \longmapsto \overline{\sigma}.$$

Here is

$$\overline{\sigma} \colon \overline{S} \longrightarrow \overline{S} \colon s + \mathfrak{M} \longmapsto s^\sigma + \mathfrak{M}.$$

Proof. See [Lan87, 8, §3, Proposition 4, p. 103]. □

Let k be a subfield of $\mathbb{C}$. Then the extension $k \cdot F_N/k(j)$ is Galois, and, denoting its group by G_N, we see that G_N is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$. Now let

$$\mathfrak{o}_\tau = \{f \in k(j) : f \text{ analytic at } \tau\},$$
$$\mathfrak{O}_\tau = \{f \in k \cdot F_N : f \text{ analytic at } \tau\}.$$

Let τ be a CM point and $S_\tau = \cap_\gamma \mathfrak{O}_{\gamma\tau}$.

Lemma 3.3.2. *(1) The integral closure of $\mathfrak{o}_\tau$ in $k \cdot F_N$ is equal to S_τ.*
(2) Let $\mathfrak{M}_{\gamma\tau} = \{f \in S_\tau : f(\gamma\tau) = 0\}$, where $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Then $\mathfrak{M}_{\gamma\tau}$ is a maximal ideal in S_τ.

Proof. Let $f \in S_\tau$. Then $f^n + a_{n-1}f^{n-1} + \ldots + a_0 = 0$ for some $a_i \in \mathfrak{o}_\tau$. Hence

$$(f \circ \gamma)^n = -a_{n-1}(f \circ \gamma)^{n-1} - \ldots - a_0$$

for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Consequently the functions $f \circ \gamma$ cannot have a pole at τ because all coefficients a_i are analytic at τ. Thus $S_\tau \subset \cap_\gamma \mathfrak{O}_{\gamma\tau}$. Conversely, let $f \in \cap_\gamma \mathfrak{O}_{\gamma\tau}$. Then the functions $f \circ \gamma$ are all analytic at τ, hence they lie in $\mathfrak{o}_\tau$. This means that the coefficients of the minimal polynomial of f over $k(j)$, which is given by $\prod_\gamma (X - f \circ \gamma)$, actually lie in $\mathfrak{o}_\tau$. This proves (1).

We will prove that the ideal $\mathfrak{M}_{\gamma\tau}$ is maximal. Let $g \in S_\tau \setminus \mathfrak{M}_{\gamma\tau}$. Let $v_1, \ldots, v_t$ be the nonzero values of g attained at the points $\alpha\tau$, where α runs through $\mathrm{SL}_2(\mathbb{Z})$. Note that there is at least one such value because $g(\gamma\tau) \neq 0$. Let L be a Galois extension of $k \cdot \mathbb{Q}(\zeta_N)$ containing the values v_i. Let

$$G = \prod_{i=1}^{t} \prod_\sigma (g - v_i^\sigma),$$

where σ runs through all automorphisms in $\mathrm{Gal}(L/k\cdot\mathbb{Q}(\zeta_N))$. Then $G\in\mathfrak{M}_{\gamma\tau}$ and for every $\alpha\in\mathrm{SL}_2(\mathbb{Z})$ we have

$$(G+g)(\alpha\tau)=\begin{cases}v_j, & \text{if } g(\alpha\tau)=v_j,\\ \pm\prod_{i=1}^{t}\prod_{\sigma}v_i^{\sigma}, & \text{if } g(\alpha\tau)=0.\end{cases}$$

In particular $(G+g)(\alpha\tau)\neq 0$ for all $\alpha\in\mathrm{SL}_2(\mathbb{Z})$. Therefore the function $G+g$ is invertible in S_τ. Consequently $\mathfrak{M}_{\gamma\tau}+S_\tau g=S_\tau$ and so the ideal $\mathfrak{M}_{\gamma\tau}$ is maximal. □

We are now in a position to apply Proposition 3.3.1 with maximal ideals

$$\begin{aligned}\mathfrak{M}_\tau&=\{f\in S_\tau : f(\tau)=0\},\\ \mathfrak{m}_\tau&=\{f\in\mathfrak{o}_\tau : f(\tau)=0\},\end{aligned}$$

and corresponding residue fields

$$\begin{aligned}S_\tau/\mathfrak{M}_\tau&\cong k(f(\tau):f\in S_\tau),\\ \mathfrak{o}_\tau/\mathfrak{m}_\tau&\cong k(j(\tau)).\end{aligned}$$

Finally, let

$$\begin{aligned}R_{N,\tau}&=k(f(\tau):f\in S_\tau),\\ G_{N,\tau}&=\mathrm{Gal}(R_N(\tau)/k(j(\tau))),\end{aligned}$$

and

$$\begin{aligned}F_N(\tau)&=k(j(\tau),f_N^{(r,s)}(\tau):(r,s)\in s_N),\\ D_{N,\mathfrak{M}_\tau}&=\{\sigma\in G_N:\sigma\mathfrak{M}_\tau=\mathfrak{M}_\tau\}.\end{aligned}$$

The following commutative diagram illustrates our situation.

$$\begin{array}{ccccccc}
R_{N,\tau} & \longleftarrow & S_\tau/\mathfrak{M}_\tau & \longleftarrow & S_\tau & \longrightarrow & k\cdot F_N\\
\uparrow & & & & \uparrow & & \uparrow\\
F_{N,\tau} & & & & & & \\
\uparrow & & & & & & \\
k(j(\tau)) & \longleftarrow & \mathfrak{o}_\tau/\mathfrak{m}_\tau & \longleftarrow & \mathfrak{o}_\tau & \longrightarrow & k(j)
\end{array}$$

Proposition 3.3.1 provides a surjective homomorphism

$$D_{N,\mathfrak{M}_\tau}\longrightarrow G_{N,\tau}\colon\sigma\longmapsto\overline{\sigma}.$$

We will now show that actually $R_{N,\tau}=F_{N,\tau}$. We need two simple lemmas.

Lemma 3.3.3. *Let $\alpha\in\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be such that $u\alpha=\varepsilon_u u$ for every $u\in s_N$, where $\varepsilon_u=\pm1$. Then $\alpha=\pm1$.*

Lemma 3.3.4. *Let $\tau\in\mathfrak{H}_1$, and let $\alpha\in\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be such that $f_N^{u\alpha}(\tau)=f_N^u(\tau)$ for all $u\in s_N$. Then $\alpha=\pm1$.*

Proposition 3.3.5. *Let $\tau \in \mathfrak{H}_1$. Then $R_{N,\tau} = F_{N,\tau}$.*

Proof. Let $H = \mathrm{Gal}(R_{N,\tau}/F_{N,\tau})$. Take $\overline{\sigma} \in H$. Then $(f_N^u(\tau))^{\overline{\sigma}} = f_N^u(\tau)$ for all $u \in S_N$. Let σ be the inverse image of $\overline{\sigma}$ in $D_{N,\mathfrak{M}_\tau}$, and let α_σ be the matrix representing the automorphism σ of $k \cdot F_N$ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. We have $(f_N^u(\tau))^{\overline{\sigma}} = (f_N^u)^\sigma(\tau) = f_N^{u\alpha_\sigma}(\tau)$ for all $u \in s_N$. It follows therefore that $f_N^u(\tau) = f_N^{u\alpha_\sigma}(\tau)$ for all $u \in S_N$. Thus, according to Lemma 3.3.3, we have $\alpha_\sigma = \pm 1$. Consequently, σ is the identity automorphism, and so is $\overline{\sigma}$. Therefore H is trivial, and so $R_{N,\tau} = F_{N,\tau}$. □

The next proposition shows that the representations ρ_N and $\rho_{N,\tau}$ are compatible.

Proposition 3.3.6. *The diagram*

$$\begin{array}{ccc} D_{N,\mathfrak{M}_\tau} & \xrightarrow{\rho_N} & \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\} \\ \downarrow & & \uparrow \\ G_{N,\tau} & \xrightarrow{\rho_{N,\tau}} & \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \end{array}$$

is commutative.

Proof. Let $\sigma \in D_{N,\mathfrak{M}_\tau}$. We see that

$$\begin{aligned} (f_N^{(r,s)}(\tau))^{\overline{\sigma}} &= x\left((r,s)\begin{pmatrix} P_1 \\ P_2 \end{pmatrix}\right)^{\overline{\sigma}} \\ &= x\left((r,s)\begin{pmatrix} P_1^{\overline{\sigma}} \\ P_2^{\overline{\sigma}} \end{pmatrix}\right) \\ &= x\left((r,s)\rho_{N,\tau}(\overline{\sigma})\begin{pmatrix} P_1 \\ P_2 \end{pmatrix}\right) \\ &= f_N^{(r,s)\rho_{N,\tau}(\overline{\sigma})}(\tau). \end{aligned}$$

On the other hand we have

$$(f_N^{(r,s)}(\tau))^{\overline{\sigma}} = (f_N^{(r,s)})^\sigma(\tau) = f_N^{(r,s)\rho_N(\sigma)}(\tau).$$

Therefore $f_N^{(r,s)\rho_{N,\tau}(\overline{\sigma})}(\tau) = f_N^{(r,s)\rho_N(\sigma)}(\tau)$ for all $(r,s) \in s_N$. Lemma 3.3.3 now implies that $\rho_{N,\tau}(\overline{\sigma}) = \pm\rho_N(\sigma)$ which completes the proof. □

Let us return to the elliptic curve E_τ defined in (3.25). Choose $\tau \in \mathfrak{H}_1$ such that $K = \mathbb{Q}(\tau)$ is an imaginary quadratic field, and let $\mathcal{O}$ be the order in K corresponding to the lattice $\Lambda_\tau = [\tau, 1]$. We know that the E_τ has complex multiplication by $\mathcal{O}$ meaning that $\mathrm{End}(E_\tau) \cong \mathcal{O}$. For $\lambda \in \mathcal{O}$ denote the corresponding multiplication map on $\mathbb{C}/\Lambda_\tau$ by $[\lambda]$, so that $[\lambda](z + \Lambda) = \lambda z + \Lambda$. For every such λ there is a unique endomorphism of E_τ with the property that the diagram

$$\begin{array}{ccc} \mathbb{C}/\Lambda_\tau & \xrightarrow{[\lambda]} & \mathbb{C}/\Lambda_\tau \\ \downarrow{\scriptstyle \Phi_\tau} & & \downarrow{\scriptstyle \Phi_\tau} \\ E_\tau & \xrightarrow{[\lambda]_E} & E_\tau \end{array}$$

is commutative. According to Proposition 1.3.2, we have $\wp(\lambda z) = R(\wp(z))$, where R is a rational function depending on λ and with coefficients in $K(j(\tau))$. Differentiating we get $\wp'(\lambda z) = \lambda^{-1}\wp'(z)R'(\wp(z))$. Therefore

$$\Phi \circ [\lambda](z+\lambda) = (R(\wp(z)), \lambda^{-1}\wp'(z)R'(\wp(z)), 1),$$

and

$$[\lambda]_E(x,y) = (R(x), \lambda^{-1}yR'(x), 1).$$

Now we have the commutative diagram

$$\begin{array}{ccc} \mathcal{O} & \longrightarrow & \mathrm{End}(E_\tau) \\ \downarrow & & \downarrow \\ \mathcal{O}/N\mathcal{O} & \longrightarrow & \mathrm{End}(E_\tau[N]) \end{array}$$

Consequently we get a homomorphism $(\mathcal{O}/N\mathcal{O})^\times \longrightarrow \mathrm{Aut}(E_\tau[N])$. This homomorphism is easily seen to be injective. The choice of basis in (3.26) gives us therefore an embedding of $(\mathcal{O}/N\mathcal{O})^\times$ into $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Let us denote by $W_{N,\tau}$ its image.

We will now assume that the point $\tau \in \mathfrak{H}_1$ satisfy the following properties: $\mathbb{Q}(\tau) = K$, the order of Λ_τ is $\mathcal{O}$, and $A\tau^2 + B\tau + C = 0$ with $A, B, C \in \mathbb{Z}$ relatively prime.

Proposition 3.3.7. *We have*

$$W_{N,\tau} = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \cap \left\{ s\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + t\begin{pmatrix} 0 & -C \\ A & B \end{pmatrix} : s,t \in \mathbb{Z}/N\mathbb{Z} \right\}.$$

Proof. Let $\lambda \in \mathcal{O}$ be such that $\lambda + N\mathcal{O}$ is invertible. Write

$$\lambda\begin{pmatrix} \tau \\ 1 \end{pmatrix} = M_\lambda \begin{pmatrix} \tau \\ 1 \end{pmatrix}, \tag{3.27}$$

where $M_\lambda \in \mathrm{M}_2(\mathbb{Z})$. Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be the image of M_λ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Then

$$\frac{\lambda\tau}{N} + \Lambda = \frac{a\tau + b}{N} + \Lambda, \qquad \frac{\lambda}{N} + \Lambda = \frac{c\tau + d}{N} + \Lambda.$$

Next

$$\begin{aligned} [\lambda]_{E_\tau}(P_1) &= \Phi \circ [\lambda] \circ \Phi^{-1}(P_1) \\ &= \Phi_\tau \circ [\lambda]\left(\frac{\tau}{N} + \Lambda\right) \\ &= \Phi_\tau\left(\frac{a\tau + b}{N} + \Lambda\right) \\ &= aP_1 + bP_2. \end{aligned}$$

Similarly, $[\lambda]_{E_\tau}(P_2) = cP_1 + dP_2$. Therefore $\rho_{N,\tau}([\lambda]_{E_\tau}) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Now from (3.27) we compute that $M_\lambda \tau = \tau$. Thus $c\tau^2 + (d-a)\tau - b = 0$. Comparing this with $A\tau^2 + B\tau + C = 0$ we obtain the desired form for our matrix. □

Let $C_{N,\tau}$ be the centralizer of $W_{N,\tau}$ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, that is,

$$C_{N,\tau} = \{\alpha \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})\colon \alpha M = M\alpha \text{ for all } M \in W_{N,\tau}\}.$$

Proposition 3.3.8. *We have $\rho_{N,\tau}(G_{N,\tau}) \subset C_{N,\tau}$.*

Proof. Let $\overline{\sigma} \in G_{N,\tau}$. We have

$$\begin{aligned}\overline{\sigma} \circ [\lambda]_{E_\tau}(x,y) &= \overline{\sigma}(R(x), \lambda^{-1}yR'(x)) = (R(x^{\overline{\sigma}}), \lambda^{-1}y^{\overline{\sigma}}R'(x^{\overline{\sigma}}))\\ [\lambda]_{E_\tau} \circ \overline{\sigma}(x,y) &= [\lambda]_{E_\tau}(x^{\overline{\sigma}}, y^{\overline{\sigma}}) = (R(x^{\overline{\sigma}}), \lambda^{-1}y^{\overline{\sigma}}R'(x^{\overline{\sigma}}))\end{aligned}$$

Therefore $\overline{\sigma} \circ [\lambda]_{E_\tau} = [\lambda]_{E_\tau} \circ \overline{\sigma}$ and so

$$\rho_{N,\tau}(\overline{\sigma})\rho_{N,\tau}([\lambda]_{E_\tau}) = \rho_{N,\tau}([\lambda]_{E_\tau})\rho_{N,\tau}(\overline{\sigma}).$$

Hence $\rho_{N,\tau}(\overline{\sigma})$ lies in $C_{N,\tau}$. □

Proposition 3.3.9. *We have $C_{N,\tau} = W_{N,\tau}$.*

Proof. We will prove the proposition under the assumption that $(A, N) = 1$. Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in C_{N,\tau}$. Then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & -C \\ A & B \end{pmatrix} = \begin{pmatrix} 0 & -C \\ A & B \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Consequently, $bA = -cC$ and $aA + cB = dA$. Since A is invertible modulo N,

$$b = -C\frac{c}{A}, \qquad d = a + B\frac{c}{A}, \qquad c = A\frac{c}{A}.$$

Hence $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = a\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) + \frac{c}{A}\left(\begin{smallmatrix} 0 & -C \\ A & B \end{smallmatrix}\right)$. □

Theorem 3.3.10. *Suppose that $f \in F_N$ is analytic at a CM point $\tau \in \mathfrak{H}_1$. Let $K = \mathbb{Q}(\tau)$ be the corresponding imaginary quadratic field. Then $f(\tau) \in K(j(\tau))$ provided that the group $W_{N,\tau}$ acts trivially on f.*

Proof. Let $\overline{\sigma} \in G_{N,\tau}$. Let σ be the inverse image of $\overline{\sigma}$ in G_N. By Proposition 3.3.6 we have $\rho_{N,\tau}(\overline{\sigma}) = \pm\rho_N(\sigma)$. On the other hand, Proposition 3.3.8 and Proposition 3.3.9 imply that $\rho_{N,\tau}(\overline{\sigma}) \in W_{N,\tau}$. Suppose that $W_{N,\tau}$ acts trivially on f. We see that

$$f(\tau)^{\overline{\sigma}} = f^{\sigma}(\tau) = f^{\rho_N(\sigma)}(\tau) = f^{\rho_{N,\tau}(\overline{\sigma})}(\tau) = f(\tau).$$

Thus $f(\tau) \in K(j(\tau))$ as asserted. □

This criterion can be used to prove Weber's results on class invariants. See [Gee99, 6.,8.] for details.

3.4 Heegner's proof

Proposition 3.4.1. *Let p be a positive integer and let*

$$\tau_p = \frac{-1 + \sqrt{-p}}{2}, \qquad \theta_p = \sqrt{-p}.$$

Suppose that the class number of $\mathcal{O}_{\tau_p}$ is equal to 1. Then the number $j(\theta_p)$ is algebraic of degree 3.

Proof. Note that $j(\theta_p) = j(2\tau_p)$. Consider the modular polynomial $\Phi_2^j(X,Y) \in \mathbb{Z}[X,Y]$. We have

$$\Phi_2(X, j(\tau_p)) = (X - j(\theta_p)) \left(X - j\left(\frac{-1+\sqrt{-p}}{4}\right)\right)\left(X - j\left(\frac{1+\sqrt{-p}}{4}\right)\right).$$

Because the class number of $\mathcal{O}_{\tau_p}$ is 1, the number $j(\tau_p)$ is a rational integer. Since $\Phi_2(j(\theta_p), j(\tau_p)) = 0$, we see that $j(\theta_p)$ is a root of a cubic polynomial with integer coefficients. Therefore to prove that $j(\theta_p)$ is of degree 3, we must prove that $j(\theta_p)$ is neither rational or quadratic.

If $j(\theta_p)$ were quadratic, then one of the remaining roots of $\Phi_2(X, j(\tau_p))$ would be rational. However, for $p > 16$ the arguments $(\pm 1 + \sqrt{-p})/4$ lie inside the fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$, and so the corresponding values of the j-invariant are not even real (the j-invariant is a bijection mapping the imaginary axis and the boundary of the fundamental domain onto the real axis; this is easy to see directly from the Fourier expansion of j, see [Apo, 2.7, p. 40]).

If $j(\theta_p)$ were rational, then by Theorem 3.1.4 it would actually be a rational integer. Let $t = e^{2\pi i \tau_p}$ so that $t^2 = e^{2\pi i \theta_p}$. Then

$$\begin{aligned} j(\tau_p) &= \frac{1}{t} + 744 + 196884t + 21493760t^2 + O(t^2), \\ j(\theta_p) &= \frac{1}{t^2} + 744 + 196884t^2 + O(t^4). \end{aligned}$$

Eliminating polar and constant terms we obtain

$$j(\tau_p)^2 - 1488 j(\tau_p) + 160512 - j(\theta_p) = 42987520t + O(t^2). \tag{3.28}$$

The left hand side of (3.28) is supposedly a rational integer. However, for p sufficiently large, the right hand side of (3.28) is strictly between 0 and 1.

According to Stark, $p > 60$ is large enough. If we wanted to verify this, we would need some explicit bound on the coefficients of the j-invariant. Write $j = \sum_{n \geq -1} c_n q^n$. Then it is easy to show that $c_n < e^{4\pi\sqrt{n}}$ for $n \geq 1$ (see [hde]). This provides a bound of a required type. □

Theorem 3.4.2 (Heegner)**.** *Let K be an imaginary quadratic field such that*

$$h(\mathcal{O}_K) = 1, \quad D_K \equiv 5 \pmod 8, \quad D_K \not\equiv 0 \pmod 3.$$

Then

$$D_K \in \{-11, -19, -43, -67, -163\}.$$

Proof. Write $p = -D_K$, so that $p \equiv 3 \pmod 8$, and let

$$\theta_p = \sqrt{-p}, \quad \tau_p = \frac{-3+\sqrt{-p}}{2}, \quad \alpha_p = \zeta_8 \mathfrak{f}_2(\tau_p)^2.$$

We claim that

$$\alpha_p = \frac{1}{\mathfrak{f}(\theta_p)^2}. \tag{3.29}$$

To see this recall that

$$\begin{aligned} \mathfrak{f}_1(\tau+1) &= \zeta_{48}^{-1} \mathfrak{f}(\tau), \\ \mathfrak{f}(\tau+1) &= \zeta_{48}^{-1} \mathfrak{f}_1(\tau), \\ \mathfrak{f}_1(2\tau)\mathfrak{f}_2(\tau) &= \sqrt{2}, \end{aligned}$$

for every $\tau \in \mathfrak{H}$. Consequently

$$\begin{aligned} \mathfrak{f}_1(-3+\theta_p)\mathfrak{f}_2(\tau_p) &= \sqrt{2}, \\ \zeta_{48}^3\mathfrak{f}(\theta_p)\mathfrak{f}_2(\tau_p) &= \sqrt{2}, \\ \zeta_8\mathfrak{f}(\theta_p)^2\mathfrak{f}_2(\tau_p)^2 &= 2, \\ \alpha_p\mathfrak{f}(\theta_p)^2 &= 2, \end{aligned}$$

thus proving (3.29). Let

$$K_p = \mathbb{Q}(j(\theta_p)).$$

By Proposition 3.4.1 the extension $K_p/\mathbb{Q}$ is of degree 3. Weber's theorem on the function $\mathfrak{f}$ now implies that $K_p = \mathbb{Q}(\mathfrak{f}(\theta_p)^2)$. Therefore by (3.29) $K_p = \mathbb{Q}(\alpha_p)$. Note that $K_p = \mathbb{Q}(\alpha_p^4)$.

From Proposition 2.5.9 and the fact that the j-invariant is a cube follows that the minimal equation of the number α_p^4 over $\mathbb{Q}$ is

$$x^3 - \gamma_2(\tau_p)x - 16 = 0. \tag{3.30}$$

Let

$$x^3 + ax^2 + bx + c = 0, \quad a, b, c \in \mathbb{Z}, \tag{3.31}$$

be the minimal equation of α_p over $\mathbb{Q}$. Transposing the terms of even degree and squaring, we get

$$\begin{aligned} (x^3+bx)^2 &= (-c-ax^2)^2, \\ x^6 + (2b-a^2)x^4 + (b^2-2ac)x^2 - c^2 &= 0. \end{aligned}$$

Consequently, the number α_p^2 is a solution to the cubic equation

$$x^3 + sx^2 + tx + u = 0,$$

where

$$\begin{aligned} s &= 2b - a^2, \\ t &= b^2 - 2ac, \\ u &= -c^2. \end{aligned} \tag{3.32}$$

Repeating this process, we find that α_p^4 satisfies the cubic equation

$$x^3 + (2t - s^2)x^2 + (t^2 - 2su)x - u^2 = 0. \tag{3.33}$$

But the minimal polynomial for α_p^4 is unique, and from (3.30) we already know it to be

$$x^3 - \gamma_2(\tau_p)x - 16 = 0. \tag{3.34}$$

Comparing the coefficients of (3.33) and (3.34) we obtain

$$\begin{aligned} 0 &= 2t - s^2, \\ -\gamma_2(\tau_p) &= t^2 - 2su, \\ -u^2 &= -16. \end{aligned} \tag{3.35}$$

Since $c^4 = 16$, it follows that $c = \pm 2$. Replacing α_p by $-\alpha_p$ preserves α_p^4, and by (3.31) takes (a, b, c) to $(-a, b, -c)$. Therefore we may assume that $c = 2$. Substituting into (3.35) from (3.32) yields

$$0 = 2(b^2 - 4a) - (2b - a^2)^2, \tag{3.36}$$

$$-\gamma_2(\tau_p) = (b^2 - 4a)^2 + 8(2b - a^2). \tag{3.37}$$

From the first equation of (3.35) we see that s and t are even. Therefore by (3.32) so are a and b. We let

$$X = -\frac{a}{2}, \qquad Y = \frac{b - a^2}{2}.$$

Equation (3.36) can now be rewritten as

$$2X(X^3 + 1) = Y^2. \tag{3.38}$$

This equation can be easily solved in integers (see [Kez, Proposition 6.6., p. 34] and [Cox11, §12.,E, Proposition 12.37., p. 273]). The only solutions are $(X, Y) = (0, 0), (-1, 0), (1, \pm 2)$, and $(2, \pm 6)$.

In the following table we list the corresponding values of a, b, and $\gamma_2(\tau_p)$ (using (3.37)).

X	Y	$a = -2X$	$b = 2Y + 4X^2$	$\gamma_2(\tau_p) = (b^2 - 4a)^2 - 8(2b - a^2)$
0	0	0	0	0
-1	0	2	4	-96
1	2	-2	8	-5280
1	-2	-2	0	-32
2	6	-4	28	-640320
2	-6	-4	4	-960

We have thus proved that $j(\tau_p)$ can attain only 6 distinct values. By virtue of Proposition 2.2.2, (2) the point τ_p is therefore restricted to 6 orbits of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$. Consequently there are only 5 possibilities for K, one being disqualified because we assumed that the discriminant is not divisible by 3. But we already know that the imaginary quadratic fields corresponding to the listed discriminants have class number equal to 1. The proof is complete. For the actual computation of the values of $\gamma_2(\tau_p)$ see [Kez, Theorem 6.5., p. 32] and [Cox11, §12.,D, p. 263]. □

4. Siegel's proof

In this chapter we will give an exposition of Siegel's proof that there are exactly 9 imaginary quadratic fields with class number 1. We follow the article [Sie68]. For an approach using covering relations between Riemann surfaces and moduli spaces of elliptic curves see Imin Chen's article [Che99].

4.1 The Dirichlet-Kronecker formula

Let $\tau = x + iy \in \mathfrak{H}$, so $y > 0$. Define the function

$$E(\tau, s) = \sum_{m,n\in\mathbb{Z}}{}' \frac{y^s}{|m\tau + n|^{2s}}, \qquad \mathrm{Re}(s) > 1,$$

Here the sum is over all $(0,0) \neq (m,n) \in \mathbb{Z}^2$. The function $E(\tau, s)$ has analytic continuation as a function of s to the entire complex plane except for a simple pole at $s = 1$, and it satisfies a functional equation similar to that of the Riemann zeta function. The next theorem determines the residue and the constant term of the Laurent expansion of $E(\tau, s)$ at $s = 1$. Recall that the Dedekind eta function is defined as follows

$$\eta(\tau) = q^{1/24} \prod_{n=1}^{\infty}(1 - q^n), \qquad q = e^{2\pi i\tau}. \tag{4.1}$$

Theorem 4.1.1 (Kronecker first limit formula)**.** *Let $\tau = x + iy \in \mathfrak{H}$ and let γ be the Euler's constant. Then for s near 1 we have*

$$E(\tau, s) = \frac{\pi}{s-1} + 2\pi\left(\gamma - \log 2 - \log(y^{1/2}\,|\eta(\tau)|^2)\right) + O(s-1).$$

Proof. See [Web08, §141., p. 526], [DIT18], [Lan87, 20.], [SR80, 1.], and also [DS05, 4.10.]. □

As the first application of the Kronecker limit formula we will prove the functional equation of the Dedekind η-function.

Theorem 4.1.2. *We have*

$$\eta\left(\frac{a\tau + b}{c\tau + d}\right) = \varepsilon(a,b,c,d)\sqrt{c\tau + d}\,\eta(\tau), \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), \quad c \geq 0,$$

where $\varepsilon(a,b,c,d)$ is a 24-th root of unity, and the square root is positive on the positive real axis.

Proof. We claim that $E(\gamma\tau, s) = E(\tau, s)$ if $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Recall that

$$\mathrm{Im}(\gamma\tau) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2}, \qquad \text{if } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Now we compute

$$\begin{aligned} E(\gamma\tau, s) &= \sum_{m,n\in\mathbb{Z}}{}' \frac{\operatorname{Im}(\gamma\tau)^s}{|m(\gamma\tau)+n|^{2s}} = \sum_{m,n\in\mathbb{Z}}{}' \frac{\operatorname{Im}(\tau)^s\,|c\tau+d|^{-2s}}{\left|m\frac{a\tau+b}{c\tau+d}+n\right|^{2s}} \\ &= \sum_{m,n\in\mathbb{Z}}{}' \frac{\operatorname{Im}(\tau)^s\,|c\tau+d|^{-2s}}{\left|m\frac{a\tau+b}{c\tau+d}+n\right|^{2s}} \\ &= \sum_{m,n\in\mathbb{Z}}{}' \frac{\operatorname{Im}(\tau)^s\,|c\tau+d|^{-2s}}{|(ma+nc)\tau+(mb+nd)|^{2s}\,|c\tau+d|^{-2s}} \end{aligned}$$

The map $(m,n)\longmapsto(m,n)\gamma$ is a bijection of $\mathbb{Z}^2$ preserving $(0,0)$. For $\operatorname{Re}(s)>1$ the sum defining $E(\tau,s)$ converges absolutely (see [DS05, 4.10, p. 148]) and so we can rearrange the terms in the sum as we like. Hence $E(\gamma\tau,s)=E(\tau,s)$. Let

$$h(\tau)=y^{1/2}\,|\eta(\tau)|^2\,,\qquad \tau=x+iy,\quad y>0.$$

Comparing constant coefficients of the Laurent expansions in $E(\gamma\tau,s)=E(\tau,s)$ we get by Theorem 4.1.1 the relation $h(\gamma\tau)=h(\tau)$, or

$$\begin{aligned} |c\tau+d|^{-1}\,y^{1/2}\,|\eta(\gamma\tau)|^2 &= y^{1/2}\,|\eta(\tau)|^2\,, \\ |\eta(\gamma\tau)| &= |c\tau+d|^{1/2}\,|\eta(\tau)|\,. \end{aligned} \tag{4.2}$$

Let

$$f(\tau)=\frac{\eta(\gamma\tau)}{(c\tau+d)^{1/2}\eta(\tau)}.$$

Then f is analytic on $\mathfrak{H}$, and (4.2) implies that $|f(\tau)|=1$ for all $\tau\in\mathfrak{H}$. The maximum modulus principle states that an analytic function cannot attain its local maximum on its domain, unless it is locally constant. Therefore f is constant on $\mathfrak{H}$:

$$f(\tau)=\varepsilon(a,b,c,d),\qquad |\varepsilon(a,b,c,d)|=1.$$

We have proved

$$\eta(\gamma\tau)=\varepsilon(a,b,c,d)\sqrt{c\tau+d}\,\eta(\tau),$$

where $\varepsilon(a,b,c,d)$ is a constant with absolute value equal to 1. To prove that $\varepsilon(a,b,c,d)$ is actually a 24-nth of unity we can restrict ourselves to $T=\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and $-S=\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$, because the modular group is generated by those two matrices. By definition (4.1) we have $\eta(T\tau)=\zeta_{24}\eta(\tau)$, so $\varepsilon(T)=\zeta_{24}$. Next put $\tau=it, t>0$ and $\gamma=S$ in (4.2) to obtain

$$|\eta\,(i/t)|=t^{1/2}\,|\eta(it)|\,.$$

By definition (4.1) the η-function is real and positive on the positive imaginary axis, hence

$$\eta\,(i/t)=t^{1/2}\eta(it),\qquad t>0. \tag{4.3}$$

But the η-function is analytic on $\mathfrak{H}$, so (4.3) is true for all t such that $\operatorname{Im}(i/t)>0$, $\operatorname{Im}(it)>0$, and $\operatorname{Re}(t)>0$. On setting $t=-i\tau$ we get $\varepsilon(S)=1$. Therefore $\varepsilon(a,b,c,d)$ is a 24-root of unity and the proof is complete. This proof is due to Siegel (see [SR80, 1.1, p. 15]). For other proofs see [SR80, 1.1, p. 17], [Apo, 3.], [Cox11, 12.19., p. 236], [Web08, §38., p. 124], [DS05, 1.2.5, p. 20], and [Ser12, VII, Thm. 6]. □

Let K be a imaginary quadratic field, d_K its discriminant. Let f be a positive integer and consider the order $\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K$ in K. With $\mathcal{O}_f$ are associated the following groups:

$$\begin{aligned}
I(\mathcal{O}_f) &= \text{the group generated by proper ideals of } \mathcal{O}_f,\\
P(\mathcal{O}_f) &= \text{the group generated by principal ideals of } \mathcal{O}_f,\\
I(\mathcal{O}_f, f) &= \text{the group generated by ideals of } \mathcal{O}_f \text{ prime to } f,\\
P(\mathcal{O}_f, f) &= \text{the group generated by principal ideals of } \mathcal{O}_f \text{ prime to } f,\\
I_K(f) &= \text{the group generated by ideals of } \mathcal{O}_K \text{ prime to } f,\\
P_K(f) &= \text{the group generated by principal ideals of } \mathcal{O}_K \text{ prime to } f,\\
P_{K,\mathbb{Z}}(f) &= \text{the group generated by principal ideals of the form } \alpha\mathcal{O}_K,\\
&\quad \text{where } \alpha \in \mathcal{O}_K \text{ satisfies } \alpha \equiv t \pmod{f\mathcal{O}_K} \text{ for some } t \in \mathbb{Z} \text{ prime to } f,\\
\mathrm{Cl}_f &= I(\mathcal{O}_f)/P(\mathcal{O}_f) \text{ the class group of } \mathcal{O}_f.
\end{aligned}$$

We have the isomorphisms

$$\mathrm{Cl}_f \cong \frac{I(\mathcal{O}_f, f)}{P(\mathcal{O}_f, f)} \cong \frac{I_K(f)}{P_{K,\mathbb{Z}}(f)}.$$

The first isomorphism is induced by the inclusion $I(\mathcal{O}_f) \hookleftarrow I(\mathcal{O}_f, f)$, the second is induced by the isomorphism $I(\mathcal{O}_f, f) \cong I_K(f)\colon \mathfrak{a}_f \longmapsto \mathfrak{a}_f\mathcal{O}_K$. Let f' be a divisor of f. Since $P_{K,\mathbb{Z}}(f) \subseteq P_{K,\mathbb{Z}}(f')$, the inclusion $I_K(f) \hookrightarrow I_K(f')$ induces a surjective homomorphism

$$\frac{I_K(f)}{P_{K,\mathbb{Z}}(f)} \longrightarrow \frac{I_K(f')}{P_{K,\mathbb{Z}}(f')}.$$

This gives us a surjective homomorphism

$$\psi_{f,f'}\colon \mathrm{Cl}_f \longrightarrow \mathrm{Cl}_{f'}\,.$$

For proofs of these statements, see [Cox11, §7.,C. ,D.].

When $\tau \in \mathfrak{H}$ is CM point we can relate the Eisenstein series to the partial zeta function corresponding to the ideal class of the fractional ideal $[\tau, 1]$ in $\mathrm{Cl}_f \cong I_K(f)/P_{K,\mathbb{Z}}(f)$. The partial zeta-function is defined as

$$\zeta_f(s, C) = \sum_{\substack{\mathfrak{a} \in I_K(f)\\ [\mathfrak{a}]=C,\, \mathfrak{a} \subseteq \mathcal{O}_K}} \frac{1}{N(\mathfrak{a})^s}.$$

This defines an analytic function in some half-plane. We shall not deal here with convergence issues.

Proposition 4.1.3. *Let $\mathcal{O}_f$ be the order of K with conductor f, $\tau_C \in \mathfrak{H}$ be a CM point representing the ideal class C of Cl_f, and w_f the number of units in $\mathcal{O}_f$. We have*

$$E(\tau_C, s) = \frac{f^s\,|d_K|^{s/2}}{2^s} \sum_{f'|f} w_{f'}(f'/f)^{2s}\zeta_{f'}(s, \psi_{f,f'}(C^{-1})).$$

Proof. Let $\mathfrak{c}_f = [\alpha, \beta]$ be a proper ideal of $\mathcal{O}_f = \mathcal{O}_\tau$ which is prime to f, where f is the conductor of τ_C, such that $\alpha/\beta = \tau_C$ and $[\mathfrak{c}] = C$. In the following sums we shall always omit the terms with zero denominator. We have

$$E(\tau_C, s) = E(\alpha/\beta, s) = \operatorname{Im}(\alpha/\beta)^s \left|\beta\right|^{2s} \sum_{m,n} \frac{1}{\left|m\alpha + n\beta\right|^{2s}}.$$

Let $0 \neq \gamma \in \mathfrak{c}_f$. Since $\gamma \in \mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K$, we have $\gamma \equiv t \pmod{f\mathcal{O}_K}$ for some $t \in \mathbb{Z}$. Let $d \geq$ be the greatest common divisor of f and t in $\mathbb{Z}$. Then $d\mathcal{O}_K = f\mathcal{O}_K + t\mathcal{O}_K = f\mathcal{O}_K + \gamma\mathcal{O}_K$. Write $\gamma = \gamma' d$, $f = f'd$, $t = t'd$, where $f', t' \in \mathbb{Z}$ and $\gamma \in \mathcal{O}_{f'}$. We now rearrange the sum over $0 \neq \gamma \in \mathfrak{c}_f$ according to the greatest common divisor of γ and f.

$$\begin{aligned}\sum_{m,n} \frac{1}{\left|m\alpha + n\beta\right|^{2s}} &= \sum_{\gamma \in \mathfrak{c}_f} \frac{1}{\left|\gamma\right|^{2s}} = \sum_{d|f} \sum_{(\gamma, f) = d} \frac{1}{\left|\gamma\right|^{2s}} = \sum_{d|f} \frac{1}{d^{2s}} \sum_{(\gamma/d, f/d) = 1} \frac{1}{\left|\gamma/d\right|^{2s}} \\ &= \sum_{f'|f} (f'/f)^{2s} \sum_{(\gamma', f') = 1} \frac{1}{\left|\gamma'\right|^{2s}}\end{aligned}$$

Since $\gamma \in \mathfrak{c}_f$, we have $\gamma\mathcal{O}_f = \mathfrak{c}_f\mathfrak{a}_f$ for some $\mathcal{O}_f$-ideal $\mathfrak{a}_f$ depending on γ. Multiplying by $\mathcal{O}_K$ we obtain $\gamma\mathcal{O}_K = \mathfrak{c}\mathfrak{a}$, where $\mathfrak{c} = \mathfrak{c}_f\mathcal{O}_K$ and $\mathfrak{a} = \mathfrak{a}_f\mathcal{O}_K$ are ideals in $\mathcal{O}_K$. The ideal $\mathfrak{c}_f$ is prime to f and so $\mathfrak{c}$ is also prime to f. Consequently $\mathfrak{c}$ is prime to d, a divisor of f. Since d divides γ, the ideal $d\mathcal{O}_K$ divides $\mathfrak{c}\mathfrak{a}$. Therefore $d\mathcal{O}_K$ divides $\mathfrak{a}$. Write $\mathfrak{a} = d\mathcal{O}_K\mathfrak{a}'$. Then $\gamma'\mathcal{O}_K = \mathfrak{c}\mathfrak{a}'$, and $\mathfrak{a}'$ is prime to f' since γ' is. We can write $\gamma' \equiv t' \pmod{f'\mathcal{O}_K}$ because $\gamma \equiv t \pmod{f\mathcal{O}_K}$. Thus, as $(t', f') = 1$, we have $\gamma'\mathcal{O}_K \in P_{K,\mathbb{Z}}(f')$. It follows that $[\mathfrak{a}'] = C^{-1}$ in $I_K(f')/P_{K,\mathbb{Z}}(f')$. Conversely, if $\mathfrak{a}' \in I_K(f)$ and $[\mathfrak{a}'] = C^{-1}$ in $I_K(f')/P_{K,\mathbb{Z}}(f')$, then there exists $\gamma' \in P_{K,\mathbb{Z}}(f')$ such that $\gamma'\mathcal{O}_K = \mathfrak{c}\mathfrak{a}'$. If u is a unit in $\mathcal{O}_{f'}$, then to γ' and $u\gamma'$ corresponds the same ideal $\mathfrak{a}'$.

$$\begin{aligned}\sum_{m,n} \frac{1}{\left|m\alpha + n\beta\right|^{2s}} &= \sum_{f'|f} w_{f'} (f'/f)^{2s} \sum_{\gamma'\mathcal{O}_K \in P_{K,\mathbb{Z}}(f')} \frac{1}{N(\gamma'\mathcal{O}_K)^s} \\ &= \frac{1}{N(\mathfrak{c})^s} \sum_{f'|f} w_{f'} (f'/f)^{2s} \sum_{\substack{\mathfrak{a} \in I_K(f'), [\mathfrak{a}] = C^{-1} \\ \mathfrak{a} \subseteq \mathcal{O}_K}} \frac{1}{N(\mathfrak{a})^s}\end{aligned}$$

We have proved that

$$E(\tau_C, s) = \frac{\operatorname{Im}(\alpha/\beta)^s \left|\beta\right|^{2s}}{N(\mathfrak{c})^s} \sum_{f'|f} w_{f'} (f'/f)^{2s} \sum_{\substack{\mathfrak{a} \in I_K(f'), [\mathfrak{a}] = C^{-1} \\ \mathfrak{a} \subseteq \mathcal{O}_K}} \frac{1}{N(\mathfrak{a})^s}.$$

It remains to calculate the factor in the front. The norm $N(\mathfrak{c})$ can be calculated from the basis $[\alpha, \beta]$ as follows.

$$N(\mathfrak{c}) = \frac{\left|\Delta(\mathfrak{b})\right|^{1/2}}{f \left|d_K\right|^{1/2}} = \frac{\left|\det \left(\begin{smallmatrix} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{smallmatrix}\right)\right|}{f \left|d_K\right|^{1/2}} = \frac{\left|\alpha\overline{\beta} - \overline{\alpha}\beta\right|}{f \left|d_K\right|^{1/2}}$$

Next

$$\frac{\left|\alpha\overline{\beta} - \overline{\alpha}\beta\right|^s}{\left|\beta\right|^{2s}} = \frac{\left|\alpha\overline{\beta} - \overline{\alpha}\beta\right|^s}{\left|\left|\beta\right|^2\right|^s} = \frac{\left|\alpha\overline{\beta} - \overline{\alpha}\beta\right|^s}{\left|\beta\overline{\beta}\right|^s} = \left|\frac{\alpha}{\beta} - \frac{\overline{\alpha}}{\overline{\beta}}\right|^s = 2^s \operatorname{Im}(\alpha/\beta)^s.$$

Hence

$$\frac{\operatorname{Im}(\alpha/\beta)^s\,|\beta|^{2s}}{N(\mathfrak{c})^s} = \frac{f^s\,|d_K|^{s/2}}{\left|\alpha\overline{\beta}-\overline{\alpha}\beta\right|^s}\operatorname{Im}(\alpha/\beta)^s\,|\beta|^{2s} = \frac{f^s\,|d_K|^{s/2}}{2^s}.$$

This proof is based on [Mey57, II.,§4.]. □

Now consider a homomorphism $\chi\colon I_K(f) \longrightarrow \mathbb{C}^\times$ which is trivial on $P_{K,\mathbb{Z}}(f)$, or equivalently a homomorphism $\chi\colon \mathrm{Cl}_f \longrightarrow \mathbb{C}^\times$. Thus if C is the ideal class of $\mathfrak{a}$ in $I_K(f)/P_{K,\mathbb{Z}}(f)$, then $\chi(C) = \chi([\mathfrak{a}]) = \chi(\mathfrak{a})$. We can extend χ to all ideals of $\mathcal{O}_K$ by setting $\chi(\mathfrak{a}) = 0$ if $\mathfrak{a}$ is not prime to f. The L-series of conductor f associated with χ is defined as

$$L_f(s,\chi) = \sum_{\substack{\mathfrak{a}\in I_K(f)\\ \mathfrak{a}\subseteq\mathcal{O}_K}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}.$$

This series converges absolutely and locally uniformly in some half-plane, and the function $L_f(s,\chi)$ has analytic continuation to the entire complex plane, except for a simple pole at $s=1$ when χ is the trivial character. Arranging the ideals in the sum according to their ideal class we obtain

$$L_f(s,\chi) = \sum_{C\in\mathrm{Cl}_f} \chi(C)\zeta_f(s,C).$$

Let f' be a divisor of f. Consider a character $\chi\colon \mathrm{Cl}_f \longrightarrow \mathbb{C}^\times$. The character χ factors through $\psi_{f,f'}$ if and only if χ is trivial on $\ker\psi_{f,f'}$. A character $\chi\colon \mathrm{Cl}_f \longrightarrow \mathbb{C}^\times$ is called primitive if it does not factor through $\psi_{f,f'}$ for any divisor f' of f, except for $f'=f$.

Proposition 4.1.4. *Let w_f be the number of units in $\mathcal{O}_f$ and let $\chi\colon \mathrm{Cl}_f \longrightarrow \mathbb{C}^\times$ be a primitive character. We have*

$$w_f\frac{f^s\,|d_K|^{s/2}}{2^s}L_f(s,\chi) = \sum_{C\in\mathrm{Cl}_f}\overline{\chi}(C)E(\tau_C,s).$$

Proof. Note that $\overline{\chi}(C) = \chi(C^{-1})$. By Proposition 4.1.3 we have

$$\begin{aligned}
\sum_{C\in\mathrm{Cl}_f}\overline{\chi}(C)E(\tau_C) &= \frac{f^s\,|d_K|^{s/2}}{2^s}\sum_{f'|f} w_{f'}(f'/f)^{2s}\sum_{C\in\mathrm{Cl}_f}\chi(C^{-1})\zeta_{f'}(s,\psi_{f,f'}(C^{-1}))\\
&= \frac{f^s\,|d_K|^{s/2}}{2^s}\sum_{f'|f} w_{f'}(f'/f)^{2s}\sum_{C\in\mathrm{Cl}_f}\chi(C)\zeta_{f'}(s,\psi_{f,f'}(C))\\
&= \frac{f^s\,|d_K|^{s/2}}{2^s}\sum_{f'|f} w_{f'}(f'/f)^{2s}\sum_{C'\in\mathrm{Cl}_{f'}}\zeta_{f'}(s,C')\sum_{C\in\psi_{f,f'}^{-1}(C')}\chi(C).
\end{aligned}$$

Let

$$S_{f,f'} = \sum_{C\in\psi_{f,f'}^{-1}(C')}\chi(C).$$

If $f' = f$ then $\psi_{f,f'}$ is the identity map, and so $S_{f,f'} = \chi(C)$. We claim that if $1 \leq f' < f$ then $S_{f',f} = 0$. Let $C_0 \in \psi_{f,f'}^{-1}(C')$. We have

$$S_{f,f'} = \chi(C_0) \sum_{D \in \ker \psi_{f,f'}} \chi(D). \tag{4.4}$$

Since χ is a primitive character of Cl_f, there exists $D_0 \in \ker \psi_{f,f'}$ such that $\chi(D_0) \neq 1$. On multiplying (4.4) by $\chi(D_0)$ we obtain

$$\chi(D_0) S_{f,f'} = \chi(C_0) \sum_{D \in \ker \psi_{f,f'}} \chi(D_0 D) = \chi(C_0) \sum_{D_1 \in \ker \psi_{f,f'}} \chi(D_1) = S_{f,f'}.$$

It follows that $(\chi(D_0) - 1) S_{f,f'} = 0$. But $\chi(D_0) \neq 0$, so $S_{f,f'} = 0$, proving our claim. If we now look at our sum, we see that the only nonzero contribution comes from $f' = f$. This completes the proof. This proof is based on [Mey57, II.,§4.]. Meyer in turn credits Dedekind [Ded00]. □

Proposition 4.1.5. *Let χ be a primitive character of Cl_f. In the case $f = 1$ suppose also that χ is nontrivial. In a neighbourhood of $s = 1$ we have*

$$\frac{1}{2\pi} w_f \frac{f^s \left|d_K\right|^{s/2}}{2^s} L_f(s, \chi) = - \sum_{C \in \mathrm{Cl}_f} \overline{\chi}(C) \log \left(y_C^{1/2} \left|\eta(\tau_C)\right|^2 \right) + O(s-1).$$

In particular, since $L_f(s, \chi)$ is analytic at $s = 1$, we have

$$\frac{1}{2\pi} \frac{w_f}{2} f \left|d_K\right|^{1/2} L_f(1, \chi) = - \sum_{C \in \mathrm{Cl}_f} \overline{\chi}(C) \log \left(y_C^{1/2} \left|\eta(\tau_C)\right|^2 \right).$$

Proof. By Proposition 4.1.4 we have

$$w_f \frac{f^s \left|d_K\right|^{s/2}}{2^s} L_f(s, \chi) = \sum_{C \in \mathrm{Cl}_f} \overline{\chi}(C) E(\tau_C, s).$$

By virtue of the Kronecker limit formula (Theorem 4.1.1), the right-hand side of this expression is

$$\sum_{C \in \mathrm{Cl}_f} \overline{\chi}(C) \left(\frac{\pi}{s-1} + 2\pi \left(\gamma - \log 2 - \log(y_C^{1/2} \left|\eta(\tau_C)\right|^2) \right) + O(s-1) \right).$$

Since χ is a nontrivial character, we have $\sum_{C \in \mathrm{Cl}_f} \overline{\chi}(C) = 0$. Therefore

$$w_f \frac{f^s \left|d_K\right|^{s/2}}{2^s} L_f(s, \chi) = -2\pi \sum_{C \in \mathrm{Cl}_f} \overline{\chi}(C) \log(y_C^{1/2} \left|\eta(\tau_C)\right|^2) + O(s-1).$$

This is the first relation. Note that the character sum does not cause the error terms to cancel, because each of them depends on the corresponding ideal class. We obtain the second relation by letting s tend to 1. □

For any field discriminant D, or $D = 1$, the Kronecker symbol χ_D is defined as

$$\chi_D(p) = \left(\frac{D}{p} \right), \qquad p \text{ odd prime},$$

$$\chi_D(2) = \begin{cases} 0, & \text{if } D \equiv 0 \pmod 4, \\ 1, & \text{if } D \equiv 1 \pmod 8, \\ -1, & \text{if } D \equiv 5 \pmod 8, \end{cases}$$

$$\chi_D(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \chi_D(p_1)^{\alpha_1} \cdots \chi_D(p_k)^{\alpha_k}.$$

Theorem 4.1.6. *The function χ_D is periodic modulo $|D|$, so we can extend it to a real Dirichlet character $\chi_D\colon \mathbb{Z} \longrightarrow \{\pm 1\}$. The character χ_D is primitive, and conversely every every real primitive Dirichlet character is of this form. We have*

$$\chi_D(-1) = \begin{cases} 1, & \text{if } D > 0, \\ -1, & \text{if } D < 0. \end{cases}$$

The value of the character χ_D at a prime p determines the decomposition of the ideal $p\mathcal{O}_K$ into prime ideals in the quadratic field $K = \mathbb{Q}(\sqrt{D})$:

$$\chi_D(p) = \begin{cases} -1 & \text{if } p\mathcal{O}_K = \mathfrak{p}, \\ 1 & \text{if } p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}, \mathfrak{p} \neq \overline{\mathfrak{p}}, \\ 0 & \text{if } p\mathcal{O}_K = \mathfrak{p}^2. \end{cases}$$

If D_1 and D_2 are relatively prime discriminants of quadratic fields, then D_1D_2 is also a discriminant of a quadratic field and $\chi_{D_1D_2} = \chi_{D_1}\chi_{D_2}$.

Proof. See [Zag81, §5., Satz 4; §11., Satz 1]. □

With the character χ_D is associated its L-series

$$L_D(s) = \sum_{n=1}^{\infty} \frac{\chi_D(n)}{n^s}, \qquad \mathrm{Re}(s) > 0.$$

For $\mathrm{Re}(s) > 1$ we have an Euler product representation

$$L_D(s) = \prod_p \left(1 + \frac{\chi_D(p)}{p^s} + \frac{\chi_D(p^2)}{p^{2s}} + \cdots\right) = \prod_p \left(1 - \frac{\chi_D(p)}{p^s}\right)^{-1}.$$

Now we use the Kronecker symbol χ_D to define certain real characters of $\mathrm{Cl}_f \cong I_K(f)/P_{K,\mathbb{Z}}(f)$, the so called genus characters. First we restrict ourselves to the case of $\mathrm{Cl}_K = I_K/P_K$. Write $d_K = gt$, where $g > 0$ and $t < 0$ are either discriminants of quadratic fields, or $g = 1$ and $t = d_K$. For a nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ define

$$\chi_{g,t}(\mathfrak{p}) = \begin{cases} \chi_g(N(\mathfrak{p})) & \text{if } (N(\mathfrak{p}), g) = 1, \\ \chi_t(N(\mathfrak{p})) & \text{if } (N(\mathfrak{p}), t) = 1. \end{cases}$$

Theorem 4.1.7. *Let K be an imaginary quadratic field and d_K its discriminant.*

(1) The function $\chi_{g,t}$ is a well defined real character of Cl_K.

(2) There is a bijective correspondence between the real characters of Cl_K and the decompositions of the discriminant d_k of the form $d_K = gt$, where $g > 0$ and $t < 0$ are either discriminants of quadratic fields, or $g = 1$ and $t = d_K$. The decomposition $d_K = gt$ corresponds to the character $\chi_{g,t}$.

(3) We have the following decomposition of L-series

$$L(s, \chi_{g,t}) = L_g(s)L_t(s).$$

Proof. See [Zag81, §21., Satz 2]. □

Now we need a generalization of the character $\chi_{g,t}$. Let f be a positive integer and write $f^2 d_k = (fg)(ft)$, where g and t are as above. Then we define for prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ prime to f

$$\chi_{fg,ft}(\mathfrak{p}) = \begin{cases} \chi_{fg}(N(\mathfrak{p})) & \text{if } (N(\mathfrak{p}), g) = 1, \\ \chi_{ft}(N(\mathfrak{p})) & \text{if } (N(\mathfrak{p}), t) = 1. \end{cases}$$

Note that the norm $N(\mathfrak{p})$ is prime to at least one of the discriminants g, t. See [Zag81, p. 40].

Proposition 4.1.8. *The function $\chi_{fg,ft}$ is a primitive character of the class group $\mathrm{Cl}_f \cong I_K(f)/P_{K,\mathbb{Z}}(f)$.*

Proof. (1) $\chi_{fg,ft}$ is well defined. We must prove that $\chi_{fg}(N(\mathfrak{p})) = \chi_{ft}(N(\mathfrak{p}))$ where $\mathfrak{p}$ is a prime ideal which is prime to both of the discriminants g and t. If $N(\mathfrak{p}) = p^2$ then

$$\chi_{fg}(N(\mathfrak{p})) = \chi_{fg}(p^2) = \chi_{fg}(p)^2 = 1 = \chi_{ft}(p)^2 = \chi_{ft}(p^2) = \chi_{ft}(N(\mathfrak{p})),$$

so in this case the definition is valid. If $N(\mathfrak{p}) = p$, then since $\mathfrak{p}$ is prime to the discriminant gt, we have $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ with $\mathfrak{p} \neq \overline{\mathfrak{p}}$. Therefore $\chi_{gt}(p) = 1$, or

$$\left(\frac{gt}{p}\right) = 1, \qquad \left(\frac{fg}{p}\right)\left(\frac{ft}{p}\right) = 1, \qquad \left(\frac{fg}{p}\right) = \left(\frac{ft}{p}\right),$$

or $\chi_{fg}(N(\mathfrak{p})) = \chi_{fg}(p) = \chi_{ft}(p) = \chi_{ft}(N(\mathfrak{p}))$.

(2) $\chi_{fg,ft}$ is trivial on $P_{K,\mathbb{Z}}(f)$. Let $\alpha\mathcal{O}_K \in P_{K,\mathbb{Z}}(f)$. Then $N(\alpha\mathcal{O}_K) = N(\alpha) = \alpha\overline{\alpha}$. By definition of $P_{K,\mathbb{Z}}(f)$, we have $\alpha \equiv a \pmod{f\mathcal{O}_K}$ for some $a \in \mathbb{Z}$ prime to f. Hence $N(\alpha\mathcal{O}_K) \equiv a^2 \pmod{f}$. Next, we have

$$\alpha = \frac{x + y\sqrt{gt}}{2}, \quad x, y \in \mathbb{Z}, \qquad N(\alpha\mathcal{O}_K) = \frac{x^2 + y^2\,|gt|}{4} \equiv \frac{x^2}{4} \pmod{g, t}.$$

Since $(f, gt) = 1$, there exists $t \in \mathbb{Z}$ such that

$$\begin{aligned} t &\equiv a \pmod{f}, \\ t &\equiv x/2 \pmod{g, t}. \end{aligned}$$

Using the fact that $(f, gt) = 1$ one more time, we get

$$N(\alpha\mathcal{O}_K) \equiv t^2 \pmod{fg, ft}.$$

Without loss of generality we may suppose that α and g are relatively prime. Then

$$\chi_{fg,ft}(\alpha\mathcal{O}_K) = \chi_{fg}(N(\alpha\mathcal{O}_K)) = \chi_{fg}(t^2) = \chi_{fg}(t)^2 = 1.$$

(3) $\chi_{fg,ft}$ is primitive. We will prove this only in the case when f is a prime inert in K, as this is the only case which we will use. We must exhibit an element $\alpha\mathcal{O}_K \in P_{K,\mathbb{Z}}(1) = P_K$ such that $\chi_{fg,ft}(\alpha\mathcal{O}_K) = -1$. Take $\alpha = f + \sqrt{gt}$. Then $N(\alpha) = f^2 - gt$, and

$$\begin{aligned} \chi_{fg,ft}(\alpha\mathcal{O}_K) &= \chi_{fg}(N(\alpha)) = \chi_f(N(\alpha))\chi_g(N(\alpha)) = \chi_f(f^2 - gt)\chi_g(f^2 - gt) \\ &= \chi_f(-1)\chi_f(gt)\chi_g(f^2) = \chi_f(gt), \end{aligned}$$

because by Theorem 4.1.6 we have $\chi_{fg} = \chi_f\chi_g$ and $\chi_f(-1) = 1$. Since $f \equiv 1 \pmod 4$, Quadratic Reciprocity implies

$$\left(\frac{p}{f}\right) = \left(\frac{f}{p}\right), \quad p \text{ odd}, \quad \left(\frac{2}{f}\right) = \left(\frac{f}{2}\right) = \begin{cases} 1 & \text{if } f \equiv 1 \pmod 8, \\ -1 & \text{if } f \equiv 5 \pmod 8. \end{cases} \tag{4.5}$$

If $gt = 2^\alpha p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the prime factorization of gt, then according to the definition of the Kronecker symbol and (4.5) we have

$$\begin{aligned} \chi_f(gt) &= \left(\frac{f}{2}\right)^\alpha \left(\frac{f}{p_1}\right)^{\alpha_1} \cdots \left(\frac{f}{p_k}\right)^{\alpha_k} = \left(\frac{2}{f}\right)^\alpha \left(\frac{p_1}{f}\right)^{\alpha_1} \cdots \left(\frac{p_k}{f}\right)^{\alpha_k} \\ &= \left(\frac{gt}{f}\right) = \chi_{gt}(f) = -1. \end{aligned}$$

as f is inert in K. Therefore $\chi_{fg,ft}(\alpha\mathcal{O}_K) = -1$, meaning that the character $\chi_{fg,ft}$ is primitive. For the general case, see Siegel's remarks in [Sie68].

□

Proposition 4.1.9. *We have the decompostion*

$$L_f(s, \chi_{fg,ft}) = L_{fg}(s)L_{ft}(s).$$

Proof. We compare the local factors in

$$L_f(s, \chi_{fg,ft}) = \prod_{\mathfrak{p}} \left(1 - \frac{\chi_{fg,ft}(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1} \tag{4.6}$$

and

$$L_{fg}(s)L_{ft}(s) = \prod_p \left(1 - \frac{\chi_{fg}(p)}{p^s}\right)^{-1} \left(1 - \frac{\chi_{ft}(p)}{p^s}\right)^{-1}. \tag{4.7}$$

Here we set $\chi_{fg,ft}(\mathfrak{p}) = 0$ if $\mathfrak{p}$ and f are not relatively prime. Let $K = \mathbb{Q}(\sqrt{gt})$ and write $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. For every local factor in the Euler product there are three possibilities for the value of $\chi_{fg,ft}(\mathfrak{p})$:

(1) $\chi_{fg,ft}(\mathfrak{p}) = -1$. We know that p does not divide f and at least one of the discriminants g and t. We may suppose that p does not divide g, as the other case is dealt with similarly. Next $N(\mathfrak{p}) = p$ or p^2, but it cannot be p^2, because $\chi_{fg}(N(p)) = -1$. Therefore $N(\mathfrak{p}) = p$, and so either $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ with $\mathfrak{p} \neq \overline{\mathfrak{p}}$ or $p\mathcal{O}_K = \mathfrak{p}^2$.

(a) $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ and $\mathfrak{p} \neq \overline{\mathfrak{p}}$. We have $\chi_{fg,ft}(\overline{\mathfrak{p}}) = \chi_{fg}(N(\overline{\mathfrak{p}})) = \chi_{fg}(p) = -1$. Thus the contribution of $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ to the product (4.6) is

$$\left(1 - \frac{\chi_{fg,ft}(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1} \left(1 - \frac{\chi_{fg,ft}(\overline{\mathfrak{p}})}{N(\mathfrak{p})^s}\right)^{-1} = \left(1 + \frac{1}{p^s}\right)^{-2}.$$

On the other hand, since p does not divide t, we have $\chi_{ft}(p) = \chi_{fg}(p) = -1$ and so the contribution of p to the product (4.7) is

$$\left(1 - \frac{\chi_{fg}(p)}{p^s}\right)^{-1} \left(1 - \frac{\chi_{ft}(p)}{p^s}\right)^{-1} = \left(1 + \frac{1}{p^s}\right)^{-2}.$$

(b) $p\mathcal{O}_K = \mathfrak{p}^2$. The contribution to the product (4.6) coming from $\mathfrak{p}$ is

$$\left(1 - \frac{\chi_{fg,ft}(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1} = \left(1 + \frac{1}{p^s}\right)^{-1}.$$

Since $\mathfrak{p}$ is ramified and p does not divide g, p must divide t, and so $\chi_{ft}(p) = 0$. As $\chi_{fg}(p) = -1$, the contribution of p to the product (4.7) is

$$\left(1 - \frac{\chi_{fg}(p)}{p^s}\right)^{-1}\left(1 - \frac{\chi_{ft}(p)}{p^s}\right)^{-1} = \left(1 + \frac{1}{p^s}\right)^{-1}.$$

(2) $\chi_{fg,ft}(\mathfrak{p}) = 1$. We have two possibilities for the norm $N(\mathfrak{p})$:
   (a) $N(\mathfrak{p}) = p$. In this case the proof is the same as in the case (1),(a), but the contributions will have minus sign.
   (b) $N(\mathfrak{p}) = p^2$. In this case we have $p\mathcal{O}_K = \mathfrak{p}$, so $\chi_{gt}(p) = 1$. Observe that

$$\chi_{fg}(p)\chi_{ft}(p) = \left(\frac{fg}{p}\right)\left(\frac{ft}{p}\right) = \left(\frac{f^2}{p}\right)\left(\frac{gt}{p}\right) = -1.$$

It follows that $\{\chi_{fg}(p), \chi_{ft}(p)\} = \{1, -1\}$. Therefore

$$\begin{aligned}\left(1 - \frac{\chi_{fg,ft}(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1} &= \left(1 - \frac{1}{p^{2s}}\right)^{-1} = \left(1 + \frac{1}{p^s}\right)^{-1}\left(1 - \frac{1}{p^s}\right)^{-1} \\ &= \left(1 - \frac{\chi_{fg}(p)}{p^s}\right)^{-1}\left(1 - \frac{\chi_{ft}(p)}{p^s}\right)^{-1}\end{aligned}$$

which shows that the contribution of $\mathfrak{p}$ and p to the respective products (4.6) and (4.7) is the same.

(3) $\chi_{fg,ft}(\mathfrak{p}) = 0$. In this case p divides f so $\chi_{fg}(p) = \chi_{ft}(p) = 0$. Consequently the contribution to the products (4.6) and (4.7) is 1.

Note that the Euler product representations are valid for $\mathrm{Re}(s) > 1$, as are our manipulations with the individual factors because of absolute convergence. By analytic continuation our decomposition is valid for all s, except possibly for $s = 1$, this occurs when $\chi_{fg,ft}$ is the trivial character and its L-series has a simple pole at $s = 1$. □

Theorem 4.1.10 (Dirichlet class number formula)**.** *Let K be a quadratic field and d_K its discriminants. If $d_K < 0$ we have*

$$L_{d_K}(1) = \frac{2\pi h_K}{\#\mathcal{O}_K^\times |d_K|^{1/2}},$$

If $d_K > 0$ we have

$$L_{d_K}(1) = \frac{2h_K \log \varepsilon_K}{d_K^{1/2}},$$

where ε_K is a fundamental unit in $\mathcal{O}_K$ such that $\varepsilon_K > 1$.

Proof. See [Zag81, §8., Satz 5]. □

Theorem 4.1.11 (Dirichlet-Kronecker formula)**.** *Let $K = \mathbb{Q}(\sqrt{gt})$ be an imaginary quadratic field with discriminant d_K. Consider the decomposition $f^2 d_K = fgft$, where $f > 0$ and $g > 0$ are either discriminants of real quadratic fields, or $f = 1$ and $g = 1$ (in the case $f = 1$, we suppose that $g \neq 1$ to prevent $\chi_{fg,ft}$ from being the trivial character), and $t < 0$ is a discriminant of an imaginary quadratic field. Let h_{fg} and h_{ft} be the class numbers of the quadratic fields $\mathbb{Q}(\sqrt{fg})$ and $\mathbb{Q}(\sqrt{ft})$, respectively. Further let $w_{gt,f}$ be the number of units in the order $\mathcal{O}_f$ of conductor f in $K = \mathbb{Q}(\sqrt{gt})$, and $w_{ft,1}$ the number of units in the maximal order (the ring of integers) $\mathcal{O}_1 = \mathcal{O}_{\mathbb{Q}(\sqrt{ft})}$ of the imaginary quadratic field $\mathbb{Q}(ft)$. We have*

$$\varepsilon_{fg}^{w_{gt,f} w_{ft,1}^{-1} h_{fg} h_{ft}} = \prod_{C \in \mathrm{Cl}_f} \left| y_C^{1/2} \eta(\tau_C)^2 \right|^{-\chi_{fg,ft}(C)}.$$

In particular, if the only units in $\mathcal{O}_{\mathbb{Q}(\sqrt{ft})}$ and $\mathcal{O}_{\mathbb{Q}(\sqrt{gt})}$ are $\{\pm 1\}$, then

$$\varepsilon_{fg}^{h_{fg} h_{ft}} = \prod_{C \in \mathrm{Cl}_f} \left| y_C^{1/2} \eta(\tau_C)^2 \right|^{-\chi_{fg,ft}(C)}.$$

Proof. As the character $\chi_{fg,ft}$ is primitive and in the case $f = 1$ nontrivial, we may apply Proposition 4.1.5 to obtain

$$\frac{1}{2\pi} \frac{w_{gt,f}}{2} fg^{1/2} |t|^{1/2} L_f(1, \chi_{fg,ft}) = -\sum_{C \in \mathrm{Cl}_f} \chi(C) \log \left(y_C^{1/2} |\eta(\tau_C)|^2 \right).$$

Using the decomposition of L-series provided by Proposition 4.1.9 we get

$$\frac{1}{2\pi} \frac{w_{gt,f}}{2} fg^{1/2} |t|^{1/2} L_{fg}(1) L_{ft}(1) = -\sum_{C \in \mathrm{Cl}_f} \chi(C) \log \left(y_C^{1/2} |\eta(\tau_C)|^2 \right).$$

The right-hand side, according to the Dirichlet class number formula (Theorem 4.1.10) for discriminants $fg > 0$ and $ft < 0$, is

$$\frac{1}{2\pi} \frac{w_{gt,f}}{2} fg^{1/2} |t|^{1/2} \cdot \frac{2 h_{fg} \log \varepsilon_{fg}}{f^{1/2} g^{1/2}} \cdot \frac{2\pi h_{ft}}{w_{ft,1} f^{1/2} |t|^{1/2}}.$$

This simplifies to

$$\frac{\omega_{gt,f}}{w_{ft,1}} h_{fg} h_{ft} \log \varepsilon_{fg}.$$

Taking the exponential we get the desired formula. □

4.2 Class number 1 and an inert conductor f

Theorem 4.2.1. *Let K be an imaginary quadratic field, d_K its discriminant, $\mathcal{O}_f$ the order of conductor f in K, and h_f the class number of $\mathcal{O}_f$. Then*

$$h_f = \frac{h_K f}{[\mathcal{O}_K^\times : \mathcal{O}_f^\times]} \prod_{p \mid f} \left(1 - \frac{\chi_{d_K}(p)}{p} \right).$$

In particular, if f is a prime which is inert in K, $h_K = 1$, and $d_K < -4$, then we have $h_f = f + 1$.

$$h_f = \begin{cases} f + 1 & \text{if } d_K < -4, \\ \frac{1}{2}(f+1) & \text{if } d_K = -4, \\ \frac{1}{3}(f+1) & \text{if } d_K = -3. \end{cases}$$

Proof. See [Cox11, §7., D., Thm. 7.24., p. 132]. The second statement follows from Theorem 4.1.6 which says that a prime p is inert in K if and only if $\chi_{d_K}(p) = -1$, and from the fact that a proper order can contain only the trivial units ± 1. □

From now on we shall assume that $K = \mathbb{Q}(\sqrt{-p})$, where $p \equiv 3 \pmod 4$ is a prime, that f is a prime inert in K, and that the class number of K is equal to 1. Our decomposition $f^2 d_K = fgft$ is therefore necessarily $f^2(-p) = f \cdot 1 \cdot f(-p)$, that is, $g = 1$ and $t = -p$. Now consider the matrices

$$\alpha_k = \begin{pmatrix} 1 & k \\ & f \end{pmatrix}, \qquad \alpha_\infty = \begin{pmatrix} f & \\ & 1 \end{pmatrix},$$

and the set

$$R_f = \{\alpha_k \colon k \bmod f\} \cup \{\alpha_\infty\}.$$

The set R_f is a set of representatives for the left action of $\mathrm{SL}_2(\mathbb{Z})$ on the set $M_2^f(\mathbb{Z})$ of 2-by-2 matrices with integral entries and determinant equal to f:

$$\mathrm{SL}_2(\mathbb{Z}) \backslash M_2^f(\mathbb{Z}) = \{\mathrm{SL}_2(\mathbb{Z})\alpha \colon \alpha \in R_f\}.$$

Note that $\# R_f = f + 1$.

Proposition 4.2.2. *Let $\tau \in \mathfrak{H} \cap K$. Then the fractional ideals $[\alpha\tau, 1]$, where $\alpha \in R_f$, are proper ideals of $\mathcal{O}_f$.*

Proof. We may assume that $\mathcal{O}_K = [\tau, 1]$, for otherwise, as $h_K = 1$, there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and $\omega \in \mathfrak{H}$ such that $\tau = \gamma\omega$ and $\mathcal{O}_K = [1, \omega]$, so our fractional ideals are $[\alpha\gamma\omega, 1] = [\gamma'\alpha'\omega, 1] = \lambda[\alpha'\omega, 1]$, where $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$, $\alpha' \in R_f$, and $\lambda \in K^\times$. We have accordingly $[\alpha_\infty\tau, 1] = [f\tau, 1] = \mathcal{O}_f$ and this is trivially a proper ideal of $\mathcal{O}_f$. Define

$$M_k = \{\lambda \in K \colon \lambda[\alpha_k\tau, 1] \subseteq [\alpha_k\tau, 1]\}.$$

We want to show that $M_k = \mathcal{O}_f$. To show that $\mathcal{O}_f \subseteq M_k$, it suffices to show that $f\tau \in M_k$. The fractional ideal $[\alpha_k\tau, 1]$ is proper if and only if the ideal $[\tau + k, f]$ is proper. Let $\tau^2 + B\tau + C = 0$ be the minimal equation of τ. We have

$$\begin{aligned} (f\tau)f &= f^2(\tau + k) - (kf)f, \\ f\tau(\tau + k) &= (fk - Bf)(\tau + k) - (C + k^2 - kB)f, \end{aligned}$$

meaning that $f\tau \in M_k$. Conversely, let $\lambda \in M_k$. We know that λ is an algebraic integer, so we can write $\lambda = a + b\tau$, where $a, b \in \mathbb{Z}$. We have

$$\begin{aligned} (a + b\tau)(\tau + k) &= x(\tau + k) + yf, \qquad x, y \in \mathbb{Z}, \\ (a - x + b\tau)(\tau + k) &\equiv 0 \pmod{f\mathcal{O}_K}. \end{aligned}$$

Since $f\mathcal{O}_K$ is a prime ideal, f must divide $\tau + k$ or $a - x + b\tau$. But f cannot divide $\tau + k$, because otherwise $\tau = -k + f\alpha$, for some $\alpha \in \mathcal{O}_K$, or $\tau \in \mathcal{O}_f$, a contradiction. Therefore $a - x + b\tau \equiv 0 \pmod{f\mathcal{O}_K}$. Again, because $f\mathcal{O}_K$ is a prime ideal, b is either invertible modulo f, or it is divisible by f. If b were invertible modulo f, then $\tau \equiv (x - a)b^{-1} \pmod{f\mathcal{O}_K}$, and we have contradiction as before. Thus b is divisible by f, and so $\lambda \in \mathcal{O}_f$, proving that $M_k \subseteq \mathcal{O}_f$. □

Proposition 4.2.3. *Let $\tau \in \mathfrak{H} \cap K$. Further let α_k, $\alpha_r \in R_f$, and $\lambda \in K^\times$ be such that $\lambda[\alpha_k\tau, 1] = [\alpha_r\tau, 1]$. Then $\lambda \in \mathcal{O}_K^\times$.*

Proof. As before we may assume that $\mathcal{O}_K = [\tau, 1]$. By symmetry, it is sufficient to prove that $\lambda \in \mathcal{O}_K$. We have

$$\begin{aligned} \lambda\frac{\tau+k}{f} &= a\frac{\tau+r}{f} + b, \\ \lambda &= c\frac{\tau+r}{f} + d, \end{aligned}$$

where $a, b, c, d \in \mathbb{Z}$, $ad - bc = 1$, implying

$$\begin{aligned} (c(\tau+r) + df)(\tau+k) &= ((\tau+r) + bf)f, \\ c(\tau+r)(\tau+k) &\equiv 0 \pmod{f\mathcal{O}_K}. \end{aligned}$$

Since $f\mathcal{O}_K$ is a prime ideal, we have $c = ft$ for some $t \in \mathbb{Z}$, similarly as in the proof of Proposition 4.2.2. Therefore $\lambda = t(\tau + r) + d$ is an element of $\mathcal{O}_K$. □

Proposition 4.2.4. *Let $\tau \in \mathfrak{H} \cap K$. Let $\alpha_k, \alpha_\infty \in R_f$. Let $\lambda \in K^\times$ be such that $\lambda[\alpha_k\tau, 1] = [\alpha_\infty\tau, 1]$. Then $\lambda \in \mathcal{O}_K^\times \cup f\mathcal{O}_K^\times$. If $d_K < -4$ then the lattices $[\alpha_k\tau, 1]$ and $[\alpha_\infty\tau, 1]$ are not homothetic.*

Proof. As before we may assume that $\mathcal{O}_K = [\tau, 1]$. Let $\lambda \in K^\times$ be such that $\lambda[\alpha_k\tau, 1] = [\alpha_\infty\tau, 1]$. Then

$$\begin{aligned} \lambda\frac{\tau+k}{f} &= af\tau + b, \\ \lambda &= cf\tau + d, \end{aligned} \tag{4.8}$$

where $a, b, c, d \in \mathbb{Z}$, $ad - bc = 1$, implying

$$\begin{aligned} (cf\tau + d)(\tau+k) &= (af\tau + b)f, \\ d(\tau+k) &\equiv 0 \pmod{f\mathcal{O}_K}. \end{aligned}$$

Since $f\mathcal{O}_K$ is a prime ideal, we have, as before, $d = ft$ for some $t \in \mathbb{Z}$. Now (4.8) implies that $\lambda = f\lambda'$ for some $\lambda' \in \mathcal{O}_K$. On the other hand, we have

$$\begin{aligned} \lambda^{-1}f\tau &= d\frac{\tau+k}{f} - b, \\ \lambda^{-1} &= -c\frac{\tau+k}{f} + a, \end{aligned}$$

or $f = (-c(\tau+k) + a)\lambda$, meaning that λ divides f. Therefore either $\lambda = uf$ for some $u \in \mathcal{O}_K^\times$, or $\lambda \in \mathcal{O}_K^\times$, because of the first part of the proof, or because $f\mathcal{O}_K$ is a prime ideal. If $d_K < -4$ then λ is a nonzero integer. Consequently, $f = (-c(\tau+k) + a)\lambda$ is a linear equation for τ, unless $c = 0$. But if $c = 0$, then $1 = ad - bc = aft$, a contradiction. □

Proposition 4.2.5. *Let $\tau \in \mathfrak{H} \cap K$ and let $\alpha_k, \alpha_\infty \in R_f$. Then $[\alpha_k\tau, 1] = [\alpha_r\tau, 1]$ if and only if $k \equiv r \pmod{f}$.*

Proof. If $k \equiv r \pmod f$ then clearly $[\tau + k, f] = [\tau + r, f]$. If $[\alpha_k \tau, 1] = [\alpha_r \tau, 1]$ then

$$\begin{aligned} \tau + k &= a(\tau + r) + bf, \\ f &= c(\tau + r) + df. \end{aligned}$$

for some $a, b, c, d \in \mathbb{Z}$, $ad - bc = 1$. Since $\tau \in \mathfrak{H}$, we must have $c = 0$, and so $d = 1$. The condition $ad - bc = 1$ implies that $a = 1$. Therefore the first equation is $k = r + bf$. □

The four previous propositions give together the following theorem.

Theorem 4.2.6. *Let $d_K < -4$. The fractional ideals $[\alpha\tau, 1], \alpha \in R_f$ form a complete set of representatives of the $f + 1$ ideal classes in Cl_f.*

We have $g = 1$ and $t = -p$, so our genus character is $\chi_{f,-fp}$. Let $\mathfrak{c}_k = [\alpha_k \tau, 1]$ and $\mathfrak{c}_\infty = [\alpha_\infty \tau, 1]$. We want a way to calculate the values of $\chi_{f,-fp}([\mathfrak{c}_k])$ and $\chi_{f,-fp}([\mathfrak{c}_\infty])$. The character $\chi_{f,-fp}$ was defined using norms of ideals in $I_K(f)$, that is, norms relatively prime to f. According to [Cox11, §7., C., 7.20.] these are the same norms as the norms of ideals in $I(\mathcal{O}_f, f)$. Again, by [Cox11, §7., B., 7.17.], the norms of ideals in $I(\mathcal{O}_f, f)$ are exactly the numbers relatively prime to f represented by the quadratic forms corresponding to these ideals. We have $f\mathfrak{c}_k = [\tau + k, f]$ and $\mathfrak{c}_\infty = [f\tau, 1]$. let $A^2\tau + B\tau + C = 0$ be the minimal equation for τ, that is, $A, B, C \in \mathbb{Z}$ and $(A, B, C) = 1$. Suppose that A is not divisible by f. The corresponding quadratic forms are

$$\begin{aligned} Q_k(x, y) &= (x(\tau + k) + yf)(x(\overline{\tau} + k) + yf) \\ &\equiv x^2(k^2 - BA^{-1}k + CA^{-1}) \pmod f, \\ Q_\infty(x, y) &= (xf\tau + y)(xf\overline{\tau} + y) \equiv y^2 \pmod f. \end{aligned}$$

Let $Q(k) = A(Ak^2 - Bk + C)$. We have

$$\begin{aligned} \chi_{f,-fp}([\mathfrak{c}_k]) &= \chi_f(Q(k)), \\ \chi_{f,-fp}([\mathfrak{c}_\infty]) &= \chi_f(y^2) = 1. \end{aligned}$$

Note that $Q(k)$ is not divisible by f, because

$$4Q(k) = (2Ak - B)^2 - (B^2 - 4AC),$$

and f is inert in K, so $\chi_f(B^2 - 4AC) = \chi_f(d_K) = -1$. Note also that we have by Quadratic Reciprocity (as in the proof of Proposition 4.1.8)

$$\chi_f(Q(k)) = \left(\frac{f}{Q(k)}\right) = \left(\frac{Q(k)}{f}\right).$$

Theorem 4.2.7. *Let $K = \mathbb{Q}(\sqrt{-p})$ be an imaginary quadratic field, where $p \equiv 3 \pmod 4$ is a prime such that $p > 3$. Suppose that $h_K = 1$. Let $\tau \in \mathfrak{H} \cap K$, and let $A\tau^2 + B\tau + C = 0$ be the minimal equation for τ, that is, $A, B, C \in \mathbb{Z}$ and $(A, B, C) = 1$. Let $f \equiv 1 \pmod 4$ be a prime inert in K and not dividing A. Let $Q_\tau(k) = Q(k)$ be as above. Then*

$$\varepsilon_f^{h_f h_{-fp}/2} = f^{-1/2} |\eta(f\tau)|^{-1} \prod_{k=0}^{f-1} \left| \eta\left(\frac{\tau + k}{f}\right) \right|^{-\chi_f(Q_\tau(k))} \tag{4.9}$$

Proof. We have by Theorem 4.1.11

$$\begin{aligned}\varepsilon_f^{h_f h_{-fp}} &= \prod_{C\in \mathrm{Cl}_f} \left|\mathrm{Im}(\tau_C)^{1/2}\eta(\tau_C)^2\right|^{-\chi_{f,-fp}(C)} \\ &= \mathrm{Im}(\alpha_\infty\tau)^{-1/2}\left|\eta(\alpha_\infty)\right|^{-2}\prod_{k=0}^{f-1}\mathrm{Im}(\alpha_k\tau)^{-\chi_f(Q(k))/2}\left|\eta(\alpha_k\tau)\right|^{-2\chi_f(Q(k))}\end{aligned}$$

Thus the product

$$\prod_{k=0}^{f-1}\left|\eta(\alpha_k\tau)\right|^{-2\chi_f(Q(k))}$$

is multiplied by the factor

$$f^{-1/2}\,\mathrm{Im}(\tau)^{-1/2}\left|\eta(f\tau)\right|^{-2} f^{1/2\sum_{k=0}^{f-1}\chi_f(Q(k))}\,\mathrm{Im}(\tau)^{-1/2\sum_{k=0}^{f-1}\chi_f(Q(k))}.$$

But $\sum_{k=0}^{f-1}\chi_f(Q(k)) = -1$, so this is equal to

$$f^{-1/2}\,\mathrm{Im}(\tau)^{-1/2}\left|\eta(f\tau)\right|^{-2} f^{-1/2}\,\mathrm{Im}(\tau)^{1/2} = f^{-1}\left|\eta(f\tau)\right|^{-2}.$$

Taking the positive square roots we obtain our formula. □

Note that, since f and p are distinct primes, the class number h_{-fp} is even. This follows from the existence of genus characters. See [Zag81, §12.] for details. Note also that if f divides B, then, since f is inert in K, C is a quadratic nonresidue modulo f, and so $Q(0) = -1$, meaning that the factor $|\eta(\alpha_0\tau)| = |\eta(\tau/f)|$ is in the numerator of the product in (4.9).

The formula (4.9) leads us to consider the modular function

$$\phi_f(\tau) = f^{-1/2}\eta(f\tau)^{-1}\prod_{k=0}^{f-1}\eta\left(\frac{\tau+k}{f}\right)^{-\chi_f(Q_\tau(k))}.$$

It is easy to see that the 24-th power

$$\phi_f(\tau)^{24} = f^{-12}\Delta(f\tau)^{-1}\prod_{k=0}^{f-1}\Delta\left(\frac{\tau+k}{f}\right)^{-\chi_f(Q_\tau(k))}$$

is a modular function of level f. Note that the function ϕ_f has no zeros and no poles in the upper half-plane. Modular functions of this type are called modular units. They are the subject of the book of Kubert and Lang titled *Modular Units* [KL81]. According to their Theorem 1.1 [KL81, 4., §1., p. 82], if $\ell > 3$ is a prime and g is a modular function such that g^k is a modular unit of level ℓ^a, then g is a modular function of level ℓ^a. Applying this to our function ϕ_f, we conclude that ϕ_f is a modular function of level f. It is not clear (to the author) whether there is a more direct proof of this. The theorem of Kubert and Lang was pointed out by J. Rouse.

In the case of $f = 5$ it is possible to prove a weaker version of the formula (4.9) directly without using the Kronecker limit formula or the class number formula. The function ϕ_5 has Fourier coefficients in $\mathbb{Q}(\sqrt{5})$ (see the proof of Theorem 4.4.3), so a minor modification of the criterion for class invariants (Theorem 3.3.10)

implies that the value $\phi_5(\tau)$ is an element of $K(\sqrt{5})$ if the coefficients of the minimal equation for τ have suitable reduction modulo 5. If τ has suitable real part, then the value $\phi_5(\tau)$ will be real, so $\phi_5(\tau) \in \mathbb{Q}(\sqrt{5})$. Now by an elementary theorem of Deuring [Deu58, 22., p. 42] the values at τ of the eta-quotients occurring in (4.9) are algebraic units. But all units in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ are generated by ε_5, so $\phi_5(\tau) = \varepsilon_5^m$ for some integer m. Since $\varepsilon_5 > 1$, if a lower bound on $|\phi_5(\tau)|$ was to be obtained, for example coming from the known Fourier expansion of the eta function, we could show that m is positive. This weaker version would be sufficient for the application in the class number problem.

Serre in the appendix to his book *Lectures on the Mordell-Weil Theorem* [Ser90, A.7., p. 197] gives an abstract way of constructing the function ϕ_f^{24}. Serre writes that *sometimes* the 24-th root ϕ_f can be used, but he does not specify what *sometimes* means.

Another question is, for which f does the function ϕ_f have Fourier coefficients in $\mathbb{Q}(\sqrt{f})$? If they are not in $\mathbb{Q}(\sqrt{f})$ then in which extension they lie?

4.3 Specialization to $f = 5$

In the following sections we will as before assume that $K = \mathbb{Q}(\sqrt{-p})$ is an imaginary quadratic field with class number 1, p being a prime such that $p \equiv 3 \pmod 4$. We shall now specialize $f = 5$. The assumption that 5 is inert in K means

$$-1 = \chi_{-p}(5) = \left(\frac{-p}{5}\right) = \left(\frac{p}{5}\right),$$

implying that $p \equiv 2, 3 \pmod 5$. Note that this in agreement with Proposition 1.2.3 which says that primes q such that $2 \leq q < p/4$ are inert in $K = \mathbb{Q}(\sqrt{-p})$ if K has class number 1. For $\mathcal{O}_K$ we choose the basis $[\omega, 1]$, where

$$\omega = \frac{fp + \sqrt{-p}}{2}.$$

We have $\omega\overline{\omega} = (f^2p^2 + p)/4$, so the function $Q_\omega(k)$ of the previous section is $Q_\omega(k) \equiv k^2 - p \pmod 5$, and

$$\chi_f(Q_\omega(k)) = \left(\frac{Q_\omega(k)}{5}\right) = \left(\frac{k^2 - p}{5}\right).$$

Note that it does not matter which set of representatives modulo f we choose in (4.9); we choose $-2, -1, 0, 1, 2$ following Siegel. We have

$$\begin{aligned}
&Q_\omega(1) = Q_\omega(4) = 1 \qquad Q_\omega(0) = Q_\omega(2) = Q_\omega(3) = -1 \qquad \text{if } p \equiv 2 \pmod 5,\\
&Q_\omega(2) = Q_\omega(3) = 1 \qquad Q_\omega(0) = Q_\omega(1) = Q_\omega(4) = -1 \qquad \text{if } p \equiv 3 \pmod 5.
\end{aligned}$$

Since $h_5 = 1$, the formula (4.9) takes the following form

$$\begin{aligned}
\varepsilon_5^{m_p} &= -5^{-1/2}\frac{\eta\left(\frac{\omega}{5}\right)\eta\left(\frac{\omega+2}{5}\right)\eta\left(\frac{\omega-2}{5}\right)}{\eta(5\omega)\,\eta\left(\frac{\omega+1}{5}\right)\eta\left(\frac{\omega-1}{5}\right)}, \qquad \text{if } p \equiv 2 \pmod 5,\\
\varepsilon_5^{m_p} &= -5^{-1/2}\frac{\eta\left(\frac{\omega}{5}\right)\eta\left(\frac{\omega+1}{5}\right)\eta\left(\frac{\omega-1}{5}\right)}{\eta(5\omega)\,\eta\left(\frac{\omega+2}{5}\right)\eta\left(\frac{\omega-2}{5}\right)}, \qquad \text{if } p \equiv 3 \pmod 5. \qquad (4.10)
\end{aligned}$$

Here $m_p = h_{-5p}/2$ is a positive integer, because as remarked above, the class number h_{-fp} is even by genus theory [Zag81]. Next

$$\varepsilon_5 = \frac{1+\sqrt{5}}{2}$$

is the fundamental unit of $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ normalized in such a way that $\varepsilon_5 > 1$. It remains to justify the discarding of the absolute values. Let

$$z_k = \frac{z+k}{5}, \qquad z_\infty = 5z.$$

where $z \in \mathbb{C}$ and $k \in \mathbb{Z}$. Observe that

$$-\overline{\omega_k} = \frac{-\overline{\omega}-k}{5} = \frac{\omega-5p-k}{5} = \frac{\omega-k}{5} - p = \omega_{-k} - p.$$

The definition of the eta function

$$\eta(\tau) = e^{2\pi i\tau/24}\prod_{n=1}^{\infty}(1-e^{2\pi i\tau n})$$

implies

$$\begin{aligned}\eta(\tau+1) &= \zeta_{24}\eta(\tau),\\ \overline{\eta(\tau)} &= \eta(-\overline{\tau}).\end{aligned}$$

Therefore

$$\overline{\eta(\omega_k)} = \eta(-\overline{\omega_k}) = \eta(\omega_{-k}-p) = \zeta_{24}^{-p}\eta(\omega_{-k}).$$

Next we have

$$\begin{aligned}2\pi i\omega_0 &= \pi ip - 5^{-1}\pi p^{1/2},\\ 2\pi i\omega_\infty &= \pi i25p - 5\pi p^{1/2},\end{aligned}$$

implying that

$$\begin{aligned}1-e^{2\pi i\omega_0 n} &= 1-(-1)^n e^{-5^{-1}\pi p^{1/2}n} > 0,\\ 1-e^{2\pi i\omega_\infty n} &= 1-(-1)^n e^{-5\pi p^{1/2}n} > 0.\end{aligned}$$

In the case of $p \equiv 3 \pmod 5$ the right hand side of our formula (4.10) is therefore

$$e^{(2\pi i/24)(\omega_0+\omega_1+\omega_{-1}-\omega_\infty-\omega_2-\omega_{-2})}\frac{\prod_{n=1}^{\infty}(1-e^{2\pi i\omega_0 n})}{\prod_{n=1}^{\infty}(1-e^{2\pi i\omega_\infty n})}\frac{|\eta(\omega_1)|^2}{|\eta(\omega_2)|^2}.$$

The argument of the exponential factor is equal to

$$\begin{aligned}\frac{2\pi i}{24}(\omega_0-\omega_\infty) &= \frac{2\pi i}{24}\left(\frac{\omega}{5}-5\omega\right)\\ &= -\frac{2\pi i\omega}{5} = -\frac{2\pi i}{5}\left(\frac{5p+\sqrt{-p}}{2}\right) = -\pi ip + 5^{-1}\pi p^{1/2}.\end{aligned}$$

Hence the exponential factor is negative, meaning that we are done with absolute values. In the case of $p \equiv 2 \pmod 5$ the proof is identical.

4.4 Modular functions of level 5

Following Siegel we now define two modular functions by

$$\varphi(\tau) = -5^{-1/2}\frac{\eta(\tau_0)\eta(\tau_1)\eta(\tau_{-1})}{\eta(\tau_\infty)\eta(\tau_2)\eta(\tau_{-2})}, \qquad \psi(\tau) = -5^{-1/2}\frac{\eta(\tau_0)\eta(\tau_2)\eta(\tau_{-2})}{\eta(\tau_\infty)\eta(\tau_1)\eta(\tau_{-1})},$$

where, as before,

$$\tau_k = \alpha_5\tau = \frac{\tau+k}{5}, \qquad \tau_\infty = \alpha_\infty\tau = 5\tau.$$

In the previous section we have proved the following theorem.

Theorem 4.4.1. *Let $K = \mathbb{Q}(\sqrt{-p})$ be an imaginary quadratic field with class number 1, $p > 3$ being a prime such that $p \equiv 3 \pmod 4$. Let $\mathcal{O}_K = [\omega, 1]$, where $\omega = \frac{5p+\sqrt{-p}}{2}$, and let $\varepsilon = \varepsilon_5 = \frac{1+\sqrt{5}}{2}$. Then*

$$\varepsilon^{m_p} = \begin{cases} \psi(\omega) & \text{if } p \equiv 2 \pmod 5, \\ \varphi(\omega) & \text{if } p \equiv 3 \pmod 5, \end{cases}$$

where m_p is a positive integer depending on p.

According to Siegel, the functions φ and ψ are modular of level 5. He writes *"Es ist auch leicht festzustellen, daß die Funktionen [φ, ψ] bei der Kongruenzgruppe fünfter Stufe sämtlich invariant sind[.]"*. However, we will not use this fact in this section.

Now we will investigate the behaviour of the functions φ and ψ under the transformation by the generators of the modular group

$$T = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}, \qquad S = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}.$$

We will again use the notation

$$\alpha_k = \begin{pmatrix} 1 & k \\ & 5 \end{pmatrix}, \qquad \alpha_\infty = \begin{pmatrix} 5 & \\ & 1 \end{pmatrix}.$$

It is easily computed that

$$\begin{aligned}
&\alpha_k T = \alpha_{k+1}, \qquad T\alpha_k = \alpha_{k+5}, \qquad \alpha_\infty T = T^5\alpha_\infty, \\
&\alpha_0 S = S\alpha_\infty, \qquad S\alpha_0 = \alpha_\infty S, \\
&\alpha_1 S = -ST^5S\alpha_{-1}, \qquad \alpha_{-1}S = ST^{-5}S\alpha_1, \\
&\alpha_2 S = -ST^2ST^{-2}S\alpha_2, \qquad \alpha_{-2}S = -ST^{-2}ST^2S\alpha_{-2}, \\
&-ST^5S = \begin{pmatrix} 1 & \\ 5 & 1 \end{pmatrix}, \qquad ST^{-5}S = \begin{pmatrix} -1 & \\ 5 & -1 \end{pmatrix}, \\
&-ST^2ST^{-2}S = \begin{pmatrix} -2 & -1 \\ 5 & 2 \end{pmatrix}, \qquad -ST^{-2}ST^2S = \begin{pmatrix} 2 & -1 \\ 5 & -2 \end{pmatrix}.
\end{aligned}$$

Using these relations we further compute that

$$\begin{aligned}
-\sqrt{5}\varphi\circ T &= \frac{\eta(\alpha_{-1}T\tau)\eta(\alpha_1T\tau)\eta(\alpha_0T\tau)}{\eta(\alpha_{-2}T\tau)\eta(\alpha_2T\tau)\eta(\alpha_\infty T\tau)} = \frac{\eta(\alpha_{-2}\tau)\eta(\alpha_0\tau)\eta(\alpha_{-1}\tau)}{\eta(T\alpha_2\tau)\eta(\alpha_1\tau)\eta(T^5\alpha_\infty\tau)} \\
&= \zeta_{24}^{-6}\frac{\eta(\alpha_{-2}\tau)\eta(\alpha_0\tau)\eta(\alpha_{-1}\tau)}{\eta(\alpha_2\tau)\eta(\alpha_1\tau)\eta(\alpha_\infty\tau)},
\end{aligned}$$

and similarly

$$\begin{aligned}
-\sqrt{5}\phi \circ T^2 &= \zeta_{24}^{-10}\frac{\eta(\alpha_2\tau)\eta(\alpha_{-1}\tau)\eta(\alpha_{-2}\tau)}{\eta(\alpha_1\tau)\eta(\alpha_0\tau)\eta(\alpha_\infty\tau)},\\
-\sqrt{5}\phi \circ T^3 &= \zeta_{24}^{10}\frac{\eta(\alpha_2\tau)\eta(\alpha_1\tau)\eta(\alpha_{-2}\tau)}{\eta(\alpha_{-1}\tau)\eta(\alpha_0\tau)\eta(\alpha_\infty\tau)},\\
-\sqrt{5}\phi \circ T^4 &= \zeta_{24}^{6}\frac{\eta(\alpha_0\tau)\eta(\alpha_2\tau)\eta(\alpha_1\tau)}{\eta(\alpha_{-1}\tau)\eta(\alpha_{-2}\tau)\eta(\alpha_\infty\tau)},\\
\varphi \circ T^5 &= \varphi.
\end{aligned}$$

The transformation by S is pain in the neck, due to the transformation formula $\eta(S\tau) = \sqrt{-i\tau}\,\eta(\tau)$. We compute that

$$\begin{aligned}
\eta(\alpha_{-1}S\tau) &= \eta(ST^{-5}S\alpha_1\tau) = \sqrt{-iT^{-5}S\alpha_1\tau}\cdot\eta(T^{-5}S\alpha_1\tau)\\
&= \zeta_{24}^{-5}\sqrt{-iT^{-5}S\alpha_1\tau}\cdot\eta(S\alpha_1\tau) = \zeta_{24}^{-5}\sqrt{-iT^{-5}S\alpha_1\tau}\sqrt{-i\alpha_1\tau}\cdot\eta(\alpha_1\tau)\\
&= \zeta_{24}^{-5}\sqrt{i\frac{5\tau}{-\tau+1}}\sqrt{i\frac{\tau-1}{5}}\eta(\alpha_1\tau) = \zeta_{24}^{-5}\sqrt{\tau}\cdot\eta(\alpha_1\tau),\\
\eta(\alpha_1S\tau) &= \zeta_{24}^{5}\frac{1}{\sqrt{S\tau}}\cdot\eta(\alpha_{-1}S^2\tau) = \zeta_{24}^{5}\frac{1}{\sqrt{\frac{-1}{\tau}}}\cdot\eta(\alpha_{-1}\tau) = \zeta_{24}^{5}\frac{\sqrt{\tau}}{\sqrt{-1}}\cdot\eta(\alpha_{-1}\tau)\\
&= \zeta_{24}^{-1}\sqrt{\tau}\cdot\eta(\alpha_{-1}\tau),\\
\eta(\alpha_0S\tau) &= \eta(S\alpha_\infty\tau) = \sqrt{-i\alpha_\infty\tau}\cdot\eta(\alpha_\infty\tau) = \sqrt{-i5\tau}\cdot\eta(\alpha_\infty\tau)\\
&= \sqrt{-i}\sqrt{5\tau}\cdot\eta(\alpha_\infty\tau) = \sqrt{-i}\sqrt{5\tau}\cdot\eta(\alpha_\infty\tau) = \zeta_{24}^{-3}\sqrt{5\tau}\cdot\eta(\alpha_\infty\tau),\\
\eta(\alpha_\infty S\tau) &= \zeta_{24}^{3}\frac{1}{\sqrt{5S\tau}}\eta(\alpha_0S^2\tau) = \zeta_{24}^{3}\frac{1}{\sqrt{\frac{-5}{\tau}}}\eta(\alpha_0\tau)\\
&= \zeta_{24}^{3}\frac{1}{\sqrt{-1}}\sqrt{\frac{\tau}{5}}\cdot\eta(\alpha_0\tau) = \zeta_{24}^{-3}\sqrt{\frac{\tau}{5}}\cdot\eta(\alpha_0\tau),
\end{aligned}$$

and

$$\begin{aligned}
\eta(\alpha_2S\tau) &= \eta(ST^2ST^{-2}S\alpha_2\tau) = \zeta_{24}^{2}\sqrt{-iT^2ST^{-2}S\alpha_2\tau}\cdot\eta(ST^{-2}S\alpha_2\tau)\\
&= \sqrt{-iT^2ST^{-2}S\alpha_2\tau}\sqrt{-iT^{-2}S\alpha_2\tau}\cdot\eta(S\alpha_2\tau)\\
&= \sqrt{-iT^2ST^{-2}S\alpha_2\tau}\sqrt{-iT^{-2}S\alpha_2\tau}\sqrt{-i\alpha_2\tau}\cdot\eta(\alpha_2\tau)\\
&= \sqrt{-i\frac{5\tau}{2\tau+1}}\sqrt{-i\frac{2\tau+1}{-\tau+2}}\sqrt{-i\frac{\tau-2}{5}}\cdot\eta(\alpha_2\tau)\\
&= \sqrt{-i}\sqrt{\tau}\cdot\eta(\alpha_2\tau) = \zeta_{24}^{-3}\sqrt{\tau}\cdot\eta(\alpha_2\tau),\\
\eta(\alpha_{-2}S\tau) &= \eta(ST^{-2}ST^2S\alpha_{-2}\tau) = \zeta_{24}^{-2}\sqrt{-iT^{-2}ST^2S\alpha_{-2}\tau}\cdot\eta(ST^2S\alpha_{-2}\tau)\\
&= \sqrt{-iT^{-2}ST^2S\alpha_{-2}\tau}\sqrt{-iT^2S\alpha_{-2}\tau}\cdot\eta(S\alpha_{-2}\tau)\\
&= \sqrt{-iT^{-2}ST^2S\alpha_{-2}\tau}\sqrt{-iT^2S\alpha_{-2}\tau}\sqrt{-i\alpha_{-2}\tau}\cdot\eta(\alpha_{-2}\tau)\\
&= \sqrt{-i\frac{5\tau}{-2\tau+1}}\sqrt{-i\frac{2\tau-1}{\tau+2}}\sqrt{-i\frac{\tau+2}{5}}\cdot\eta(\alpha_{-2}\tau)\\
&= \sqrt{-i}\sqrt{\tau}\cdot\eta(\alpha_{-2}\tau) = \zeta_{24}^{-3}\sqrt{\tau}\cdot\eta(\alpha_{-2}\tau).
\end{aligned}$$

We now use the formulas just obtained to determine how the function φ transforms under transformations of the form ST^k.

$$\begin{aligned}
-\sqrt{5}\varphi(\tau) &= \frac{\eta(\alpha_{-1}\tau)\eta(\alpha_1\tau)\eta(\alpha_0\tau)}{\eta(\alpha_{-2}\tau)\eta(\alpha_2\tau)\eta(\alpha_\infty\tau)},\\
-\sqrt{5}\varphi(S\tau) &= \frac{\eta(\alpha_{-1}S\tau)\eta(\alpha_1S\tau)\eta(\alpha_0S\tau)}{\eta(\alpha_{-2}S\tau)\eta(\alpha_2S\tau)\eta(\alpha_\infty S\tau)}\\
&= \frac{\zeta_{24}^{-5}\sqrt{\tau}\cdot\eta(\alpha_1\tau)\zeta_{24}^{-1}\sqrt{\tau}\cdot\eta(\alpha_{-1}\tau)\zeta_{24}^{-3}\sqrt{5\tau}\cdot\eta(\alpha_\infty\tau)}{\zeta_{24}^{-3}\sqrt{\tau}\cdot\eta(\alpha_{-2}\tau)\zeta_{24}^{-3}\sqrt{\tau}\cdot\eta(\alpha_2\tau)\zeta_{24}^{-3}\sqrt{\tau/5}\cdot\eta(\alpha_0\tau)}\\
&= \frac{\eta(\alpha_1\tau)\eta(\alpha_{-1}\tau)\eta(\alpha_\infty\tau)}{\eta(\alpha_{-2}\tau)\eta(\alpha_2\tau)\eta(\alpha_0\tau)},\\
-\sqrt{5}\varphi(ST\tau) &= \frac{\eta(\alpha_1T\tau)\eta(\alpha_{-1}T\tau)\eta(\alpha_\infty T\tau)}{\eta(\alpha_{-2}T\tau)\eta(\alpha_2T\tau)\eta(\alpha_0T\tau)}\\
&= \frac{\eta(\alpha_0\tau)\eta(\alpha_{-2}\tau)\eta(T^5\alpha_\infty\tau)}{\eta(T\alpha_2\tau)\eta(\alpha_1\tau)\eta(\alpha_{-1}\tau)}\\
&= \zeta_{24}^{4}\frac{\eta(\alpha_0\tau)\eta(\alpha_{-2}\tau)\eta(\alpha_\infty\tau)}{\eta(\alpha_2\tau)\eta(\alpha_1\tau)\eta(\alpha_{-1}\tau)},\\
-\sqrt{5}\varphi(ST^2\tau) &= \zeta_{24}^{4}\frac{\eta(\alpha_0T\tau)\eta(\alpha_{-2}T\tau)\eta(\alpha_\infty T\tau)}{\eta(\alpha_2T\tau)\eta(\alpha_1T\tau)\eta(\alpha_{-1}T\tau)}\\
&= \zeta_{24}^{4}\frac{\eta(\alpha_{-1}\tau)\eta(T\alpha_2\tau)\eta(T^5\alpha_\infty\tau)}{\eta(\alpha_1\tau)\eta(\alpha_0\tau)\eta(\alpha_{-2}\tau)}\\
&= \zeta_{24}^{10}\frac{\eta(\alpha_{-1}\tau)\eta(\alpha_2\tau)\eta(\alpha_\infty\tau)}{\eta(\alpha_1\tau)\eta(\alpha_0\tau)\eta(\alpha_{-2}\tau)},
\end{aligned}$$

$$\begin{aligned}
-\sqrt{5}\varphi(ST^3\tau) &= \zeta_{24}^{10}\frac{\eta(\alpha_{-1}T\tau)\eta(\alpha_2T\tau)\eta(\alpha_\infty T\tau)}{\eta(\alpha_1T\tau)\eta(\alpha_0T\tau)\eta(\alpha_{-2}T\tau)}\\
&= \zeta_{24}^{10}\frac{\eta(\alpha_{-2}\tau)\eta(\alpha_1\tau)\eta(T^5\alpha_\infty\tau)}{\eta(\alpha_0\tau)\eta(\alpha_{-1}\tau)\eta(T\alpha_2\tau)}\\
&= \zeta_{24}^{-10}\frac{\eta(\alpha_{-2}\tau)\eta(\alpha_1\tau)\eta(\alpha_\infty\tau)}{\eta(\alpha_0\tau)\eta(\alpha_{-1}\tau)\eta(\alpha_2\tau)},\\
-\sqrt{5}\varphi(ST^4\tau) &= \zeta_{24}^{-10}\frac{\eta(\alpha_{-2}T\tau)\eta(\alpha_1T\tau)\eta(\alpha_\infty T\tau)}{\eta(\alpha_0T\tau)\eta(\alpha_{-1}T\tau)\eta(\alpha_2T\tau)}\\
&= \zeta_{24}^{-10}\frac{\eta(T\alpha_2\tau)\eta(\alpha_0\tau)\eta(T^5\alpha_\infty\tau)}{\eta(\alpha_{-1}\tau)\eta(\alpha_{-2}\tau)\eta(\alpha_1\tau)}\\
&= \zeta_{24}^{-4}\frac{\eta(\alpha_2\tau)\eta(\alpha_0\tau)\eta(\alpha_\infty\tau)}{\eta(\alpha_{-1}\tau)\eta(\alpha_{-2}\tau)\eta(\alpha_1\tau)}.
\end{aligned}$$

We now define 10 functions as follows. For $0 \le k \le 4$ set

$$\begin{aligned}
\varphi_k(\tau) &= \varphi(T^k\tau),\\
\varphi_{k+4}(\tau) &= \varphi(ST^4\tau).
\end{aligned}$$

The calculations above and some little more work show how the matrices T and S act on the functions $\varphi = \varphi_0, \ldots, \varphi_9$. We have recorded the corresponding permutations of these functions in the following table.

	φ_0	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6	φ_7	φ_8	φ_9
S	φ_5	φ_8	φ_3	φ_2	φ_7	φ_0	φ_6	φ_4	φ_1	φ_9
T	φ_1	φ_2	φ_3	φ_4	φ_0	φ_6	φ_7	φ_8	φ_9	φ_5

Next step is to determine the values $\varphi_k(\zeta_3)$ for $0 \le k \le 9$. Note that

$$\begin{aligned} \zeta_3 = \zeta_{24}^8 &= \frac{-1+\sqrt{-3}}{2}, \\ ST\zeta_3 &= \zeta_3, \\ T\zeta_3 = \zeta_3 + 1 &= -\zeta_3^2 = \zeta_{24}^{12+16} = \zeta_{24}^4. \end{aligned}$$

We substitute $\tau = T\zeta_3$ into the following formulas which were obtained earlier,

$$\begin{aligned} \eta(\alpha_{-1}S\tau) &= \zeta_{24}^{-5}\sqrt{\tau}\cdot\eta(\alpha_1\tau), & \eta(\alpha_1 S\tau) &= \zeta_{24}^{-1}\sqrt{\tau}\cdot\eta(\alpha_{-1}\tau), \\ \eta(\alpha_0 S\tau) &= \zeta_{24}^{-3}\sqrt{5\tau}\cdot\eta(\alpha_\infty\tau), & \eta(\alpha_\infty S\tau) &= \zeta_{24}^{-3}\sqrt{\frac{\tau}{5}}\cdot\eta(\alpha_0\tau), \\ \eta(\alpha_2 S\tau) &= \zeta_{24}^{-3}\sqrt{\tau}\cdot\eta(\alpha_2\tau), & \eta(\alpha_{-2}S\tau) &= \zeta_{24}^{-3}\sqrt{\tau}\cdot\eta(\alpha_{-2}\tau), \end{aligned}$$

obtaining

$$\begin{aligned} \eta(\alpha_{-1}\zeta_3) &= \zeta_{24}^{-5}\sqrt{\zeta_{24}^4}\cdot\eta(\alpha_1 T\zeta_3) = \zeta_{24}^{-3}\eta(\alpha_1 T\zeta_3) = \zeta_{24}^{-3}\eta(\alpha_0\zeta_3), \\ \eta(\alpha_1\zeta_3) &= \zeta_{24}^{-1}\sqrt{\zeta_{24}^4}\cdot\eta(\alpha_{-1}T\zeta_3) = \zeta_{24}\eta(\alpha_{-1}T\zeta_3) = \zeta_{24}\eta(\alpha_{-2}\zeta_3), \\ \eta(\alpha_0\zeta_3) &= \zeta_{24}^{-3}\sqrt{5\zeta_{24}^4}\cdot\eta(\alpha_\infty T\zeta_3) = \zeta_{24}^{-1}\sqrt{5}\cdot\eta(\alpha_\infty T\zeta_3) = \zeta_{24}^4\sqrt{5}\cdot\eta(\alpha_\infty\zeta_3), \\ \eta(\alpha_\infty\zeta_3) &= \zeta_{24}^{-3}\sqrt{\frac{\zeta_{24}^4}{5}}\cdot\eta(\alpha_0 T\zeta_3) = \zeta_{24}^{-1}\frac{1}{\sqrt{5}}\cdot\eta(\alpha_0 T\zeta_3) = \zeta_{24}^{-1}\frac{1}{\sqrt{5}}\cdot\eta(\alpha_{-1}\zeta_3), \\ \eta(\alpha_2\zeta_3) &= \zeta_{24}^{-3}\sqrt{\zeta_{24}^4}\cdot\eta(\alpha_2 T\zeta_3) = \zeta_{24}^{-1}\eta(\alpha_2 T\zeta_3) = \zeta_{24}^{-1}\eta(\alpha_1\zeta_3), \\ \eta(\alpha_{-2}\zeta_3) &= \zeta_{24}^{-3}\sqrt{\zeta_{24}^4}\cdot\eta(\alpha_{-2}T\zeta_3) = \zeta_{24}^{-1}\eta(\alpha_{-2}T\zeta_3) = \eta(\alpha_2\zeta_3). \end{aligned}$$

Following Siegel we now set

$$\eta(\alpha_0\zeta_3) = \zeta_{24}^2 a, \qquad \eta(\alpha_{-2}\zeta_3) = b, \qquad ba^{-1} = c,$$

so that

$$\begin{aligned} \eta(\alpha_1\zeta_3) &= \zeta_{24}b, & \eta(\alpha_2\zeta_3) &= b, \\ \eta(\alpha_{-1}\zeta_3) &= \zeta_{24}^{-1}a, & \eta(\alpha_\infty\zeta_3) &= \zeta_{24}^{-2}5^{-1/2}a. \end{aligned}$$

We are now able to compute the values $\varphi(\zeta_3)$ in terms of c. For example

$$\begin{aligned} \varphi_0(\zeta_3) &= -\frac{1}{\sqrt{5}}\frac{\eta(\alpha_{-1}\zeta_3)\eta(\alpha_1\zeta_3)\eta(\alpha_0\zeta_3)}{\eta(\alpha_{-2}\zeta_3)\eta(\alpha_2\zeta_3)\eta(\alpha_\infty\zeta_3)} \\ &= -\frac{1}{\sqrt{5}}\frac{\zeta_{24}^{-1}a\zeta_{24}b\zeta_{24}^2 a}{b^2\zeta_{24}^{-2}5^{-1/2}a} = -\zeta_{24}^4 c^{-1} = \zeta_3^{-1}c^{-1}, \\ \varphi_1(\zeta_3) &= -\frac{1}{\sqrt{5}}\zeta_{24}^{-6}\frac{\eta(\alpha_{-2}\zeta_3)\eta(\alpha_0\zeta_3)\eta(\alpha_{-1}\zeta_3)}{\eta(\alpha_2\zeta_3)\eta(\alpha_1\zeta_3)\eta(\alpha_\infty\zeta_3)} \\ &= -\frac{1}{\sqrt{5}}\zeta_{24}^{-6}\frac{b\zeta_{24}^2 a\zeta_{24}^{-1}a}{b\zeta_{24}b\zeta_{24}^{-2}5^{-1/2}a} = \zeta_3 c^{-1}. \end{aligned}$$

The remaining values are calculated in similar way. We record them in the following table.

$\phi_0(\zeta_3)$	$\phi_1(\zeta_3)$	$\phi_2(\zeta_3)$	$\phi_3(\zeta_3)$	$\phi_4(\zeta_3)$
$\zeta_3^{-1}c^{-1}$	$\zeta_3 c^{-1}$	c	c^3	c

$\phi_5(\zeta_3)$	$\phi_6(\zeta_3)$	$\phi_7(\zeta_3)$	$\phi_8(\zeta_3)$	$\phi_9(\zeta_3)$
$\zeta_3 c^{-1}$	$\zeta_3^{-1}c^{-1}$	$\zeta_3^{-1}c^{-1}$	c	$\zeta_3 c^{-1}$

To calculate the value of c we use the case of $p = 3$. For $p = 3$ we have

$$\omega = \frac{15 + \sqrt{-3}}{2} = \zeta_3 + 8.$$

We would now like use Theorem 4.2.7 or Theorem 4.4.1, but these theorems are not quite true when $p = 3$ due to additional units. However, the formula of Theorem 4.1.11 remains valid. According to Theorem 4.2.1 there are 2 ideal classes, so there will be one eta-factor in the numerator and one in the denominator. After taking the third powers and a little calculation, we get our function on the right hand side, that is, $\varepsilon^{3m_3} = \varphi(\omega)$. We therefore have

$$\varepsilon^{3m_3} = \varphi(\omega) = \varphi_0(\zeta_3 + 8) = \varphi_0(\zeta_3 + 3) = \varphi_3(\zeta_3) = c^3.$$

Next $h_{-15} = 2m_{-3}$ and $h_{-15} = 2$, so $\varepsilon^3 = c^3$. To prove that $\varepsilon = c$, it suffices to prove that c is real. We have

$$\varphi_8(\zeta_3) = \sqrt{5}\zeta_{24}^2 \frac{\eta(\alpha_\infty\zeta_3)\eta(\alpha_{-2}\zeta_3)\eta(\alpha_1\zeta_3)}{\eta(\alpha_2\zeta_3)\eta(\alpha_0\zeta_3)\eta(\alpha_{-1}\zeta_3)},$$

and similarly as in Section 4.3 we compute

$$\begin{aligned}
\overline{\eta\left(\frac{\zeta_3}{5}\right)} &= \eta\left(-\frac{\overline{\zeta_3}}{5}\right) = \eta\left(-\frac{\zeta_3^2}{5}\right) = \eta\left(\frac{\zeta_3+1}{5}\right) \\
\overline{\eta\left(\frac{\zeta_3+2}{5}\right)} &= \eta\left(-\frac{\overline{\zeta_3+2}}{5}\right) = \eta\left(-\frac{-\zeta_3-1+2}{5}\right) = \eta\left(\frac{\zeta_3-1}{5}\right) \\
\alpha_2\zeta_3 &= \frac{\zeta_3-2}{5} = -\frac{1}{2} + i\frac{\sqrt{3}}{10} \\
\alpha_\infty\zeta_3 &= 5\zeta_3 = -\frac{5}{2} + i\frac{5\sqrt{3}}{2} \\
\frac{\eta(\alpha_\infty\zeta_3)}{\eta(\alpha_2\zeta_3)} &= e^{\frac{2\pi i}{24}\left(-2+i\frac{24\sqrt{3}}{10}\right)} \frac{\prod_{n=1}^\infty (1-(-1)^n e^{-\pi\sqrt{3}n/5})}{\prod_{n=1}^\infty (1-(-1)^n e^{-\pi 5\sqrt{3}n})} \\
\zeta_{24}^2 \frac{\eta(\alpha_\infty\zeta_3)}{\eta(\alpha_2\zeta_3)} &= e^{-2\pi\frac{\sqrt{3}}{10}} \frac{\prod_{n=1}^\infty (1-(-1)^n e^{-\pi\sqrt{3}n/5})}{\prod_{n=1}^\infty (1-(-1)^n e^{-\pi 5\sqrt{3}n})}
\end{aligned}$$

Therefore the number $\varphi_8(\zeta_3) = c$ is real, and so $c = \varepsilon$. We have thus determined all values of $\varphi_k(\tau)$ for $0 \le k \le 9$, and we obtain the following theorem.

Theorem 4.4.2.

$$\prod_{k=0}^{9} (X - \varphi_k(\zeta_3)) = (X - \varepsilon^3)\left((X-\varepsilon)(X^2 + \varepsilon^{-1}X + \varepsilon^{-2})\right)^3.$$

Theorem 4.4.3. *The functions $\varphi(\tau)$, $\psi(\tau)$, and $j(\tau)$ satisfy the following relations.*

$$(\varphi(\tau)-\varepsilon^3)\left((\varphi(\tau)-\varepsilon)(\varphi(\tau)^2+\varepsilon^{-1}\varphi(\tau)+\varepsilon^{-2})\right)^3+5^{-5/2}j(\tau)\varphi(\tau)^5=0,$$

$$(\psi(\tau)-\varepsilon^{-3})\left((\psi(\tau)-\varepsilon^{-1})(\psi(\tau)^2+\varepsilon\psi(\tau)+\varepsilon^2)\right)^3+5^{-5/2}j(\tau)\psi(\tau)^5=0.$$

Proof. Consider the polynomial

$$\prod_{k=0}^{9}(X-\varphi_k(\tau))=X^{10}-\Phi_1(\tau)X^9+\cdots+\Phi_{10}(\tau).$$

The functions $\Phi_i(\tau)$, being the elementary symmetric polynomials in $\varphi_k(\tau)$, are modular functions of level 1 holomorphic on $\mathfrak{H}$. In particular, the functions $\Phi_i(\tau)$ have Fourier expansions of the form

$$\Phi_i(\tau)=\sum_{n=-N}^{\infty}a_n^{(i)}q^n. \tag{4.11}$$

On the other hand, from the definition of $\varphi_k(\tau)$ we see that

$$\varphi_k(\tau)=-5^{1/2}\zeta_{24}^{v_k}e^{\frac{2\pi i}{24}\left(\sum_{r=-2}^{2}d_r^{(k)}\frac{\tau-r}{5}+d_\infty^{(k)}5\tau\right)}(1+\textstyle\sum_{n=1}^{\infty}c_n^{(k)}q^{n/5}),$$

where $c_n^{(k)}\in\mathbb{Q}(\zeta_5)$, $v_k\in\{0,\pm4,\pm6,\pm10\}$. The numbers $d_r^{(k)},d_\infty^{(k)}\in\{\pm1\}$ indicate if the corresponding factor $\eta(\alpha_r\tau)$, or $\eta(\alpha_\infty\tau)$, is in the numerator or in the denominator of the defining product for $\varphi_k(\tau)$. Next we have

$$\begin{aligned}\sum_{r=-2}^{2}d_r^{(k)}\frac{\tau-r}{5}+d_\infty^{(k)}5\tau&=-\frac{1}{5}\sum_{r=-2}^{2}rd_r^{(k)}+\left(\frac{1}{5}\sum_{r=-2}^{2}d_r^{(k)}+5d_\infty^{(k)}\right)\tau\\&=\begin{cases}d_k+\left(\frac{1}{5}-5\right)\tau=d_k-\frac{24}{5}\tau & \text{if } 0\le k\le 4,\\ d_k+\left(-\frac{1}{5}+5\right)\tau=d_k+\frac{24}{5}\tau & \text{if } 5\le k\le 9,\end{cases}\end{aligned}$$

where d_k is a constant. This is because if $0\le k\le 4$ then the factor $\eta(\alpha_\infty\tau)$ is in the denominator and there are three factors of the type $\eta(\alpha_r\tau)$ in the numerator, and two in the denominator. Similarly if $5\le k\le 9$ then $\eta(\alpha_\infty\tau)$ is in the numerator, and there are two remaining factors in the numerator, and three in the denominator. Therefore we have

$$\phi_k(\tau)=-5^{1/2}\zeta_{24}^{v_k+d_k}q^{\mp1/5}(1+\textstyle\sum_{n=1}^{\infty}c_n^{(k)}q^{n/5}), \tag{4.12}$$

according to whether $0\le k\le 4$ or $5\le k\le 9$. We claim that $\Phi_i(\tau)$ is a constant function if $i\ne5$. To prove this, write

$$\begin{aligned}\Phi_i(\tau)&=\sum_{k_0,\dots,k_{i-1}}\phi_{k_0}(\tau)\cdots\phi_{k_{i-1}}(\tau)\\&=\sum_{k_0,\dots,k_{i-1}}c_{k_0,\dots,k_{i-1}}q^{(a_{k_0}+a_{k_1}+\cdots+a_{k_{i-1}})/5}+O(1)\\&=\sum_m\left(\sum_{a_{k_0}+a_{k_1}+\cdots+a_{k_{i-1}}=m}c_{k_0,\dots,k_{i-1}}\right)q^{m/5}+O(1)\end{aligned}$$

where $c_{k_0,\dots,k_{i-1}} \in \mathbb{C}$, and by (4.12), $a_{k_j} \in \{\pm 1\}$. Consider the term in the sum above with minimal $m = M$. If M were nonnegative, then $\Phi_i(\tau)$ would be holomorphic at infinity and consequently constant. Therefore we may assume that $M < 0$. Since the Fourier expansion is uniquely determined, (4.11) shows that M is divisible by 5. Since $1 \le i \le 10$ and $a_{k_j} \in \{\pm 1\}$, we have $M \in \{-5, -10\}$. If $M = -10$, then $i = 10$, and $a_{k_j} = -1$ for all $1 \le j \le 10$, which is impossible, because $a_{k_j} = 1$ for 5 values of j. We must therefore have $M = -5$. This means that among the a_{k_j}, the value -1 must occur at least 5 times. But there cannot be more than 5 terms in the sum for M, because any other term would make the sum greater than -5. Therefore $M < 0$ only for $i = 5$. We have therefore

$$\begin{aligned}\Phi_5(\tau) &= \prod_{k=0}^{4} \varphi_k(\tau) + O(1) = \prod_{k=0}^{4} \left(-5^{-1/2}\zeta_{24}^{v_k+d_k} q^{-1/5} + O(1)\right) + O(1) \\ &= -5^{-5/2}\zeta_{24}^{\sum_{k=0}^{4} v_k+d_k} q^{-1} + O(1).\end{aligned}$$

The exponent of ζ_{24} is easily calculated to be

$$\sum_{k=0}^{4} v_k + d_k = (0 - 6 - 10 + 10 + 6) + \left(0 - \frac{6}{5} - \frac{2}{5} + \frac{2}{5} + \frac{6}{5}\right) = 0.$$

Therefore

$$\begin{aligned}\Phi_5(\tau) &= -5^{-5/2}q^{-1} + O(1), \\ 5^{5/2}\Phi_5(\tau) + j(\tau) &= O(1).\end{aligned}$$

Hence the function $5^{5/2}\Phi_5(\tau) + j(\tau)$ is constant, let us say C. Then $-\Phi_5(\tau) = 5^{-5/2}C + 5^{-5/2}j(\tau)$. We can now write

$$\prod_{k=0}^{9} (X - \varphi_k(\tau)) = P(X) + 5^{-5/2}j(\tau)X^5,$$

where $P \in \mathbb{C}[X]$. Setting $\tau = \zeta_3$, we obtain

$$\prod_{k=0}^{9} (X - \varphi_k(\zeta_3)) = P(X) + 5^{-5/2}j(\zeta_3)X^5.$$

But $j(\zeta_3) = 0$ and we already know the left-hand side. Consequently

$$P(X) = \prod_{k=0}^{9} (X - \varphi_k(\zeta_3)) = (X - \varepsilon^3)\left((X - \varepsilon)(X^2 + \varepsilon^{-1}X + \varepsilon^{-2})\right)^3.$$

It follows that

$$\prod_{k=0}^{9} (X - \varphi_k(\tau)) = (X - \varepsilon^3)\left((X - \varepsilon)(X^2 + \varepsilon^{-1}X + \varepsilon^{-2})\right)^3 + 5^{-5/2}j(\tau)X^5.$$

We now substitute $X = \varphi(\tau) = \varphi_0(\tau)$ to find that

$$0 = (\varphi(\tau) - \varepsilon^3)\left((\varphi(\tau) - \varepsilon)(\varphi(\tau)^2 + \varepsilon^{-1}\varphi(\tau) + \varepsilon^{-2})\right)^3 + 5^{-5/2}j(\tau)\varphi(\tau)^5.$$

This is the first desired relation. We claim that the functions

$$\varphi(\tau) = -\frac{1}{\sqrt{5}}\frac{\eta(\alpha_{-1}\tau)\eta(\alpha_1\tau)\eta(\alpha_0\tau)}{\eta(\alpha_{-2}\tau)\eta(\alpha_2\tau)\eta(\alpha_\infty\tau)}, \quad \psi(\tau) = -\frac{1}{\sqrt{5}}\frac{\eta(\alpha_0\tau)\eta(\alpha_2\tau)\eta(\alpha_{-2}\tau)}{\eta(\alpha_\infty\tau)\eta(\alpha_1\tau)\eta(\alpha_{-1}\tau)}$$

have Fourier coefficients in $\mathbb{Q}(\sqrt{5})$. We have

$$\begin{aligned}\varphi(\tau) &= -\frac{1}{\sqrt{5}}q^{-1/5}\prod_{n=1}^{\infty}\frac{(1-\zeta_5^n q^{n/5})(1-\zeta_5^{-n}q^{n/5})(1-q^{n/5})}{(1-\zeta_5^{2n}q^{n/5})(1-\zeta_5^{-2n}q^{n/5})(1-q^{5n})}\\ &= -\frac{1}{\sqrt{5}}q^{-1/5}\prod_{n=1}^{\infty}\frac{(1-(\zeta_5^n+\zeta_5^{-n})q^{n/5}+q^{2n/5})(1-q^{n/5})}{(1-(\zeta_5^{2n}+\zeta_5^{-2n})q^{n/5}+q^{2n/5})(1-q^{5n})}.\end{aligned}$$

Write $(X-\zeta_5)(X-\zeta_5^4) = X^2+-X+1$ and $(X-\zeta_5^2)(X-\zeta_5^3) = X^2-bX+1$. Then

$$\begin{aligned}X^4+X^3+X^2+X+1 &= (X^2-aX+1)(X^2-bX+1)\\ &= X^4-(a+b)X^3+(ab+2)X^2-(a+b)X+1.\end{aligned}$$

Comparing coefficients, we see that a and b are roots of Y^2+Y-1, so $\{a,b\} = \{\zeta_5+\zeta_5^4, \zeta_5^2+\zeta_5^3\} = \{\frac{-1\pm\sqrt{5}}{2}\}$. Therefore $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta_5)$, and in fact $\mathbb{Q}(\sqrt{5}) = \mathbb{R}\cap\mathbb{Q}(\zeta_5)$. Because the automorphism σ of $\mathbb{Q}(\zeta_5)$ determined by $\sigma(\zeta_5) = \zeta_5^2$ interchanges a and b, we have $\sigma(\sqrt{5}) = -\sqrt{5}$. The numbers $\zeta_5^n+\zeta_5^{-n}$ and $\zeta_5^{2n}+\zeta_5^{-2n}$ are fixed under complex conjugation, so they are real, and consequently lie in $\mathbb{Q}(\sqrt{5})$. This proves that $\varphi(\tau) \in \mathbb{Q}(\sqrt{5})((q^{1/5}))$. Next we show that $\varphi(\tau)^\sigma = -\psi(\tau)$. We have $\sigma(\zeta_5^n+\zeta_5^{-n}) = \zeta_5^{2n}+\zeta_5^{-2n}$ and $\sigma(\zeta_5^{2n}+\zeta_5^{-2n}) = \zeta_5^n+\zeta_5^{-n}$. Write

$$\begin{aligned}f(\tau) &= \prod_{n=1}^{\infty}(1-(\zeta_5^n+\zeta_5^{-n})q^{n/5}+q^{2n/5}) = \sum_{n=0}^{\infty}c_n q^{n/5},\\ g(\tau) &= \prod_{n=1}^{\infty}(1-(\zeta_5^{2n}+\zeta_5^{-2n})q^{n/5}+q^{2n/5}) = \sum_{n=0}^{\infty}d_n q^{n/5}.\end{aligned}$$

There exists a sequence of polynomials $P_n \in \mathbb{Z}[X_1,\dots,X_n]$ such that

$$\begin{aligned}c_n &= P_n(\zeta_5+\zeta_5^{-1},\dots,\zeta_5^n+\zeta_5^{-n}),\\ d_n &= P_n(\zeta_5^2+\zeta_5^{-2},\dots,\zeta_5^{2n}+\zeta_5^{-2n}),\end{aligned}$$

for all $n \geq 1$. Thus $\sigma(c_n) = d_n$ for all $n \geq 1$. Consequently, $f(\tau)^\sigma = g(\tau)$, which in turn implies that $\varphi(\tau)^\sigma = -\psi(\tau)$. We now apply the automorphism σ on the relation between $\varphi(\tau)$ and $j(\tau)$. Since $\sigma(\varepsilon) = -\varepsilon^{-1}$, $\sigma(\sqrt{5}) = -\sqrt{5}$, and $j(\tau)^\sigma = j(\tau)$, we obtain

$$0 = (-\psi(\tau)+\varepsilon^{-3})\left((-\psi(\tau)+\varepsilon^{-1})(\psi(\tau)^2-\varepsilon\psi(\tau)+\varepsilon^2)\right)^3 - 5^{5/2}j(\tau)(-\psi(\tau))^5.$$

This is the second desired relation. □

4.5 The diophantine equation

Since $h_K = 1$, we have $j(\omega) \in \mathcal{O}_K$ (we know already that $j(\omega)$ is a cube in $\mathbb{Z}$, but we follow Siegel's reasoning). We know that $j(\omega) = -q^3$, where $q \in \mathcal{O}_K$. We also

know that $j(\omega)$ is real, so that $q^3 = \overline{q^3}$. Since K is an imaginary quadratic field, complex conjugation is an automorphism of K, and so $\overline{q} \in \mathcal{O}_K$, meaning that $q/\overline{q} \in K$ is a third root of unity. If $p > 3$, which we will assume from now on, then K does not contain $\sqrt{-3}$, meaning that $q/\overline{q} = 1, q = \overline{q}$. Therefore q is real and therefore a rational integer. The function $j(\tau)$ attains every negative real value exactly once on the border of the fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$. Consequently, to distinct values of p will correspond distinct positive values of q.

Let $m = m_p$. From Theorem 4.4.1 and Theorem 4.4.3 we have

$$\frac{1}{\sqrt{5}}(\varepsilon^m - \varepsilon^{\pm 3})\left(5(\varepsilon^m - \varepsilon^{\pm 1})(\varepsilon^{2m} + \varepsilon^{m\mp 1} + \varepsilon^{\mp 2})\right)^3 = q^3\varepsilon^{5m}, \tag{4.13}$$

according to whether $p \equiv 3 \pmod 5$ or $p \equiv 2 \pmod 5$. If $p \equiv 3 \pmod 5$, then, since the right-hand side is positive, so must be the left-hand side, and as $\varepsilon > 1$ we must have $m > 3$. Suppose that m were even. Then after conjugating, we would have

$$-\frac{1}{\sqrt{5}}(\varepsilon^{-m} + \varepsilon^{\mp 3})\left(5(\varepsilon^{-m} + \varepsilon^{\mp 1})(\varepsilon^{-2m} - \varepsilon^{-m\pm 1} + \varepsilon^{\pm 2})\right)^3 = q^3\varepsilon^{-5m},$$

and therefore also $\varepsilon^{-2m} - \varepsilon^{-m\pm 1} + \varepsilon^{\pm 2} < 0$, a contradiction in both cases. We set $m = 2\ell \pm 3$ according to the sign in $p \equiv \pm 3 \pmod 5$, where ℓ is a positive integer. Let $v_{\sqrt{5}}$ be the valuation corresponding to the irreducible element $\sqrt{5}$ of the ring of integers of $\mathbb{Q}(\sqrt{5})$ (which is a UFD). Then, from (4.13) we have

$$v_{\sqrt{5}}(\varepsilon^{-m} + \varepsilon^{\mp 3}) - 1 + 3v_{\sqrt{5}}\left(5(\varepsilon^{-m} + \varepsilon^{\mp 1})(\varepsilon^{-2m} - \varepsilon^{-m\pm 1} + \varepsilon^{\pm 2})\right) = 3v_{\sqrt{5}}(q).$$

Therefore $v_{\sqrt{5}}(\varepsilon^{-m} + \varepsilon^{\mp 3}) \equiv 1 \pmod 3$, and since $v_{\sqrt{5}}(\varepsilon^{-m} + \varepsilon^{\mp 3}) \geq 0$, this implies $v_{\sqrt{5}}(\varepsilon^{-m} + \varepsilon^{\mp 3}) \geq 1$ Thus the first factor in (4.13) is divisible by $\sqrt{5}$. Now multiply (4.13) by $\varepsilon^{-\ell\mp 3}$ to obtain

$$\frac{1}{\sqrt{5}}(\varepsilon^{\ell} - \varepsilon^{-\ell})\left(5(\varepsilon^m - \varepsilon^{\pm 1})(\varepsilon^{2m} + \varepsilon^{m\mp 1} + \varepsilon^{\mp 2})\right)^3 = q^3\varepsilon^{3(3\ell\pm 4)}.$$

Therefore the number $\frac{1}{\sqrt{5}}(\varepsilon^{\ell} - \varepsilon^{-\ell})$ is a cube in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ and is positive. We have $\varepsilon^{2\ell} - 1 = \varepsilon^{\mp 3}(\varepsilon^m - \varepsilon^{\pm 3}) \equiv 0 \pmod{\sqrt{5}}$, or $\varepsilon^{2\ell} \equiv 1 \pmod{\sqrt{5}}$. But $\varepsilon^2 = \frac{1}{4}(1+\sqrt{5})^2 = \frac{1}{4}(10 - 4 + 2\sqrt{5}) \equiv -1 \pmod{\sqrt{5}}$. So $(-1)^{\ell} \equiv 1 \pmod{\sqrt{5}}$, meaning that ℓ is even. Let $\ell = 2L$ and $\varepsilon^L = \frac{1}{2}(x + y\sqrt{5})$, where $x, y, L \in \mathbb{Z}$. We have $N(\varepsilon^L) = N(\varepsilon)^L = (-1)^L$. On the other hand, $N(\varepsilon^L) = \varepsilon^L\overline{\varepsilon^L} = \frac{1}{4}(x^2 - 5y^2)$. Here the horizontal line denotes the nontrivial automorphism of $\mathbb{Q}(\sqrt{5})$. Therefore

$$x^2 - 5y^2 = (-1)^L 4. \tag{4.14}$$

Note that $\varepsilon^{-2L} = (-1)^{2L}\overline{\varepsilon^{2L}}$. It follows that

$$\frac{1}{\sqrt{5}}(\varepsilon^{\ell} - \varepsilon^{-\ell}) = \frac{1}{\sqrt{5}}(\varepsilon^{2L} - \varepsilon^{-2L}) = \frac{1}{\sqrt{5}}\left(\frac{(x + y\sqrt{5})^2}{4} - \frac{(x - y\sqrt{5})^2}{4}\right) = xy.$$

Since the integer xy is a cube in $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ it is also a cube in $\mathbb{Z}$. This can be seen as follows. Let $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ be a root of the $T^3 - xy$. Then $\overline{\alpha}$ is also a root of this polynomial. Therefore $T^3 - xy$ has a quadratic factor with rational

coefficients. Consequently, it has a linear factor with rational coefficients. But $\mathbb{Z}$ is integrally closed, so we get a root in $\mathbb{Z}$. The equation (4.14) implies that $gcd(x,y) = 1$ or $gcd(x,y) = 2$. Note that if $gcd(x,y) = 2$, then exactly one of x and y is divisible by 4. We therefore have three cases, according to the greatest common divisor of x and y, and from (4.14) we get the corresponding equations:

I. $(x,y) = (u^3, v^3)$ $\quad u^6 - 5v^6 = \pm 4$,
II. $(x,y) = (4u^3, 2v^3)$ $\quad 4u^6 - 5v^6 = \pm 1$,
III. $(x,y) = (2u^3, 4v^3)$ $\quad u^6 - 20v^6 = \pm 1$,

with u, v odd. Note that since xy is positive, u and v have equal sign.

Proposition 4.5.1. *The element 2 is irreducible in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. The set*

$$\{0, \varepsilon, \varepsilon^2 = 1 + \varepsilon, \varepsilon^3 = 1 + 2\varepsilon\}$$

is a complete set of representatives for $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}/(2)$.

Proposition 4.5.2. *Let u, v be odd integers having equal sign such that $u^6 - 5v^6 = -4$. Then $u = v = 1$.*

Proof. Rewrite the equation as

$$(2 + \sqrt{5}v^3)(2 - \sqrt{5}v^3) = (-u^2)^3.$$

The two factors on the left side are relatively prime. For if a irreducible $\pi \in \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ divides them both, it divides also their sum 4, and so $\pi = 2$. But then $\sqrt{5}v^3 \equiv 0 \pmod 2$, which is impossible, because v is odd, and $\sqrt{5} \equiv 0 \pmod 2$ implies $5 \equiv 0 \pmod 4$. (Alternatively, since u was assumed to be odd, so must be the factors on the left side). Therefore, since $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ is a UFD, we have

$$2 + \sqrt{5}v^3 = \varepsilon^g \mu^3, \qquad \mu = \frac{r + \sqrt{5}s}{2} \qquad \text{where } g, r, s \in \mathbb{Z}.$$

The numbers v, μ are relatively prime to 2, so by Proposition 4.5.1, $v^3, \mu^3 \equiv 1 \pmod 2$. Thus $\varepsilon^g \equiv 2 + \sqrt{5} \equiv 1 \pmod 2$. Therefore by Proposition 4.5.1 $g \equiv 0 \pmod 3$. We may assume that $g = 0$. Then

$$16 + 8\sqrt{5}v^3 = r^3 + 3\sqrt{5}r^2 s + 15rs^2 + 5\sqrt{5}s^3.$$

or

$$16 = r(r^2 + 15s^2),$$
$$8v^3 = s(3r^2 + 5s^2).$$

Therefore $r = s = 1$ and $v = 1$. Consequently $u^6 = 1$, or $u = 1$. □

Let

$$\varepsilon^n = \frac{x_n + y_n\sqrt{5}}{2} \quad x_n, y_n \in \mathbb{Z}, \quad x_n \equiv y_n \pmod 2, \quad n \geq 1.$$

If $d_n = (x_n, y_n)$, then $x_n = d_n u_n$ and $y_n = d_n v_n$, so taking norm we get $4(-1)^n = d_n^2 N(u_n + v_n\sqrt{5})$, meaning that $d_n \in \{1, 2\}$. Furthermore

$$x_n y_n = \frac{1}{\sqrt{5}}(\varepsilon^{2n} - \varepsilon^{-2n}), \qquad x_n^2 - 5y_n^2 = (-1)^n 4.$$

Proposition 4.5.2 tells us that if $(x_n, y_n) = 1$, n is odd, and $x_n y_n$ is a cube, then $n = 1$, $\varepsilon^n = \varepsilon$, and $x_n = y_n = 1$.

Now consider $n = 2k$ even, so that

$$\varepsilon^{2k} = \frac{x_{2k} + y_{2k}\sqrt{5}}{2}, \qquad (\varepsilon^k)^2 = \left(\frac{x_k + y_k\sqrt{5}}{2}\right)^2 = \frac{(x_k^2 + 5y_k^2) + 2x_k y_k\sqrt{5}}{4},$$
$$2x_{2k} = x_k^2 + 5y_k^2, \qquad y_{2k} = x_k y_k.$$

Suppose that $(x_{2k}, y_{2k}) = 1$ and that $x_{2k}y_{2k}$ is a cube. Then $(x_k, y_k) = 1$, and $x_k y_k$ is a cube. Repeating this procedure, we must arrive at some $n_0 = 2k_0$, where k_0 is odd. But then $k_0 = 1$, and $n_0 = 2$. This is a contradiction, because by our assumption x_{n_0} is a cube; but on the other hand, $\varepsilon^{n_0} = \varepsilon^2 = \frac{3+\sqrt{5}}{2}$, so $x_{n_0} = 3$ which is not a cube in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ (we have already shown that if a rational integer is a cube in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ then it is a cube in $\mathbb{Z}$).

Now consider the case of $(x_n, y_n) = 2$, $x_n y_n$ cube, and $x_n = 4u_n^3$ $y_n = 2v_n^3$, with u_n and v_n odd. Then $4u_n^6 - 5v_n^6 = (-1)^n$, and reducing modulo 4, we see that n must be odd. Write

$$(2u_n^3 - \sqrt{5}v_n^3)(2u_n^3 + \sqrt{5}v_n^3) = -1. \tag{4.15}$$

Since ε is a fundamental unit we have $2u_n^3 + \sqrt{5}v_n^3 = \varepsilon^k$ for some k. Using (4.15) we obtain $-1 = \overline{\varepsilon^k}\varepsilon^k = (-1)^k\varepsilon^{-k}\varepsilon^k = (-1)^k$, meaning that k is odd. Also $\varepsilon^k = 2u_n^3 + \sqrt{5}v_n^3 \equiv 1 \pmod 2$, so $k = 3r$, $r \in \mathbb{Z}$ by Proposition 4.5.1. Then

$$\begin{aligned}
\varepsilon^r &= \frac{x_r + y_r\sqrt{5}}{2}, \qquad -\varepsilon^{-r} = \frac{x_r - y_r\sqrt{5}}{2},\\
x_r^2 - 5y_r^2 &= -4, \qquad x_r y_r = \frac{1}{\sqrt{5}}(\varepsilon^{2r} - \varepsilon^{-2r}),\\
2u_n^3 - \sqrt{5}v_n^3 &= -\varepsilon^{-3r}, \qquad 2u_n^3 + \sqrt{5}v_n^3 = \varepsilon^{3r},\\
4u_n^3 &= \varepsilon^{3r} - \varepsilon^{-3r} = (\varepsilon^r - \varepsilon^{-r})(\varepsilon^{2r} + \varepsilon^{-2r} + 1)\\
&= x_r\left(\frac{1}{2}(x_r^2 + 5y_r^2) + 1\right)\\
&= x_r\left(\frac{1}{2}(x_r^2 + (x_r^2 + 4)) + 1\right) = x_r(x_r^2 + 3),\\
2\sqrt{5}v_n^3 &= \varepsilon^{3r} + \varepsilon^{-3r} = (\varepsilon^r + \varepsilon^{-r})(\varepsilon^{2r} + \varepsilon^{-2r} - 1)\\
&= \sqrt{5}y_r\left(\frac{1}{2}(x_r^2 + 5y_r^2) - 1\right) = \sqrt{5}y_r\left(\frac{1}{2}((5y_r^2 - 4) + 5y_r^2) - 1\right)\\
&= \sqrt{5}y_r(5y_r^2 - 3).
\end{aligned}$$

Thus $4u_n^3 = x_r(x_r^2 + 3)$ and $2v_n^3 = y_r(5y_r^2 - 3)$. Since u_n and v_n are odd, we have $(x_r, y_r) \in \{1, 2\}$. We claim that x_r, y_r are not divisible by 3. Otherwise, $\varepsilon^{2r} - \varepsilon^{-2r} \equiv 0 \pmod 3$, or $\varepsilon^{2r} - \varepsilon^{-2r} \equiv 0 \pmod 3$, $\varepsilon^{4r} \equiv 1 \pmod 3$. But $\varepsilon^4 = \frac{7+3\sqrt{5}}{2} \equiv -1 \pmod 3$, so $\varepsilon^{4r} \equiv (-1)^r \equiv -1 \pmod 3$, because r is odd, which is a contradiction. Therefore x_r, y_r are not divisible by 3. It follows that either $(x_r, y_r) = 1$ and x_r, y_r are odd, or $(x_r, y_r) = 2$ and $x_r = 4u_r$, $y_r = 2v_r$, where u_r, v_r are odd. In the former case, x_r and y_r are cubes, so $r = 1$, $x_r = 1$, $y_r = 1$, $\varepsilon^3 = 2 + \sqrt{5}$, so $u_n = v_n = 1$, $x_n = 4$, $y_n = 2$. In the latter case, u_r, v_r are cubes. If r is smallest such r, then $r = 3$ and $k = 9$. But $\varepsilon^9 = 38 + 17\sqrt{5}$, which is a contradiction, because 17 is not a cube in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$.

In the last case we have $(x_n, y_n) = 2$, $x_n y_n$ is a cube, and $x_n = 2u_n^3$, $y_n = 4v_n^3$, with u_n and v_n odd. This is resolved similarly, for more details see Siegel's article [Sie68].

Alternatively and more succinctly, we may reduce the solving of the diophantine equation (4.13) to the determination of cubes in the Fibonacci sequence. Let $F_{\ell+1} = F_\ell + F_{\ell-1}$, $F_0 = 0$, and $F_1 = 1$. We have for ℓ even

$$F_\ell = \frac{1}{\sqrt{5}}(\varepsilon^\ell - (-\varepsilon^{-1})^\ell) = \frac{1}{\sqrt{5}}(\varepsilon^\ell - \varepsilon^{-\ell}).$$

We are interested for which positive even ℓ the number F_ℓ is a cube. According to the results of [LF69], this is the case only for $\ell = 2, 6$. Hence

$$\begin{aligned} m_p = m = 2\ell - 3 = 1, 9 \qquad & \text{if } p \equiv 2 \pmod 5, \\ m_p = m = 2\ell + 3 = 7, 15 \qquad & \text{if } p \equiv 3 \pmod 5, \end{aligned}$$

We have therefore proved the following result.

Theorem 4.5.3. *Let $p > 3$ be a prime such that $p \equiv 3 \pmod 4$. Suppose that the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-p})$ has class number 1. Let*

$$w_p = \frac{5p + \sqrt{-p}}{2}.$$

Then $\psi(\omega_p) = \varepsilon, \varepsilon^9$ if $p \equiv 2 \pmod 5$, and $\varphi(\omega_p) = \varepsilon^7, \varepsilon^{15}$ if $p \equiv 3 \pmod 5$.

Now it is easy to prove that there are exactly 9 imaginary quadratic fields with class number 1. By Theorem 4.4.3 the j-invariant is rationally expressible via both of the functions φ and ψ. Therefore, by Theorem 4.5.3, there are 4 possible values for $j(w_p)$. On the other hand, the function j is injective modulo $\mathrm{SL}_2(\mathbb{Z})$, so the value $j(\omega_p)$ uniquely determines p and the corresponding imaginary quadratic field. Of the 9 discriminants

$$\{-3, -4, -7, -8, -11, -19, -43, -67, -163\}$$

corresponding to quadratic imaginary quadratic fields with class number 1, only 4 primes $p > 3$ satisfy $p \equiv 2 \pmod 3$, namely $7, 43, 67, 163$. Therefore these are the discriminants of the quadratic imaginary fields corresponding to the values $\varepsilon, \varepsilon^9$ and $\varepsilon^7, \varepsilon^{15}$. We can also calculate the corresponding values of the j-invariant using the relations of Theorem 4.4.3.

To conclude, we mention the final remark of Siegel.

"Es ist bemerkenswert, daß den sämtlichen Lösungen der diophantine Gleichung (4.13) auch wieder imaginär quadratische Körper mit der Klassenzahl 1 entsprechen; man mag in einer solchen Tatsache je nach Temperament etwa wie Leibniz und Hilbert einen Ausdruck prästabilierter Harmonie oder wie Dedekind eine schöne Sparsamkeit erblicken."

Bibliography

[Apo] Tom M. Apostol. *Modular Functions and Dirichlet Series in Number Theory (1976)*. New York: Springer.

[Bar09] Burcu Baran. A modular curve of level 9 and the class number one problem. *J. Number Theory*, 129(3):715–728, 2009.

[Bar10] Burcu Baran. Normalizers of non-split cartan subgroups, modular curves, and the class number one problem. *Journal of Number Theory*, 130(12):2753–2772, 2010.

[BCH66] A. Borel, S. Chowla, and C. S. Herz. *Seminar on complex multiplication*. Springer, 1966.

[Bir69a] Bryan J. Birch. Diophantine analysis and modular functions. In *Algebraic Geometry (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968)*, pages 35–42. Oxford Univ. Press, London, 1969.

[Bir69b] Bryan J. Birch. Webers class invariants. *Mathematika*, 16(02):283, 1969.

[Bir04] Bryan J. Birch. Heegner points: The beginnings. *Heegner Points and Rankin L-Series*, page 1–10, 2004.

[Bir11] Bryan J. Birch. Heegner's proof. *Arithmetic of L-functions*, page 281–291, 2011.

[Boo] Jeremy Booher. Modular curves and the class number one problem. `https://www.math.arizona.edu/~jeremybooher/expos/class_number_one.pdf`. Accessed: 2019-05-11.

[Che99] Imin Chen. On siegels modular curve of level 5 and the class number one problem. *Journal of Number Theory*, 74(2):278–297, 1999.

[Con] Keith Conrad. Factoring in quadratic fields. `https://kconrad.math.uconn.edu/blurbs/gradnumthy/quadraticgrad.pdf`.

[Cox11] David A Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, volume 34. John Wiley & Sons, 2011.

[cva] Foundation for german communication and related technologies. `https://www.cdvandt.org/kurt_heegner.htm`.

[DCS09] Della Dumbaugh, Leo Corry, and Joachim Schwermer. History of mathematics of the early 20th century: The role of transition. *Oberwolfach Reports*, 5(2):1295–1360, 2009.

[Ded00] Richard Dedekind. Ueber die Anzahl der Idealklassen in reinen kubischen Zahlkörpern. *J. Reine Angew. Math.*, 121:40–123, 1900.

[Deu58] Max Deuring. *Die Klassenkorper der komplexen Multiplikation*. Teubner, 1958.

[Deu68] Max Deuring. Imaginäre quadratische Zahlkörper mit der Klassenzahl Eins. *Invent. Math.*, 5:169–179, 1968.

[DIT18] William Duke, Özlem Imamoḡlu, and Árpad Tóth. Kronecker's first limit formula, revisited. *Research in the Mathematical Sciences*, 5(2):1–21, 2018.

[DS05] Fred Diamond and Jerry Michael Shurman. *A first course in modular forms*, volume 228. Springer, 2005.

[Elk99] Noam D. Elkies. The Klein quartic in number theory. In *The eightfold way*, volume 35 of *Math. Sci. Res. Inst. Publ.*, pages 51–101. Cambridge Univ. Press, Cambridge, 1999.

[GC86] Carl Friedrich. Gauss and Arthur A. Clarke. *Disquisitiones arithmeticae*. Springer, 1986.

[Gee99] Alice Gee. Class invariants by shimuras reciprocity law. *Journal de Théorie des Nombres de Bordeaux*, 11(1):45–72, 1999.

[Gol85] Dorian Goldfeld. Gauss class number problem for imaginary quadratic fields. *Bulletin of the American Mathematical Society*, 13(1):23–38, 1985.

[Gro84] Benedict H. Gross. Heegner points on $X_0(N)$. In *Modular forms (Durham, 1983)*, Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., pages 87–105. Horwood, Chichester, 1984.

[hde] Noam D. Elkies (https://mathoverflow.net/users/14830/noam-d elkies). Effective bound on the expansion of the j-invariant. MathOverflow. URL:https://mathoverflow.net/q/302799 (version: 2018-06-14).

[Hee52] Kurt Heegner. Diophantische analysis und modulfunktionen. *Mathematische Zeitschrift*, 56(3):227–253, 1952.

[Ken85] Monsur A. Kenku. A note on the integral points of a modular curve of level 7. *Mathematika*, 32(1):45–48, 1985.

[Kez] Yukako Kezuka. The class number problem. `http://wwwf.imperial.ac.uk/~buzzard/maths/research/notes/Yukako_Kezuka_MSc_Project.pdf`. Accessed: 2019-05-11.

[KL81] Daniel S. Kubert and Serge Lang. *Modular units*, volume 244 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York-Berlin, 1981.

[Lan87] Serge Lang. *Elliptic functions*. Springer, 1987.

[LF69] Hymie London and Raphael Finkelstein. On Fibonacci and Lucas numbers which are perfect powers. *Fibonacci Quart.*, 7(5):476–481, 487; errata, ibid. 8 (1970), no. 3, 248, 1969.

[Mey57] Curt Meyer. *Die Berechnung der Klassenzahl Abelscher Körper über quadratischen Zahlkörpern*. Berlin, 1957.

[Mey70] Curt Meyer. Bemerkungen zum satz von heegner-stark über die imaginär-quadratischen zahlkörper mit der klassenzahl eins. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 1970(242), 1970.

[Mil18] James S. Milne. Fields and galois theory (v4.60), 2018. Available at www.jmilne.org/math/.

[Rob73] Alain Robert. *Elliptic curves*. Lecture Notes in Mathematics, Vol. 326. Springer-Verlag, Berlin-New York, 1973. Notes from postgraduate lectures given in Lausanne 1971/72.

[Sat87] Philippe Satgé. Un analogue du calcul de Heegner. *Invent. Math.*, 87(2):425–439, 1987.

[Scha] Norbert Schappacher. El outsider de la teoria de los numeros. `http://irma.math.unistra.fr/~schappa/NSch/Presentations_files/HeegnerMadrid.pdf`.

[Schb] Norbert Schappacher. Kurt heegner. `http://irma.math.unistra.fr/~schappa/NSch/Presentations_files/HeegnerParis.pdf`.

[Sch10] Reinhard Schertz. *Complex multiplication*. Cambridge University Press, 2010.

[Ser72] Jean-P. Serre. Proprietes galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser85] Jean-P. Serre. $\Delta = b^2 - 4ac$. *Math. Medley*, 13(1):1–10, 1985.

[Ser90] Jean-P. Serre. *Lectures on the Mordell Weil theorem*. Vieweg, 1990.

[Ser12] Jean-Pierre Serre. *A course in arithmetic*, volume 7. Springer Science & Business Media, 2012.

[Sha14] Igor R. Shafarevich. On the problem of the 10th discriminant. *St. Petersburg Mathematical Journal*, 25(4):699–711, 2014.

[Shi94] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*. Princeton Univ. Press, 1994.

[Sie68] Carl Ludwig Siegel. Zum Beweise des Starkschen Satzes. *Inventiones mathematicae*, 5(3):180–191, 1968.

[Sil09] Joseph H. Silverman. *The Arithmetic of elliptic curves*. Springer-Verlag, 2009.

[Sil11] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Springer, 2011.

[SR80] Carl Ludwig Siegel and KG Ramanathan. *Advanced analytic number theory*, volume 9. Tata Institute of Fundamental Research Bombay, 1980.

[Sta67] Harold M. Stark. A complete determination of the complex quadratic fields of class-number one. *The Michigan Mathematical Journal*, 14(1):1–27, 1967.

[Sta69] Harold M. Stark. On the "gap" in a theorem of Heegner. *Journal of Number Theory*, 1:16–27, 01 1969.

[Sta11] Harold Stark. The origin of the "Stark conjectures". In *Arithmetic of L-functions*, volume 18 of *IAS/Park City Math. Ser.*, pages 33–44. Amer. Math. Soc., Providence, RI, 2011.

[Ste] Peter Stevenhagen. Elliptic functions. `https://websites.math.leidenuniv.nl/algebra/ellipticfunctions.pdf`. Accessed: 2019-05-11.

[Wal] Candy Walter. Das Gauss'sche Klassenzahl-Eins-Problem. `https://www.uni-hildesheim.de/media/fb4/mathematik/Publikationen/Walter_Masterarbeit_Gesamt.pdf`. Accessed: 2019-05-28.

[Web08] Heinrich Weber. *Lehrbuch der Algebra, vol. III.* Vieweg und Sohn, Braunschweig, 1908.

[Zag] Don B. Zagier. Elliptic modular forms and their applications. `https://people.mpim-bonn.mpg.de/zagier/files/doi/10.1007/978-3-540-74119-0_1/fulltext.pdf`. Accessed: 2019-05-11.

[Zag81] Don B. Zagier. *Zetafunktionen und quadratische Körper.* Springer-Verlag, Berlin-New York, 1981.