Traces of singular moduli

Ana Marija Vego
mail: avego@student.ethz.ch
ETH Zürich

Abstract. *In this semester project we will give an exposition of Zagier's result on traces of singular moduli. Before that, we start by giving some necessary background in the theory of complex multiplication and class field theory. Then we briefly introduce modular forms of half-integral weight. At the end we will show how the result on singular moduli implies Kronecker's class number formulas and formulas for computing Fourier coefficients of the j-invariant.*

Supervisors: Prof. Dr. Özlem Imamoglu,
Dr. Markus Schwagenscheidt

Contents

1 Introduction

We will start this paper by introducing the Weierstrass $\wp$-function and the j-invariant and giving a couple of useful properties, which will be mainly tied to the theory of complex multiplication. We want to show that the values of the j-invariant at CM-points α (i.e. *singular moduli*) are algebraic integers. For this we will recall some necessary tools from class field theory. That will occupy Chapter 2, where we mainly follow [C], but also rely on [EF] and [J]. Some useful prerequisites for introducing class field theory in Chapter 2 can also be found in the Appendix 5.

We will also see that the j-invariants of the set of Γ-equivalence classes (where $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$) of CM-points of a fixed discriminant $d < 0$ are Galois conjugates and hence we can take their sum to be the trace. This weighted trace,

$$t(d) = \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{1}{|\Gamma_Q|}(j(\alpha_Q) - 744),$$

is called the *modular trace function*. Here we take $\mathcal{Q}_d$ to be the set of positive definite integral binary quadratic forms of discriminant d, Γ_Q is the stabilizer and α_Q is the root of $Q(z,1)=0$. Also, note that the sum is finite, moreover it has $h(-d)$ summands, where $h(-d)$ denotes the class number of $-d$. For example, $h(-3)=h(-7)=1$, $h(-15)=2$ and

$$j\left(\frac{1+i\sqrt{3}}{2}\right)=0, \quad j\left(\frac{1+i\sqrt{7}}{2}\right)=-3375,$$

and

$$j\left(\frac{1+i\sqrt{15}}{2}\right)=\frac{-191025-85995\sqrt{5}}{2}, \quad j\left(\frac{1+i\sqrt{15}}{4}\right)=\frac{-191025+85995\sqrt{5}}{2}.$$

This gives

$$\begin{aligned} t(3) &= \frac{0-744}{3}=-248, \\ t(7) &= -3375-744=-4119, \\ t(15) &= -191025-2\cdot 744=-192513. \end{aligned}$$

We will see that $t(d)$ can be used to compute coefficients of a modular form of weight $3/2$:

$$g(\tau)=\theta_1(\tau)\frac{E_4(4\tau)}{\eta(4\tau)^6}=\sum_{d\geq -1}B(d)q^d=\frac{1}{q}-2+248q^3-492q^4+4119q^7+\ldots,$$

where $q=e^{2\pi i\tau}$, E_4 is the normalised Eisenstein series, η is the Dedekind eta function and

$$\theta_1(z)=\sum_{n\in\mathbb{Z}}(-1)^n q^{n^2}.$$

In Chapter 3 we will make sense of modular forms of half-integral weight and recall the operator U_4 on modular forms. Here we rely on [K], [KH], [Kohl] and [AL].

Now, to the main chapter. The main result (Theorem 4.0.1) is the following:

Theorem 1.0.1. For all $d>0$

$$t(d)=-B(d).$$

To prove this we directly follow Zagier's paper [Z] and put together all the results established in previous chapters. This will occupy the first two sections of Chapter 4. The proof idea is to compute and then compare recursion formulas for both $B(d)$ and $t(d)$. For $B(d)$ we use properties from modular forms of half-integral weight, while for $t(d)$ we will write out the "modular polynomial"

$$\Phi_n(X,j(\tau))=\prod_{M\in\Gamma\backslash\mathcal{M}_n}(X-j(M\tau)), \quad \tau\in\mathcal{H},$$

(where $\mathcal{M}_n$ is the set of 2×2 integral matrices with determinant n) in two different ways and then compare coefficients.

The last two sections of Chapter 4 are concerned with two (simple) "byproducts" of Theorem 1.0.1. In Section 4.3 we will show how to obtain Kronecker's class number relations from the proof of Theorem 1.0.1:

Proposition 1.0.2 (***Kronecker's class number relations***)**.** Let $d \in \mathbb{N}$ with $d \equiv 0$ or $3 \pmod 4$. Then

$$\sum_{|r|<2\sqrt{n}} H\left(4n-r^2\right) = \sum_{d|n} \max\{d, n/d\} + \begin{cases} 1/6, & \text{if } n \text{ is a square} \\ 0, & \text{otherwise,} \end{cases}$$

$$\sum_{|r|<2\sqrt{n}} \left(n-r^2\right) H\left(4n-r^2\right) = \sum_{d|n} \min(d, n/d)^3 - \begin{cases} n/2, & \text{if } n \text{ is a square} \\ 0, & \text{otherwise,} \end{cases}$$

where $H(d)$ is the *Hurwitz-Kronecker class number*

$$H(d) = \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{1}{w_Q},$$

for $w_Q = |\Gamma_Q|$.

Proposition 1.0.2 was also obtained by Zagier in [Z]. Finally, in Section 4.4, following [Kan], we prove formulas for computing the Fourier coefficients of the j-invariant that only rely on $t(d)$:

Theorem 1.0.3. For all $n \geq 1$ and

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

one has

$$c_n = \frac{1}{n}\left(\sum_{r \in \mathbb{Z}} t(n-r^2) - \sum_{r \geq 1,\ \text{odd}} \left((-1)^n t(4n-r^2) - t(16n-r^2)\right)\right).$$

2 An introduction to the j-invariant and the theory of complex multiplication

2.1 Complex multiplication

In this section we will first recall some necessary properties of the Weierstrass $\wp$-function and the j-invariant (mainly without proof and with references). The main goal is to give an explicit construction for the Abelian extensions of a given imaginary quadratic field K, and for that we will introduce complex multiplication. In this section we will mainly follow [C] chapter 7,10 and 11, and [EF].

For the remainder of this chapter we let $L := [w_1, w_2] = w_1\mathbb{Z} \oplus w_2\mathbb{Z}$ be a lattice in $\mathbb{C}$, generated by w_1, w_2 linearly independent over $\mathbb{R}$.

Definition 2.1.1. An ***elliptic function*** for L is a function f defined on $\mathbb{C}$ such that

(i) f is meromorphic on $\mathbb{C}$,

(ii) $f(z+w) = f(z)$, for every $w \in L$.

Note that (ii) is equivalent to $f(z+w_1) = f(z+w_2) = f(z)$, where $L = [w_1, w_2]$, hence an elliptic function is a doubly periodic meromorphic function. Elements of L are often referred to as *periods* of f.

Lemma 2.1.2. An elliptic function of order r has precisely r roots in any period parallelogram P, where

$$P := \{aw_1 + bw_2, 0 \leq a, b < 1\}.$$

Proof: See [EF] Chapter 1.

Definition 2.1.3 (***Weierstrass $\wp$-function***)**.** Take $z \in \mathbb{C} \setminus L$. Then we define the *Weierstrass $\wp$-function* as follows:

$$\wp(z; L) := \frac{1}{z^2} + \sum_{w \in L - \{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

Next, we will give a few useful properties of the Weierstrass $\wp$-function. Before that we have to introduce two important functions, called *Weierstrass invariants* on a lattice L:

$$\begin{cases} g_2(L) := 60 \sum_{w \in L - \{0\}} \frac{1}{w^4}, \\ g_3(L) := 140 \sum_{w \in L - \{0\}} \frac{1}{w^6}. \end{cases} \tag{1}$$

Proposition 2.1.4. Let L be a fixed lattice and $\wp(z)$ denote the *Weierstrass $\wp$-function* for L. Then for any $z, w, z+w \in \mathbb{C} \setminus L$ one has

(i) $\wp$ is an even elliptic function for L whose singularities are double poles at the points of L.

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

(iii) $\wp(z+w) = -\wp(z) - \wp(w) + \frac{1}{4}\left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)} \right)^2$.

Proof: See [C] pg. 200-205.

Then by writing

$$G_r(L) := \sum_{w \in L - \{0\}} \frac{1}{w^r}, \quad r > 2$$

for the Eisenstein series of weight r, one can obtain the following expression for the $\wp$-function in a neighbourhood of the origin:

$$\begin{aligned} \wp(z) &= \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) G_{2n+2}(L) z^{2n}, \\ \wp'(z) &= \frac{-2}{z^3} + \sum_{n=1}^{\infty} 2n(2n+1) G_{2n+2}(L) z^{2n-1}, \end{aligned} \tag{2}$$

where the first expression is the *Laurent expansion* of $\wp$. For the proof of this we refer to [C] chapter 10.

Definition 2.1.5. Two lattices L, L' are called ***homothetic*** if $L' = \lambda L$, for some $\lambda \in \mathbb{C} - \{0\}$.

Remark 2.1.6. Homothety is an equivalence relation.

Note that for the *Weierstrass $\wp$-function* one has

$$\wp(\lambda z; \lambda L) = \lambda^{-2} \wp(z; L). \tag{3}$$

Moreover, if $f(z)$ is an arbitrary elliptic function for L, then $f(\lambda z)$ is an elliptic function for $1/\lambda L$.

Next we would like to classify lattices up to homothety. This will be one of the main motivations for introducing the j-invariant.

Definition 2.1.7 (***j-invariant***)**.** The *j-invariant* of a lattice L is given by

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

where $\Delta(L) := g_2(L)^3 - 27 g_3(L)^2$.

Remark 2.1.8. If L is a lattice, then $\Delta(L) \neq 0$.

Let L, L' be two lattices. Using equation (1) for λL instead of L one can see that $g_2(\lambda L) = \lambda^{-4} g_2(L)$ and similarly $g_3(\lambda L) = \lambda^{-6} g_3(L)$. Using these expressions we deduce that:

$$j(L) = j(L') \quad \iff \quad L \text{ and } L' \text{ are homothetic.} \tag{4}$$

So far we have discussed the j-invariant of a lattice, but we can also consider the j-invariant of a complex number $z \in \mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. By that we mean to consider the lattice generated by 1 and z, namely $[1, z]$ and then we define the ***j-function*** $j(z)$ as

$$j(z) := j([1, z]).$$

Now we are equipped to introduce complex multiplication. For that we recall Appendix 5 for definition of order $\mathcal{O}$.

Let K be an imaginary quadratic field, and $\mathcal{O}$ an order in K. Furthermore, let $\mathfrak{a}$ be a proper fractional $\mathcal{O}$-ideal. Then $\mathfrak{a}$ is a free $\mathbb{Z}$-module of rank 2, hence there exist $\alpha, \beta \in K$ such that $\mathfrak{a} = [\alpha, \beta]$.

Now, we consider $j(\mathfrak{a})$. Note that this expression makes sense because K is imaginary quadratic and is a subset of $\mathbb{C}$, so α and β are linearly independent over $\mathbb{R}$. The values of the j-invariant at those quadratic irrationalities are called ***singular moduli***.

To introduce complex multiplication, we turn our attention to the Weierstrass $\wp$-function. Recall the formula from Proposition 2.1.4 (iii) for $z \in \mathbb{C} - L$ and $w := z$

$$\wp(2z) = -2\wp(z) + \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2. \tag{5}$$

Using Proposition 2.1.4 (ii) and the second derivative $\wp''(z) = 6\wp(z)^2 - \frac{1}{2}g_2$, equation (5) transforms to

$$\wp(2z) = -2\wp(z) + \frac{(12\wp(z)^2 - g_2)^2}{16(4\wp(z)^3 - g_2\wp(z) - g_3)}. \tag{6}$$

The main takeaway from the computation above is that $\wp(2 \cdot z)$ can be expressed as a *rational function* in $\wp(z)$. If we replace the 2 by any other integer $n \in \mathbb{N}$, one can similarly show that $\wp(nz)$ is again a rational function in $\wp(z)$.
Now, what if n was not an integer but a *complex number*, can it again be written as a rational function in $j(z)$? The next Theorem gives an answer to that question.

Theorem 2.1.9 (***complex multiplication***)**.** Let L be a lattice and $\wp(z)$ the $\wp$-function for L. For every $\alpha \in \mathbb{C} - \mathbb{Z}$ the following are equivalent:

(i) $\wp(\alpha z)$ is a rational function in $\wp(z)$,

(ii) $\alpha L \subset L$,

(iii) there exists an order $\mathcal{O}$ in an imaginary quadratic field K such that $\alpha \in \mathcal{O}$ and L is homothetic to a proper fractional $\mathcal{O}$-ideal.

If the above holds, then

$$\wp(\alpha z) = \frac{A(\wp(z))}{B(\wp(z))},$$

where $A(x), B(x)$ are relatively prime polynomials such that

$$\deg(A(x)) = \deg(B(x)) + 1 = [L : \alpha L] = N(\alpha).$$

Before proving this we will show a useful Lemma, which will also be neccessary for the proof of Theorem 2.1.9.

Lemma 2.1.10. Every even elliptic function f for L is a rational function of $\wp$.

Proof: If f has a zero or a pole at the origin, it must be of even order, since f is an even function. Therefore there exists an integer m such that $f\wp^m$ has no zero or pole at the lattice points. Thus, we may assume that f itself has no zero or pole on $L = [w_1, w_2]$.
Next, we want to count the *zeros* and *poles* of f. By Proposition 2.1.4 $\wp$ is an elliptic function, so $\wp$ is meromorphic with periods w_1 and w_2 which generate a lattice L.

Consider the period parallelogram

$$P := \{aw_1 + bw_2, 0 \leq a, b < 1\}.$$

Note that every point in $\mathbb{C}$ is congruent modulo L to a unique point in P. Moreover, we can tile the complex plane using the lattice L:

$$\mathbb{C} = \bigcup_{n,m\in\mathbb{Z}} (nw_1 + mw_2 + P).$$

Then $\wp$ is completely determined by its values in P. Completely analogously we see that f is also determined by its values in P.
Now, we would like to use $\wp$ to construct a doubly-periodic function g with the same zeros and poles as f. For that we have to find the zeros of $\wp$.

Since $\wp$ is even (by Proposition 2.1.4 (i)), we get that $\wp'$ is odd. Moreover, $\wp'$ is also periodic with periods w_1 and w_2, so

$$\wp'\left(\frac{w_1}{2}\right) = \wp'\left(\frac{w_2}{2}\right) = \wp'\left(\frac{w_1 + w_2}{2}\right) = 0.$$

Using Lemma 2.1.2 together with the fact that $\wp'$ is elliptic and has order 3, we get that the three points $w_1/2$, $w_2/2$ and $(w_1 + w_2)/2$ are the only roots of $\wp'$ in P, and they have multiplicity 1. We call these points ***half-periods***. Therefore, if we define

$$\wp\left(\frac{w_1}{2}\right) = e_1, \quad \wp\left(\frac{w_2}{2}\right) = e_2, \quad \wp\left(\frac{w_1 + w_2}{2}\right) = e_3,$$

we get that the equation $\wp(z) = e_1$ has a double root at $w_1/2$. Since $\wp$ has order 2, there are no other solutions for this equation in P.
Analogously, $\wp(z) = e_2$ and $\wp(z) = e_3$ have only double roots at $w_2/2$ and $(w_1 + w_2)/2$, respectively. In particular, e_1, e_2 and e_3 are distinct. Otherwise $\wp$ would have at least 4 roots in P, contradicting Lemma 2.1.2, since $\wp$ has order 2.

For $a \in P$ consider the function

$$\wp(z) - \wp(a).$$

By the discussion above, this has a single zero of order 2 if a is a half-period, and otherwise two distinct zeros at a and $-a$.

Let a be a zero of f. Then $-a$ is also a zero, since f is even. Moreover, we have seen that a is congruent to $-a$ if and only if it is a half-period, in which case the zero is of even order. Let $a_1, -a_1, \ldots, a_m, -a_m$ be all the zeros of f, counted with multiplicities. If a_i is not a half-period, then a_i and $-a_i$ have the multiplicity of f at these points. Otherwise, if a_i is a half-period, then a_i and $-a_i$ are congruent and each has multiplicity half of the multiplicity of f. then

$$\prod_{i=1}^{m} (\wp(z) - \wp(a_i))$$

has precisely the same roots as f.

Let $b_1, -b_1, \ldots, b_m, -b_m$ be all the poles of f with multiplicities. A similar argument shows that

$$g(z) = \prod_{i=1}^{m} \frac{\wp(z) - \wp(a_i)}{\wp(z) - \wp(b_i)} \tag{7}$$

is periodic and has the same zeros and poles as f.
Finally, since $\frac{f}{g}$ is holomorphic and doubly-periodic, it is constant. □

Corollary 2.1.11. Every elliptic function f for L is a rational function of $\wp$ and $\wp'$.

Proof: First, note that since $\wp$ is even, $\wp'$ is odd as a derivative of an even function. Next, write f as a sum of an even and an odd function:

$$f(Z) = f_{even}(z) + f_{odd}(z),$$

where

$$f_{even}(z) = \frac{f(z) + f(-z)}{2}, \qquad f_{odd}(z) = \frac{f(z) - f(-z)}{2}.$$

Then, since $f_{odd}/\wp'$ is even, we can apply Lemma 2.1.10 to f_{even} and $f_{odd}/\wp'$ to get that f is indeed a rational function of $\wp$ and $\wp'$. □

Next we will return to Theorem 2.1.9 and give a proof using Lemma 2.1.10.

Proof of Theorem 2.1.9: *"(i) $\Longrightarrow$ (ii)"* Let $\wp(\alpha z)$ be a rational function in $\wp(z)$, i.e. there exist polynomials $A(x), B(x) \in \mathbb{C}[x]$ such that

$$B\left(\wp(z)\right)\wp(\alpha z) = A\left(\wp(z)\right). \tag{8}$$

Now, for $n := \deg(B(x))$, $m := \deg(A(x))$ let

$$\begin{cases} B(\wp(z)) = \left(\frac{1}{z^2} + \sum_{w\in L-\{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2}\right)\right)^n + \text{ lower degree terms}, \\ A(\wp(z)) = \left(\frac{1}{z^2} + \sum_{w\in L-\{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2}\right)\right)^m + \text{ lower degree terms}. \end{cases} \tag{9}$$

Substituting these expressions into equation (8) one obtains

$$\frac{1}{\alpha^2 (z^2)^{n+1}} + \cdots = \frac{1}{(z^2)^m} + \ldots, \tag{10}$$

where we ignore the lower degree terms. Since $\wp(z)$ and $\wp(\alpha z)$ have double poles at the origin, we get from equation (10) that

$$\deg(A(x)) = \deg(B(x)) + 1.$$

Let $w \in L$. If w is a pole of $\wp(\alpha z)$, then by (8) $\wp(z)$ has a pole at αw. Since the poles of $\wp(z)$ are exactly the period lattice L, this shows that $\alpha w \in L$. Hence $\alpha L \subset L$.

"(ii) $\Longrightarrow$ (i)" Let $\alpha L \subset L$. Then $\wp(\alpha z)$ is meromorphic and has L as a lattice of periods. Since $\wp(z)$ is an even function, also $\wp(\alpha z)$ is even. Then Lemma 2.1.10 implies that $\wp(\alpha z)$ is a rational function in $\wp(z)$.

"(iii) $\Longrightarrow$ (ii)" This implication is trivial.

"(ii) $\implies$ *(iii)"* Assume that $\alpha L \subset L$. We can assume $L = [1, \tau]$, for some $\tau \in \mathbb{C} - \mathbb{R}$, since we can replace L by λL for a suitable λ. Then $\alpha L \subset L$ means that $\alpha\tau = a + b\tau$ and $\alpha = c + d\tau$ for some $a, b, c, d \in \mathbb{Z}$. Taking the quotient we get

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

which gives the quadratic equation

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

Since $\tau \notin \mathbb{R}$, we must have $b \neq 0$, and thus $K = \mathbb{Q}(\tau)$ is an imaginary quadratic field. Therefore

$$\mathcal{O} = \{\beta \in K : \beta L \subset L\}$$

is an order of K for which L is a proper fractional $\mathcal{O}$-ideal, and since α is already in $\mathcal{O}$, we are done.

For the proof that $N(\alpha) = [L : \alpha L]$, we refer to [C] pg. 210-211. □

Remark 2.1.12. Theorem 2.1.9 tells us that, if an elliptic function has multiplication by some $\alpha \in \mathbb{C} - \mathbb{R}$, then it has multiplication by an entire order $\mathcal{O}$ in an imaginary quadratic field.

Corollary 2.1.13. Let $\mathcal{O}$ be an order in an imaginary quadratic field. Then there exists a one-to-one correspondence between the ideal class group $C(\mathcal{O})$ and the homothety classes of lattices with $\mathcal{O}$ as their full ring of complex multiplications.

Proof: Let $\mathcal{O}$ be an order in an imaginary quadratic field. Let $L \subset \mathbb{C}$ be a lattice which has $\mathcal{O}$ as its full ring of complex multiplication. By Theorem 2.1.9 (iii) L is a proper fractional $\mathcal{O}$-ideal.
Conversely, every proper fractional $\mathcal{O}$-ideal is a lattice with $\mathcal{O}$ as its ring of complex multiplications.
If $\mathfrak{a}, \mathfrak{b}$ are proper fractional $\mathcal{O}$-ideals (for $\mathcal{O}$ an order in an imaginary quadratic field), then $\mathfrak{a}$ and $\mathfrak{b}$ determine the same class in the ideal class group $C(\mathcal{O})$ if and only if they are homothetic as lattices in $\mathbb{C}$. □

If $h(\mathcal{O})$ is the *class number*, then by Corollary 2.1.13 it is equal to the number of homothety classes of lattices having $\mathcal{O}$ as their full ring of complex multiplication.

2.2 A CRASH COURSE IN CLASS FIELD THEORY

The goal of this section is to introduce the necessary tools from class field theory in order to prove that the j-invariant defined in (2.1.7) is an algebraic integer. We advise the reader to look at Appendix 5.2 to recall some useful properties of primes in number fields and ramification. In this section we mainly follow [C] Chapters 5,7,8 and 11, and [J] Chapter IV and V.

Let $\mathcal{O}_K$ be a maximal order in a quadratic field K.

Definition 2.2.1. Let K be a number field. A ***modulus*** of K is given by

$$\mathfrak{m} := \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}, \tag{11}$$

where the product is taken over all primes in K and the following three conditions hold:

(i) $n_{\mathfrak{p}} \geq 0$ and at most finitely many are non-zero,

(ii) $n_{\mathfrak{p}} = 0$ whenever $\mathfrak{p}$ is a complex infinite prime,

(iii) $n_{\mathfrak{p}} \leq 1$ whenever $\mathfrak{p}$ is a real infinite prime.

A modulus $\mathfrak{m}$ may be considered as a product $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ with

$$\mathfrak{m}_0 := \prod_{\mathfrak{p} \text{ finite}} \mathfrak{p}^{n_{\mathfrak{p}}}, \quad \mathfrak{m}_\infty := \prod_{\mathfrak{p} \text{ real}} \mathfrak{p}^{n_{\mathfrak{p}}} \tag{12}$$

We will refer to $\mathfrak{m}_0$ as the ***finite part*** of $\mathfrak{m}$, and $\mathfrak{m}_\infty$ as the ***infinite part*** of $\mathfrak{m}$.

Next, for a given modulus $\mathfrak{m}$, define $\mathcal{I}_K(\mathfrak{m})$ as the set of fractional $\mathcal{O}_K$-ideals relatively prime to $\mathfrak{m}$. Let $\mathcal{P}_{K,1}(\mathfrak{m})$ be a subgroup of $\mathcal{I}_K(\mathfrak{m})$ generated by the principal ideals $\alpha\mathcal{O}_K$, where we take $\alpha \in \mathcal{O}_K$ such that $\alpha \equiv 1 \pmod{\mathfrak{m}_0}$ and such that for every infinite prime σ dividing $\mathfrak{m}_\infty$ we have $\sigma(\alpha) > 0$.
These two groups allow us to introduce ***congruence subgroups***, which are subgroups $H \subset \mathcal{I}_K(\mathfrak{m})$ such that

$$\mathcal{P}_{K,1}(\mathfrak{m}) \subset H \subset \mathcal{I}_K(\mathfrak{m}). \tag{13}$$

Finally, the ***generalised class group*** is defined as:

$$\mathcal{I}_K(\mathfrak{m})/H.$$

Definition 2.2.2 (***Artin symbol***)**.** Let L/K be an Abelian extension $L \supset K$ and $\mathfrak{m}$ a modulus divisible by all ramified primes of L/K. Given a prime $\mathfrak{p}$ not dividing $\mathfrak{m}$, the *Artin symbol*

$$\left[\frac{L/K}{\mathfrak{p}}\right] \in \mathrm{Gal}(L/K)$$

is given by the unique element $\sigma \in \mathrm{Gal}(L/K)$ such that for every $\alpha \in \mathcal{O}_K$ we have

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{p}},$$

and $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$.

The *Artin symbol* allows us to define the ***Artin map***:

$$\varphi_{\mathfrak{m}} : \mathcal{I}_K(\mathfrak{m}) \longrightarrow \mathrm{Gal}(L/K). \tag{14}$$

This map will be useful in the *Existence theorem* (2.2.6), but one has to show that it is a homomorphism. For that we refer to [C] Chapter 5. Then *Artin's reciprocity* theorem ([J] pg. 187, Theorem 5.8) shows that $\mathrm{Gal}(L/K)$ is a generalised ideal class group for certain modulus $\mathfrak{m}$ and that there exists an *isomorphism*:

$$\mathcal{I}_K(\mathfrak{m}) \Big/ \ker(\varphi_{\mathfrak{m}}) \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

We will only give references for this here, namely [J] Chap. V, Section 5.

Next, we want to define the *conductor*. An equivalence class of congruence subgroups is called an ***ideal group***.

Let $\mathbf{H}$ be an ideal group and let $\mathfrak{m}$ be a modulus such that there is some congruence subgroup defined (mod $\mathfrak{m}$) which belongs to $\mathbf{H}$. Then there is only one subgroup in $\mathbf{H}$ defined (mod $\mathfrak{m}$) and we denote it by $\mathbf{H}^{\mathfrak{m}}$.
One can show that whenever $\mathbf{H}^{\mathfrak{m}}$ and $\mathbf{H}^{\mathfrak{n}}$ belong to $\mathbf{H}$, then also $\mathbf{H}^{\gcd(\mathfrak{m},\mathfrak{n})} \in \mathbf{H}$. This tells us that there is a *unique* modulus $\mathfrak{f}$ such that

$$\begin{cases} \mathbf{H}^{\mathfrak{f}} \in \mathbf{H}, \\ \mathbf{H}^{\mathfrak{m}} \in \mathbf{H} \end{cases} \implies \mathfrak{f} \mid \mathfrak{m}, \tag{15}$$

where we take $\mathfrak{f}$ to be the greatest common divisor of all $\mathfrak{m}$ for which H contains a congruence subgroups defined (mod $\mathfrak{m}$). We call the modulus $\mathfrak{f}$ the ***conductor*** of $\mathbf{H}$.

Definition 2.2.3 (**reciprocity law**)**.** Let $\mathfrak{m} = \mathfrak{m}_o\mathfrak{m}_\infty$ be a modulus of a number field K. Let $K_{\mathfrak{m},1}$ be the *ray mod* $\mathfrak{m}$ (see [J] Chap. IV, pg. 137). Also denote by $\varphi_{\mathfrak{m}}$ the Artin map.
We say that the ***reciprocity law*** holds for the triple $(L, K, \mathfrak{m})$ if L is an Abelian extension of K and $\mathfrak{m}$ is a modulus for K such that $\iota(K_{\mathfrak{m},1}) \subset \ker(\varphi_{L/K})$. Here ι sends an element of the group of units of K to the principal ideal it generates in the ring of integers of K.

Definition 2.2.4 (**class field**)**.** Let L be a finite dimensional, Abelian extension of the number field K. Let $\mathbf{H}(L/K)$ be the ideal group consisting of all congruence subgroups $\mathbf{H}^{\mathfrak{m}}(L/K) = \ker(\varphi_{L/K}) \mid \mathcal{I}_K(\mathfrak{m})$, where we let $\varphi_{L/K}$ act on $\mathcal{I}_K(\mathfrak{m})$, with $\mathfrak{m}$ selected so that the reciprocity law holds for $(L, K, \mathfrak{m})$.
We call $\mathbf{H}(L/K)$ the ***class group*** of the extension L of K and L is called the ***class field*** to the ideal group $\mathbf{H}(L/K)$. The conductor of $\mathbf{H}(L/K)$ is denoted by $\mathfrak{f}(L/K)$ and is called the ***conductor of the extension*** L of K.

Theorem 2.2.5. Let $\mathfrak{f}(L/K)$ be the conductor of the Abelian extension L of K. Then $\mathfrak{f}(L/K)$ is divisible by every prime of K that ramifies in L and moreover, the reciprocity law holds for the triple $(L, K, \mathfrak{f}(L/K))$.

Proof: See [J] Chapter V, 11.11 (a).

Proposition 2.2.6. Let $K \subset L$ be an Abelian extension. Let $\mathfrak{m}$ be a modulus of K, and let $\mathbf{H}$ be a congruence subgroup for $\mathfrak{m}$. Then there exists a unique Abelian extension L of K, all of whose ramified primes (finite or infinite), divide $\mathfrak{m}$, such that if

$$\varphi_{\mathfrak{m}} : \mathcal{I}_K(\mathfrak{m}) \longrightarrow \mathrm{Gal}(L/K) \tag{16}$$

is the *Artin map* of $K \subset L$, then

$$\mathbf{H} = \ker(\varphi_{\mathfrak{m}}).$$

Proposition 2.2.6 is a consequence of one of the main theorems in class field theory, namely the *Existence theorem*:

Theorem 2.2.7 (**The existence theorem**)**.** Let K be any algebraic number field. The correspondence

$$L \longrightarrow \mathbf{H}(L/K)$$

is a one-to-one, inclusion preserving, correspondence between finite dimensional, Abelian extensions L of K and ideal groups of K.

As the proof of Theorem 2.2.7 is quite complex and not the main topic of this paper, we omit it here and only give a reference: [J] Chapter V, Theorem 9.9, pg. 215.

Corollary 2.2.8. Let L and M be Abelian extensions of K. Then $L \subset M$ if and only if there is a moduls $\mathfrak{m}$, divisible by all primes of K ramified in either L or M, such that

$$\mathcal{P}_{K,1}(\mathfrak{m}) \subset \ker(\varphi_{M/K,\mathfrak{m}}) \subset \ker(\varphi_{L/K,\mathfrak{m}}). \tag{17}$$

Proof: See [C] pg. 163, Corollary 8.7.

Let $\mathcal{O}$ be an order of conductor $\mathfrak{f}$ in an imaginary quadratic field K. Let $\mathcal{P}_{K,\mathbb{Z}}(\mathfrak{f})$ be the subgroup of $\mathcal{I}_K(\mathfrak{f})$ generated by ideals of the form $\alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}_K$ satisfies $\alpha \equiv a \pmod{\mathfrak{f}}$ for some integer a relatively prime to $\mathfrak{f}$. Then the ideal class group can be written as:

$$C(\mathcal{O}) \simeq \mathcal{I}_K(\mathfrak{f}) \Big/ \mathcal{P}_{K,\mathbb{Z}}(\mathfrak{f}),$$

and moreover one has

$$\mathcal{P}_{K,1}(\mathfrak{f}) \subset \mathcal{P}_{K,\mathbb{Z}}(\mathfrak{f}) \subset \mathcal{I}_K(\mathfrak{f}).$$

By the *Existence theorem* (2.2.6) we know that the above data yields a unique Abelian extension L of K, and we will call that extension the ***ring class field*** of the order $\mathcal{O}$.

The following two theorems will be useful in section 2.3.

Theorem 2.2.9 (***Čebotarev density theorem***)**.** Let L be a Galois extension of K, and let $\langle\sigma\rangle$ be the conjugacy class of an element $\sigma \in \mathrm{Gal}(L/K)$. Then the set

$$\mathcal{S} = \left\{ \mathfrak{p} \in \mathcal{P}_K : \mathfrak{p} \text{ is unramified in L and } \left[\frac{L/K}{\mathfrak{p}}\right] = \langle\sigma\rangle \right\} \tag{18}$$

has Dirichlet density

$$\delta(\mathcal{S}) = \frac{|\langle\sigma\rangle|}{|\mathrm{Gal}(L/K)|} = \frac{|\langle\sigma\rangle|}{[L:K]}.$$

Proof: See [J] Chapter V, Theorem 10.4.

Given two sets M and L, we say that $M \dot{\subset} L$ is $M \subset L \cup \Sigma$ for some finite set Σ. Similarly, we say that $L \doteq M$ if both $L \dot{\subset} M$ and $M \dot{\subset} L$. Also, given a finite extension $K \subset L$, we set

$$\mathcal{S}_{L/K} = \{\mathfrak{p} \in \mathcal{P}_K : \mathfrak{p} \text{ splits completely in } L\}.$$

Proposition 2.2.10. Let L and M be finite extensions of K.

(i) If M is Galois over K, then $L \subset M \iff \mathcal{S}_{M/K} \dot{\subset} \mathcal{S}_{L/K}$.

(ii) If L is Galois over K, then $L \subset M \iff \tilde{\mathcal{S}}_{M/K} \dot{\subset} \mathcal{S}_{L/K}$, where $\tilde{\mathcal{S}}_{M/K}$ is defined by

$$\tilde{\mathcal{S}}_{M/K} := \left\{ \mathfrak{p} \in \mathcal{P}_K : \mathfrak{p} \text{ unramified in } M, \mathfrak{f}_{\mathfrak{b}|\mathfrak{p}} = 1 \text{ for some prime } \mathfrak{b} \text{ of } M \right\}.$$

Proof: Let's start with (ii). Let $L \subset M$. Since L is Galois over M we have that $\tilde{\mathcal{S}}_{L/K} = \mathcal{S}_{L/K}$. Then the two sets $\tilde{\mathcal{S}}_{M/K}$ and $\tilde{\mathcal{S}}_{L/K}$ differ by the set of $\mathfrak{p} \in \mathcal{P}_K$ that

are unramified in M but not in L. Hence $\tilde{\mathcal{S}}_{M/K} \dot{\subset} \mathcal{S}_{L/K}$.
Conversely, assume that $\tilde{\mathcal{S}}_{M/K} \dot{\subset} \mathcal{S}_{L/K}$, and let N be a Galois extension of K containing both L and M. By Galois theory, it suffices to show that $\mathrm{Gal}(N/M) \subset \mathrm{Gal}(N/L)$. Thus, given $\sigma \in \mathrm{Gal}(N/M)$, we have to prove that $\sigma|_L$ is the identity.
By Čebotarev's density theorem 2.2.9 there exists a prime $\mathfrak{p}$ in K, unramified in N, such that $[(N/K)/\mathfrak{p}]$ is the conjugacy class of σ. Thus, there is some prime $\mathfrak{b}$ of N containing $\mathfrak{p}$ such that $[(N/K)/\mathfrak{b}] = \sigma$.
Claim: $\mathfrak{p} \in \tilde{\mathcal{S}}_{M/K}$.
Let $\mathfrak{b}' := \mathfrak{b} \cap \mathcal{O}_M$. Then for $\alpha \in \mathcal{O}_M$ one has

$$\alpha \equiv \sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{b}'}.$$

The first congruence follows from $\sigma|_M = 1$, and the second follows by the definition of the Artin symbol. Thus $\mathcal{O}_M/\mathfrak{b}' \simeq \mathcal{O}_K/\mathfrak{p}$, so that $\mathfrak{f}_{\mathfrak{b}'|\mathfrak{p}} = 1$. This shows that $\mathfrak{p} \in \tilde{\mathcal{S}}_{M/K}$.

Čebotarev's theorem implies that there are infinitely many such $\mathfrak{p}$'s. Thus the hypothesis $\tilde{\mathcal{S}}_{M/K} \dot{\subset} \mathcal{S}_{L/K}$ allows us to assume that $\mathfrak{p} \in \mathcal{S}_{L/K}$, i.e.

$$\left[\frac{L/K}{\mathfrak{p}}\right] = 1.$$

Now, since

$$\left[\frac{L/K}{\mathfrak{p}}\right] = \left[\frac{N/K}{\mathfrak{b}}\right]\Big|_L,$$

and $\sigma = ((N/K)/\mathfrak{b})$, we conclude that $\sigma|_L = 1$, as desired.

Now we turn our attention to part (i). Using a similar argument as before one can see that $L \subset M$ implies $\mathcal{S}_{M/L} \dot{\subset} \mathcal{S}_{L/K}$. To prove the other direction, let L' be the Galois closure of L over K. It is a standard fact that a prime of K splits completely in L if and only if it splits completely in L'.
This implies that $\mathcal{S}_{L/K} = \mathcal{S}_{L'/K}$. Since M is Galois over K, and we already have seen that $\tilde{\mathcal{S}}_{M/K} = \mathcal{S}_{M/K}$. Thus we can rewrite our hypothesis $\mathcal{S}_{M/K} \dot{\subset} \mathcal{S}_{L/K}$ as $\tilde{\mathcal{S}}_{M/K} \dot{\subset} \mathcal{S}_{L'/K}$. Then by part (ii) we get $L' \subset M$, which implies $L \subset M$. □

Next, we will give a couple of useful properties about ring class fields.

Lemma 2.2.11. Let L be the ring class field of an order $\mathcal{O}$ in an imaginary quadratic field K. Then L is a Galois extension of $\mathbb{Q}$, and its Galois group can be written as a semidirect product

$$\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{Gal}(L/K) \rtimes (\mathbb{Z}/2\mathbb{Z})$$

where the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$ acts on $\mathrm{Gal}(L/K)$ by sending σ to its inverse σ^{-1}.

Proof: See [C] Lemma 9.3.

Proposition 2.2.12. Let $n \in \mathbb{N}$, and let L be the ring class field of the order $\mathbb{Z}[\sqrt{-n}]$ in the imaginaty quadratic field $K = \mathbb{Q}(\sqrt{-n})$. If p is an odd prime not dividing n, then

$$p = x^2 + ny^2 \iff p \text{ splits completely in } L.$$

Proof: See [C] Theorem 9.4.

2.3 The j-invariant is an algebraic integer

The goal of this section is to prove that the j-invariant defined in (2.1.7) is an algebraic integer. In this section we will mainly follow [C] Chapter 8 and 11.

We start by giving a few useful properties of the j-invariant. The proof of these can be found in [C] Chapter 11. First, recall that for $\tau \in \mathcal{H}$ we define a lattice as $[1, \tau]$ and subsequently the j-function is given by $j(\tau) = j([1, \tau])$.

Theorem 2.3.1. Let $\tau \in \mathcal{H}$. Then the following statements hold:

(i) $j(\tau)$ is a holomorphic function on $\mathcal{H}$,

(ii) if $\tau, \tau' \in \mathcal{H}$, then $j(\tau) = j(\tau')$ if and only if $\tau' = \gamma\tau$ for some $\gamma \in \mathrm{SL}(2, \mathbb{Z})$; in particular $j(\tau)$ is $\mathrm{SL}(2, \mathbb{Z})$-invariant,

(iii) $j : \mathcal{H} \longrightarrow \mathbb{C}$ is surjective,

(iv) for $\tau \in \mathcal{H}$ one has $j'(\tau) \neq 0$, except in the following cases:

(a) $\tau = \gamma i$, $\gamma \in \mathrm{SL}(2, \mathbb{Z})$, where $j'(\tau) = 0$ but $j''(\tau) \neq 0$,

(b) $\tau = \gamma\omega$, $\omega = e^{2\pi i/3}$, $\gamma \in \mathrm{SL}(2, \mathbb{Z})$, where $j'(\tau) = j''(\tau) = 0$ but $j'''(\tau) \neq 0$.

Moreover, one can show that the *q-expansion* of $j(\tau)$ is given by

$$\begin{aligned} j(\tau) &= \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 \dots \\ &= \frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n, \end{aligned}$$

where $q := q(\tau) = e^{2\pi i\tau}$, $c_n \in \mathbb{Z}$ for all $n \geq 0$.

The q-expansion of $j(\tau)$ actually gives us another useful property of the j-invariant, namely that $j(\tau)$ is *meromorphic at infinity*. This means that its Fourier expansion has only finitely many non-zero coefficients for negative exponents. This shows that $j(\tau)$ is a *modular function* for $\Gamma_0(m), m \in \mathbb{N}$, where:

Definition 2.3.2 (***modular function***)**.** For $m \in \mathbb{N}$ let

$$\Gamma_0(m) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}) : c \equiv 0 \pmod{m} \right\}. \tag{19}$$

A complex-valued function $f(\tau)$ defined on the upper-half plane $\mathcal{H}$, except for isolated singularities, is called a ***modular function for*** $\Gamma_0(m)$ if the following hold:

(i) $f(\tau)$ is meromorphic on $\mathcal{H}$,

(ii) $f(\tau) = f(\gamma\tau)$, for all $\tau \in \mathcal{H}$, $\gamma \in \Gamma_0(m)$,

(iii) $f(\tau)$ is meromorphic at ∞, $\forall \gamma \in \mathrm{SL}(2, \mathbb{Z})$.

Remark 2.3.3. We say that $f(\tau)$ is ***holomorphic at*** ∞ if its q-expansion has only non-negative powers of q.

Note that $j(\tau)$ satisfies conditions (i) and (ii) by Theorem 2.3.1.
The j-invariant has an even stronger connection to general modular functions for

both $\mathrm{SL}(2,\mathbb{Z})$ and $\Gamma_0(m)$. Namely, its the main building block for constructing all modular functions:

Theorem 2.3.4. Let $m \in \mathbb{N}$. Then

(i) $j(\tau)$ is a modular function for $\mathrm{SL}(2,\mathbb{Z})$, and every modular function for $\mathrm{SL}(2,\mathbb{Z})$ is a rational function in $j(\tau)$,

(ii) $j(\tau)$ and $j(m\tau)$ are modular functions for $\Gamma_0(m)$, and every modular function for $\Gamma_0(m)$ is a rational function of $j(\tau)$ ad $j(m\tau)$.

Proof: (We follow [C] Proof of Theorem 11.9.) We start by proving the following lemma:

Lemma 2.3.5. The following two statements hold:

(i) A holomorphic modular function for $\mathrm{SL}(2,\mathbb{Z})$ which is holomorphic at ∞ is constant.

(ii) A holomorphic modular function for $\mathrm{SL}(2,\mathbb{Z})$ is a polynomial in $j(\tau)$.

Proof: Part (i). Let $f(\tau)$ be a modular function as in as in part (i) of the Lemma. Since $f(\tau)$ is holomorphic at ∞, we know that $f(\infty) = \lim_{\mathrm{Im}(\tau)\to\infty} f(\tau)$ exists as a complex number. We will show that $f(\mathcal{H} \cup \{\infty\})$ is compact. By the maximum modulus principle, this will imply that $f(\tau)$ is constant.
Let $f(\tau_k)$ be a sequence of points in the image. We want to find a subsequence that converges to a point of the form $f(\tau)$ for some $\tau \in \mathcal{H}$. Since $f(\tau)$ is $\mathrm{SL}(2,\mathbb{Z})$-invariant, we can assume that the τ_k 's lie in the region

$$R = \{\tau \in \mathcal{H} : |\mathrm{Re}(\tau)| \leq 1/2, |\mathrm{Im}(\tau)| \geq 1/2\}.$$

If the imaginary parts of the τ_k 's are unbounded, then by the above limit, a subsequence converges to $f(\infty)$. If the imaginary parts are bounded, then the τ_k 's lie in a compact subset of $\mathcal{H}$, and the desired subsequence is easily found. This proves (i).

Part (ii). Let $f(\tau)$ be a holomorphic modular function for $\mathrm{SL}(2,\mathbb{Z})$. Its q-expansion has only finitely many terms with negative powers of q. Since the q-expansion of $j(\tau)$ begins with $1/q$, one can find a polynomial $A(x)$ such that $f(\tau) - A(j(\tau))$ is holomorphic at ∞. Since it is also holomorphic on $\mathcal{H}$, it is constant by (i). Hence $f(\tau)$ is a polynomial in $j(\tau)$. □

We return to Theorem 2.3.4. Now, let $f(\tau)$ be an arbitrary modular function for $\mathrm{SL}(2,\mathbf{Z})$, possibly with poles on $\mathcal{H}$. If we can find a polynomial $B(x)$ such that $B(j(\tau))f(\tau)$ is holomorphic on $\mathcal{H}$, then the lemma above will imply that $f(\tau)$ is a rational function in $j(\tau)$. Since $f(\tau)$ has a meromorphic q-expansion, it follows that $f(\tau)$ has only finitely many poles in the region

$$R = \{\tau \in \mathcal{H} : |\mathrm{Re}(\tau)| \leq 1/2, |\mathrm{Im}(\tau)| \geq 1/2\},$$

and since $f(\tau)$ is $\mathrm{SL}(2,\mathbb{Z})$-invariant, Lemma 11.4 implies that every pole of $f(\tau)$ is $\mathrm{SL}(\ 2,\mathbb{Z})$-equivalent to one in R. Thus, if $B(j(\tau))f(\tau)$ has no poles in R, then it is holomorphic on the upper half-plane.
So, suppose that $f(\tau)$ has a pole of order m at $\tau_0 \in R$. If $j'(\tau_0) \neq 0$, then $(j(\tau) - j(\tau_0))^m f(\tau)$ is holomorphic at τ_0. In this way we can find a polynomial $B(x)$ such that $B(j(\tau))f(\tau)$ has no poles in R, except possibly for those where

$j'(\tau_0) = 0$. When this is the case, by Theorem 2.3.1 we can assume that $\tau_0 = i$ or $\omega = e^{2\pi i/3}$.
When $\tau_0 = i$, we claim that m is even. To see this, note that in a neighborhood of i, $f(\tau)$ can be written in the form

$$f(\tau) = \frac{g(\tau)}{(\tau - i)^m}$$

where $g(\tau)$ is holomorphic and $g(i) \neq 0$. Now $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$ fixes i, so that

$$f(\tau) = f(-1/\tau) = \frac{g(-1/\tau)}{(-1/\tau - i)^m}.$$

Comparing these two expressions for $f(\tau)$, we get

$$g(-1/\tau) = \frac{1}{(i\tau)^m} g(\tau)$$

Setting $\tau = i$ implies that $g(i) = (-1)^m g(i)$, and since $g(i) \neq 0$, it follows that m is even. By Theorem 2.3.1, $j(\tau) - 1728$ has a zero of order 2 at i, and hence $(j(\tau) - 1728)^{m/2} f(\tau)$ is holomorphic at i. The argument for $\tau_0 = \omega$ is similar and will be avoided here. This completes the proof of part (i) of Theorem 2.3.4.

Next, we turn to part (ii). We will assume that $j(\tau)$ and $j(m\tau)$ are both modular functions for $\Gamma_0(m)$. For the proof of that fact, we refer to [C] Chapter 11, pg. 228.

Next we will study the following set of matrices

$$C(m) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = m, a > 0, 0 \leq b < d, \gcd(a, b, d) = 1 \right\}.$$

The matrix $\sigma_0 = \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} \in C(m)$ has two properties of interest: first, $\sigma_0 \tau = m\tau$, and second,

$$\Gamma_0(m) = \left(\sigma_0^{-1} \mathrm{SL}(2, \mathbb{Z}) \sigma_0\right) \cap \mathrm{SL}(2, \mathbb{Z}).$$

For the number of elements in $C(m)$ one can compute the formula:

$$|C(m)| = m \prod_{p|m} \left(1 + \frac{1}{p}\right). \tag{20}$$

Note that these two properties account for the $\Gamma_0(m)$ invariance of $j(m\tau)$ proved above. More generally, we have the following lemma:

Lemma 2.3.6. For $\sigma \in C(m)$, the set

$$\left(\sigma_0^{-1} \mathrm{SL}(2, \mathbb{Z}) \sigma\right) \cap \mathrm{SL}(2, \mathbb{Z})$$

is a right coset of $\Gamma_0(m)$ in $\mathrm{SL}(2, \mathbb{Z})$. This induces a one-to-one correspondence between right cosets of $\Gamma_0(m)$ and elements of $C(m)$.

This lemma implies that $[\mathrm{SL}(2, \mathbb{Z}) : \Gamma_0(m)] = |C(m)|$. By equation (20) the in-

dex of $\Gamma_0(m)$ is $\mathrm{SL}(2,\mathbb{Z})$ is $m\prod_{p|m}(1+1/p)$.

We can now compute some q-expansions. Fix $\gamma \in \mathrm{SL}(2,\mathbb{Z})$, and choose $\sigma \in C(m)$ so that γ lies in the right coset corresponding to σ in Lemma 2.3.6. This means that $\sigma_0\gamma = \tilde{\gamma}\sigma$ for some $\bar{\gamma} \in \mathrm{SL}(2,\mathbb{Z})$, and hence $j(m\gamma\tau) = j(\sigma_0\gamma\tau) = j(\tilde{\gamma}\sigma\tau) = j(\sigma\tau)$ since $j(\tau)$ is $\mathrm{SL}(2,\mathbb{Z})$-invariant. Hence

$$j(m\gamma\tau) = j(\sigma\tau) \tag{21}$$

Suppose that $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. The q-expansion of $j(\tau)$ is

$$j(\tau) = \frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n, \quad c_n \in \mathbb{Z},$$

and since $\sigma\tau = (a\tau + b)/d$, it follows that

$$q(\sigma\tau) = e^{2\pi i(a\tau+b)/d} = e^{2\pi ib/d} q^{a/d}.$$

If we set $\zeta_m = e^{2\pi i/m}$, we can write this as

$$q(\sigma\tau) = \zeta_m^{ab} \left(q^{1/m}\right)^{a^2}$$

since $ad = m$. This gives us the q-expansion

$$j(m\gamma\tau) = j(\sigma\tau) = \frac{\zeta_m^{-ab}}{\left(q^{1/m}\right)^{a^2}} + \sum_{n=0}^{\infty} c_n \zeta_m^{abn} \left(q^{1/m}\right)^{a^2 n}, \quad c_n \in \mathbb{Z}. \tag{22}$$

Next, we want to introduce the *modular equation* $\Phi_m(X,Y)$. Let the right cosets of $\Gamma_0(m)$ in $\mathrm{SL}(2,\mathbb{Z})$ be $\Gamma_0(m)\gamma_i, i = 1,\ldots,|C(m)|$. Then consider the polynomial in the variable X

$$\Phi_m(X,\tau) = \prod_{i=1}^{|C(m)|} \left(X - j\left(m\gamma_i\tau\right)\right)$$

We will prove that this expression is a polynomial in X and $j(\tau)$. To see this, consider the coefficients of $\Phi_m(X,\tau)$. Being symmetric polynomials in the $j\left(m\gamma_i\tau\right)$'s, they are also holomorphic. To check invariance under $\mathrm{SL}(2,\mathbb{Z})$, pick $\gamma \in \mathrm{SL}(2,\mathbb{Z})$. Then the cosets $\Gamma_0(m)\gamma_i\gamma$ are a permutation of the $\Gamma_0(m)\gamma_i$'s, and since $j(m\tau)$ is invariant under $\Gamma_0(m)$, the $j\left(m\gamma_i\gamma\tau\right)$'s are a permutation of the $j\left(m\gamma_i\tau\right)$'s. This shows that the coefficients of $\Phi_m(X,\tau)$ are invariant under $\mathrm{SL}(2,\mathbb{Z})$.
Next, we will show that the coefficients are meromorphic at infinity. Rather than expanding in powers of q, it suffices to expand in terms of $q^{1/m} = e^{2\pi i\tau/m}$ and show that only finitely many negative exponents appear.
By (21), we know that $j\left(m\gamma_i\tau\right) = j(\sigma\tau)$ for some $\sigma \in C(m)$, and then (22) shows that the q-expansion for $j\left(m\gamma_i\tau\right)$ has only finitely many negative exponents. Since the coefficients are polynomials in the $j\left(m\gamma_i\tau\right)$'s, they clearly are meromorphic at the cusps.
This shows that the coefficients of $\Phi_m(X,\tau)$ are holomorphic modular functions, and thus, by Lemma 2.3.5, they are polynomials in $j(\tau)$. This means that there is a polynomial

$$\Phi_m(X,Y) \in \mathbb{C}[X,Y]$$

such that

$$\Phi_m(X, j(\tau)) = \prod_{i=1}^{|C(m)|} (X - j(m\gamma_i\tau)).$$

The equation $\Phi_m(X, Y) = 0$ is called the ***modular equation*** or ***modular polynomial***. Using some simple field theory, it can be proved that $\Phi_m(X, Y)$ is irreducible as a polynomial in X.

By (21), each $j(m\gamma_i\tau)$ can be written as $j(\sigma\tau)$ for a unique $\sigma \in C(m)$. Thus we can also express the modular equation in the form

$$\Phi_m(X, j(\tau)) = \prod_{\sigma \in C(m)} (X - j(\sigma\tau)). \tag{23}$$

Note that $j(m\tau)$ is always one of the $j(\sigma\tau)$'s since $\begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} \in C(m)$. Hence $\Phi_m(j(m\tau), j(\tau)) = 0$, and the degree of $\Phi_m(X, Y)$ in X is $|C(m)|$.

Next, let $f(\tau)$ be an arbitrary modular function for $\Gamma_0(m)$. To prove that $f(\tau)$ is a rational function in $j(\tau)$ and $j(m\tau)$, consider the function

$$\begin{aligned} G(X, \tau) &= \Phi_m(X, j(\tau)) \sum_{i=1}^{|C(m)|} \frac{f(\gamma_i\tau)}{X - j(m\gamma_i\tau)} \\ &= \sum_{i=1}^{|C(m)|} f(\gamma_i\tau) \prod_{j \neq i} (X - j(m\gamma_j\tau)). \end{aligned} \tag{24}$$

This is a polynomial in X, and one can show that its coefficients are modular functions for $\mathrm{SL}(2, \mathbb{Z})$ (see [C] Chap. 11). Once the coefficients are modular functions for $\mathrm{SL}(2, \mathbb{Z})$, they are rational functions of $j(\tau)$ by what we proved above. Hence $G(X, \tau)$ is a polynomial $G(X, j(\tau)) \in \mathbb{C}(j(\tau))[X]$.

We can assume that γ_1 is the identity matrix. By the product rule, we obtain

$$\frac{\partial \Phi_m}{\partial X}(j(m\tau), j(\tau)) = \prod_{j \neq 1} (j(m\tau) - j(m\gamma_j\tau)).$$

Thus, substituting $X = j(m\tau)$ in (24) gives

$$G(j(m\tau), j(\tau)) = f(\tau) \frac{\partial \Phi_m}{\partial X}(j(m\tau), j(\tau))$$

Now $\Phi_m(X, j(\tau))$ is irreducible and hence separable, so that

$$\frac{\partial}{\partial X} \Phi_m(j(m\tau), j(\tau)) \neq 0.$$

Thus we can write

$$f(\tau) = \frac{G(j(m\tau), j(\tau))}{\frac{\partial \Phi_m}{\partial X}(j(m\tau), j(\tau))},$$

which proves that $f(\tau)$ is a rational function in $j(\tau)$ and $j(m\tau)$. □

Theorem 2.3.7. Let $m \in \mathbb{N}$. Then:

(i) $\Phi_m(X,Y) \in \mathbb{Z}[X,Y]$,

(ii) $\Phi_m(X,Y)$ is irreducible when regarded as a polynomial in X,

(iii) $\Phi_m(X,Y) = \Phi_m(Y,X)$ if $m > 1$,

(iv) if m is not a perfect square, then $\Phi_m(X,Y)$ is a polynomial of degree > 1 whose leading coefficient is ± 1,

(v) if m is a prime p, then $\Phi_p(X,Y) \equiv (X^p - Y)(X - Y^p) \bmod p\mathbb{Z}[X,Y]$.

Proof: See [C] Theorem 11.18.

Lemma 2.3.8. If m is a perfect square, then $\Phi_1(X,Y)$ divides $\Phi_m(X,Y)$.

Proof: Let m be a perfect square. Then $\tilde{\sigma} := \begin{pmatrix} \sqrt{m} & \\ & \sqrt{m} \end{pmatrix} \in C(m)$ and

$$(X - j(\tilde{\sigma}\tau)) \;\Big|\; \prod_{M \in C(m)} (X - j(\sigma\tau)) = \Phi_m(X, j(\tau)).$$

Since $j(\tilde{\sigma}\tau) = j(\tau)$, we get that $\Phi_1(X,Y) = X - Y$ divides $\Phi_m(X,Y)$. □

Proposition 2.3.9. Let $m \in \mathbb{N}$. If $u, v \in \mathbb{C}$, then $\Phi_m(u,v) = 0$ is and only if there is a lattice L and a cyclic sublattice $L' \subset L$ of index m such that $u = j(L')$ and $v = j(L)$.

Proof: See [C] Theorem 11.23.

Theorem 2.3.10 (***j-invariant is an algebraic integer***)**.** Let $\mathcal{O}$ be an order in an imaginary quadratic field K and $\mathfrak{a}$ a proper fractional $\mathcal{O}$-ideal. Then $j(\mathfrak{a})$ is an algebraic integer and $K(j(\mathfrak{a}))$ is the ring class field of the order $\mathcal{O}$.

Proof: Let $\mathcal{O}$ be an order in an imaginary quadratic field. Let $\alpha \in \mathcal{O}$ be primitive. Then $\alpha\mathcal{O}$ is primitive as an ideal and $N(\alpha) = N(\alpha\mathcal{O})$.
By looking at the exact sequence

$$0 \longrightarrow \mathfrak{a}/\alpha\mathfrak{a} \longrightarrow \mathcal{O}/\alpha\mathfrak{a} \longrightarrow \mathcal{O}/\alpha\mathcal{O} \longrightarrow 0$$

we get

$$[\mathfrak{a} : \alpha\mathfrak{a}]N(\mathfrak{a}) = N(\alpha\mathfrak{a}) = N(\alpha\mathcal{O})N(\mathfrak{a}).$$

Thus $N(\alpha) = [\mathfrak{a} : \alpha\mathfrak{a}]$.
Then $\alpha\mathfrak{a}$ is a cyclic sublattice of $\mathfrak{a}$ of index $m := N(\alpha)$. By Theorem 2.3.9 we know that

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

since $j(\alpha\mathfrak{a}) = j(\mathfrak{a})$. Thus $j(\mathfrak{a})$ is a root of the polynomial $\Phi_m(X,X)$. Since $\Phi_m(X,Y)$ has integer coefficients (by 2.3.7), this shows that $j(\mathfrak{a})$ is an algebraic number. Moreover, if we choose α such that $m = N(\alpha)$ is not a perfect square, then the leading coefficient of $\Phi_m(X,Y)$ is ± 1 (again by 2.3.7). Thus $j(\mathfrak{a})$ will be an algebraic integer. By Lemma 5.1.3 $\mathcal{O} = [1, \mathfrak{f}w_K]$ and $w_K = (d_K + \sqrt{d_K})/2$. Then $\alpha = \mathfrak{f}w_K$ is primitive in $\mathcal{O}$, and one can compute that the norm $N(\alpha)$ is not a perfect square.

Let L denote the ring class field of $\mathcal{O}$. We want to show that $L = K(j(\mathfrak{a}))$.
Let $\mathcal{S}_{L/\mathbb{Q}}$ be the set of primes that split completely in L.
Claim:

$$\mathcal{S}_{L/\mathbb{Q}} \doteq \{p \text{ prime } \mid p = N(\alpha), \text{ for some } \alpha \in \mathcal{O}\}. \tag{25}$$

Assume $D \equiv 0 \pmod 4$, then $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ for some $n \in \mathbb{N}$. Thus $N(\alpha) = N(x + y\sqrt{-n}) = x^2 + ny^2$, so that (25) says, with finitely many exceptions, that the primes splitting completely in L are those represented by $x^2 + ny^2$. We have seen that in Proposition 2.2.12. Similarly one can prove the case when $D \equiv 1 \pmod 4$, but for the details we only reference [C] Section 11. This shows (25).

Let $M = K(j(\mathfrak{a}))$. By Lemma 2.2.11 L is Galois over $\mathbb{Q}$. Then by Proposition 2.2.10

$$M \subset L \quad \Longleftrightarrow \quad \mathcal{S}_{L/\mathbb{Q}} \dot{\subset} \mathcal{S}_{M/\mathbb{Q}}.$$

Let $p \in \mathcal{S}_{L/\mathbb{Q}}$ be such that p is unramified in M. By (25) $p = N(\alpha)$ for some $\alpha \in \mathcal{O}$. Then $\alpha\mathfrak{a} \subset \mathfrak{a}$ is a sublattice of index $N(\alpha) = p$, and it is cyclic since p is prime. Thus

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

Using part (v) of Theorem (2.3.7), this implies that

$$0 = \Phi_p(j(\mathfrak{a}), j(\mathfrak{a})) = -(j(\mathfrak{a})^p - j(\mathfrak{a}))^2 + p\beta,$$

for some $\beta \in \mathcal{O}_M$.
Let $\mathfrak{b}$ be any prime of M containing p. The above equation implies that

$$j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \pmod{\mathfrak{b}}. \tag{26}$$

Since $M = K(j(\mathfrak{a}))$ one can show that $\mathcal{O}_K[j(\mathfrak{a})] \subset \mathcal{O}_M$ has finite index.

Next, we claim: If p does not divide $[\mathcal{O}_M : \mathcal{O}_K[j(\mathfrak{a})]]$, then equation (26) implies that $\alpha^p \equiv \alpha \pmod{\mathfrak{b}}$ for all $\alpha \in \mathcal{O}_M$.
To prove the claim, first note that p splits completely in L, so that it splits completely in K, and hence $p \in \mathfrak{p} \subset \mathfrak{b}$ for some ideal $\mathfrak{p}$ of norm p. This implies that $\alpha^p \equiv \alpha \pmod{\mathfrak{b}}$ holds for all $\alpha \in \mathcal{O}_K$. Subsequently, the congruence holds for all $\alpha \in \mathcal{O}_K[j(\mathfrak{a})]$ by (26). Thus the claim follows.

From the claim above we get that $\mathfrak{f}_{\mathfrak{b}|p} = 1$, and since this holds for any $\mathfrak{b}$ containing p, we get that p splits completely in M. This shows that $\mathcal{S}_{L/\mathbb{Q}} \dot{\subset} \mathcal{S}_{M/\mathbb{Q}}$, and finally $M \subset L$. The inclusion $M = K(j(\mathfrak{a})) \subset L$ shows that the ring class field L contains the j-invariants of all proper fractional $\mathcal{O}$-ideals. Let $h = h(\mathcal{O})$, and let $\mathfrak{a}_i, \quad i = 1, \ldots, h$ be class representatives for $C(\mathcal{O})$. It follows that any $j(\mathfrak{a})$ equals one of $j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_h)$ and furthermore they are distinct.
Thus

$$\Delta = \prod_{i<j} (j(\mathfrak{a}_i) - j(\mathfrak{a}_j)) \tag{27}$$

is a nonzero element of $\mathcal{O}_L$.

To prove the opposite inclusion $L \subset M$, we will use the criterion $\tilde{\mathcal{S}}_{M/\mathbb{Q}} \dot{\subset} \mathcal{S}_{L/K}$ from part (ii) of Proposition 2.2.10. Let $p \in \tilde{\mathcal{S}}_{M/\mathbb{Q}}$. Then p is unramified in M and $\mathfrak{f}_{\mathfrak{b}|p} = 1$ for some prime $\mathfrak{b}$ of M containing p. This implies that p splits completely in K, and thus there exists a prime ideal $\mathfrak{p} \in \mathcal{O}$ with $p = N(\mathfrak{p})$. We can assume that $\mathfrak{p}$ does not divide $\mathfrak{f}$ (this excludes finitely many primes). Since $\mathcal{O}/\mathfrak{p} \cap \mathcal{O}$ injects into $\mathcal{O}_K/\mathfrak{p}$ and $N(\mathfrak{p})$ is prime to $\mathfrak{f}$, so is $N(\mathfrak{p} \cap \mathcal{O})$, which proves that $\mathfrak{p} \cap \mathcal{O}$ is prime to

$\mathfrak{f}$. Now, consider the natural map

$$\mathcal{O}/\mathfrak{p}\cap\mathcal{O} \longrightarrow \mathcal{O}_K/\mathfrak{p}.$$

It is injective, and since $\mathfrak{p}$ is prime to $\mathfrak{f}$, multiplication by $\mathfrak{f}$ induces an isomorphism of $\mathcal{O}_K/\mathfrak{p}$. But $\mathfrak{f}\mathcal{O}_K \subset \mathcal{O}$, and surjectivity follows. Hence

$$p = N(\mathfrak{p}\cap\mathcal{O}).$$

If we can show that $\mathfrak{p}\cap\mathcal{O}$ is a principal ideal $\alpha\mathcal{O}$, then $p = N(\alpha)$ implies that $p \in \mathcal{S}_{L/\mathbb{Q}}$ by (25). We may assume that p is relatively prime to the element Δ of (27).
Let $\mathfrak{a}' := (\mathfrak{p}\cap\mathcal{O})\mathfrak{a}$. Since $\mathfrak{p}\cap\mathcal{O}$ has norm p, $\mathfrak{a}' \subset \mathfrak{a}$ is a sublattice of index p, and it is cyclic since p is prime. Thus $\Phi_p(j(\mathfrak{a}'), j(\mathfrak{a})) = 0$. Using Theorem 2.3.7 (v) one rewrite this a

$$0 = \Phi_p(j(\mathfrak{a}'), j(\mathfrak{a})) = (j(\mathfrak{a}')^p - j(\mathfrak{a}))(j(\mathfrak{a}') - j(\mathfrak{a})^p) + pQ(j(\mathfrak{a}'), j(\mathfrak{a})),$$

for some polynomial $Q(X, Y) \in \mathbb{Z}[X, Y]$. Let $\tilde{\mathfrak{b}}$ be a prime of L containing $\mathfrak{b}$. Since $j(\mathfrak{a}')$ and $j(\mathfrak{a})$ are algebraic integers lying in L, the above equation implies that $pQ(j(\mathfrak{a}'), j(\mathfrak{a})) \in \tilde{\mathfrak{b}}$. Hence

$$j(\mathfrak{a}')^p \equiv j(\mathfrak{a}) \pmod{\tilde{\mathfrak{b}}} \qquad \text{or} \qquad j(\mathfrak{a})^p \equiv j(\mathfrak{a}') \pmod{\tilde{\mathfrak{b}}}. \tag{28}$$

However, we also know $\mathfrak{f}_{\mathfrak{b}|p} = 1$, which shows that $j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \pmod{\tilde{\mathfrak{b}}}$, and since $\mathfrak{b} \subset \tilde{\mathfrak{b}}$, we obtain

$$j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \pmod{\tilde{\mathfrak{b}}}. \tag{29}$$

Finally, (28) and (29) imply

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

If $\mathfrak{a}$ and $\mathfrak{a}'$ lay in distinct ideal classes of $C(\mathcal{O})$, then $j(\mathfrak{a}) - j(\mathfrak{a}')$ would be one of the factors of Δ from (27), and p and Δ would not be relatively prime. This is a contradiction to our choice of p, so that $\mathfrak{a}$ and $\mathfrak{a}' = (\mathfrak{p}\cap\mathcal{O})\mathfrak{a}$ must lie in the same ideal class in $C(\mathcal{O})$. This forces $\mathfrak{p}\cap\mathcal{O}$ to be a principal ideal, which (as showed above) implies $p \in \mathcal{S}_{L/\mathbb{Q}}$. Thus $\tilde{\mathcal{S}}_{M/\mathbb{Q}} \dot{\subset} \mathcal{S}_{L/\mathbb{Q}}$, which completes the proof that $L = M$. □

Definition 2.3.11 (***singular modulus***)**.** The j-invariant $j(L)$ of a lattice with complex multiplication is called a ***singular j-invariant*** or a ***singular modulus***.

3 Modular forms of half-integral weight

The aim of the next section section is to briefly recall the theory of modular forms of half-integral weight and introduce the operator U_4. Here we mainly rely on [K], [KH], [Kohl] and [AL].

We start by recalling the definition of the Jacobi theta function

$$\theta(z) = \sum_{n\in\mathbb{Z}} q^{n^2}, \quad q = e^{2\pi i z},$$

for $z \in \mathcal{H}$.

Definition 3.0.1. For $z \in \mathcal{H}, k \in \mathbb{N}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4)$ the ***automorphy factor*** $J(\gamma, z)$ is given by $j(\gamma, z)^k$, where

$$j(\gamma, z) := \frac{\theta(\gamma z)}{\theta(z)}.$$

Remark 3.0.2. For $\left(\frac{c}{d}\right)$ the Legendre symbol and

$$\epsilon_d = \sqrt{\left(\frac{-1}{d}\right)} = \begin{cases} 1, & d \equiv 1 \pmod 4 \\ i, & d \equiv 3 \pmod 4 \end{cases} \tag{30}$$

one has

$$j(\gamma, z) = \frac{\theta(\gamma z)}{\theta(z)} = \left(\frac{c}{d}\right) \epsilon_d^{-1} \sqrt{cz + d}.$$

Note that we take the branch of the square-root $\sqrt{z}$ with argument in $\left(\frac{-\pi}{2}, \frac{\pi}{2}\right]$. Then for any $k \in \mathbb{Z}$ we define $z^{\frac{k}{2}} = (\sqrt{z})^k$.

Furthermore, for $T := \{\pm 1, \pm i\}$ we define

$$G := \left\{ (\alpha, \phi(z)) \;\middle|\; \alpha \in \mathrm{GL}_2^+(\mathbb{Q}), \phi \text{ holom. on } \mathcal{H}, \phi(z)^2 = t\frac{cz+d}{\sqrt{\det \alpha}}, \text{for some } t \in T^2 \right\},$$

where $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $T^2 = \{\pm 1\}$.

We can equip G with a group structure by defining a product

$$(\alpha, \phi(z))(\beta, \rho(z)) = (\alpha\beta, \phi(\beta z)\rho(z)).$$

For $\zeta := (\alpha, \phi(z)) \in G$ and $k \in \mathbb{N}$, we define the operator $[\zeta]_{\frac{k}{2}}$ on functions f on $\mathcal{H}$ as

$$f(z)|[\zeta]_{\frac{k}{2}} := f(\alpha z)\phi(z)^{-k}.$$

This gives an action of the group G on functions on $\mathcal{H}$.
Now, let $\Gamma = \Gamma_0(4)$. Define

$$\tilde{\Gamma} := \{(\gamma, j(\gamma, z)) \mid \gamma \in \Gamma\}.$$

Definition 3.0.3. Let $k \in \mathbb{Z}$. Let f be a meromorphic function on $\mathcal{H}$ which is invariant under $[\tilde{\gamma}]_{\frac{k}{2}}$, for all $\tilde{\gamma} \in \tilde{\Gamma}$. We say that $f(z)$ is a ***modular function of***

weight k/2 for $\tilde{\Gamma}$ if f is meromorphic at every cusp of Γ. Such an f is called a ***modular form*** if it is holomorphic on $\mathcal{H}$ and at every cusp. A modular form f is a ***cusp form*** if it vanishes at all cusps.

We will write for the space of modular forms (resp. cusp forms) of weight $k/2$ $\mathcal{M}_{\frac{k}{2}}(\Gamma)$ (resp. $\mathcal{S}_{\frac{k}{2}}(\Gamma)$).

Proposition 3.0.4. Let $\theta(z) = \sum_{n=-\infty}^{\infty} q^{n^2}$, $F(z) = \sum_{n>0 \text{ odd}} \sigma_1(n)q^n$, $q = e^{2\pi iz}$. Assign weight $1/2$ to θ and weight 2 to F. Then $\mathcal{M}_{\frac{k}{2}}(\Gamma)$ is the space of all polynomials in $\mathbb{C}[\theta, F]$ having pure weight $k/2$.

Proof: See [K] Chap. IV pg. 184.

Corollary 3.0.5. $\dim \mathcal{M}_{\frac{k}{2}}(\Gamma) = 1 + \lfloor \frac{k}{4} \rfloor$.

Next, recall that $\Gamma_\infty := \{\gamma \in \Gamma \mid \gamma\infty = \infty\} = \left\{ \pm \begin{pmatrix} 1 & j \\ & 1 \end{pmatrix} \right\}$.

Definition 3.0.6. Let k be an odd integer, $k \geq 5$.

$$E_{\frac{k}{2}}(z) := \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(4)} j(\gamma, z)^{-k}.$$

As representatives γ of $\gamma \in \Gamma_\infty \setminus \Gamma_0(4)$ we take one matrix $\begin{pmatrix} a & b \\ m & n \end{pmatrix} \in \Gamma_0(4)$ for each (m, n) with $4 \mid m$, $\gcd(m, n) = 1$. Thus

$$E_{\frac{k}{2}}(z) = \sum_{\substack{m,n \in \mathbb{Z} \\ 4|m,\ n>0 \\ \gcd(m,n)=1}} j\left(\begin{pmatrix} a & b \\ m & n \end{pmatrix}, z \right)^{-k} = \sum_{\substack{4|m,\ n>0 \\ \gcd(m,n)=1}} \left(\frac{m}{n}\right) \epsilon_n^k (mz+n)^{\frac{-k}{2}},$$

where $\left(\frac{m}{n}\right)$ and ϵ_n were defined in Remark 3.0.2.

It is a classical result that for $k = 8$,

$$E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \frac{n^3 q^n}{1 - q^n}$$

is a modular form of weight 4. Additionally, for $z \in \mathcal{H}$, we define the following two series:

$$\theta_1(z) := \sum_{n \in \mathbb{Z}} (-1)^n q^{n^2}, \quad \eta(z) := q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n). \tag{31}$$

The one on the left is (one of) the Jacobi theta function(s), and the one on the right is called the Dedekind eta function.

Proposition 3.0.7. For any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $G_2(z) = 2\zeta(z) - 8\pi^2 \sum_{n=1}^{\infty} \sigma(n) q^n$ one has

$$(G_2[\gamma]_2)(z) = G_2(z) - \frac{2\pi i c}{cz + d}.$$

Proof: See [DS] pg. 18.

Consider the weight 2 Eisenstein series $E_2(z) = \dfrac{G_2(z)}{2\zeta(2)}$.

By choosing $\gamma = \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}$ in Proposition 3.0.7 one obtains the identity

$$z^{-2}E_2\left(\frac{-1}{z}\right) = E_2(z) + \frac{12}{2\pi i z}. \tag{32}$$

Next, we consider the Dedekind eta function $\eta(z)$. It satisfies the following transformation law:

$$\eta\left(\frac{-1}{z}\right) = \sqrt{-iz}\eta(z), \quad \forall z \in \mathcal{H}. \tag{33}$$

We obtain this by computing the logarithmic derivative

$$\begin{aligned}
\frac{d}{dz}\log(\eta(z)) &= \frac{\pi i}{12} - 2\pi i \sum_{d=1}^{\infty} \frac{dq^d}{1-q^d} \\
&= \frac{\pi i}{12} - 2\pi i \sum_{d=1}^{\infty} d \sum_{m=1}^{\infty} q^{dm} \\
&= \frac{\pi i}{12} - 2\pi i \sum_{m=1}^{\infty} \sum_{d=1}^{\infty} dq^{dm} \\
&= \frac{\pi i}{12} - 2\pi i \sum_{n=1}^{\infty} \left(\sum_{0<d|n}^{\infty} d \right) q^n \\
&= \frac{\pi i}{12} E_2(z).
\end{aligned}$$

Hence

$$\frac{d}{dz}\log\left(\eta\left(\frac{-1}{z}\right)\right) = \frac{\pi i}{12} z^{-2} E_2\left(\frac{-1}{z}\right),$$

and

$$\frac{d}{dz}\log(\sqrt{-iz}\eta(z)) = \frac{1}{2z} + \frac{\pi i}{12}E_2(z) = \frac{\pi i}{12}\left(E_2(z) + \frac{12}{2\pi i z}\right).$$

By equation (32) these two are equal. Therefore the equation (33) holds up to a multiplicative constant. Setting $z = i$ shows that the constant is 1.

Next, note that

$$\eta(z+1) = e^{\frac{2\pi i}{24}} \cdot e^{\frac{2\pi i z}{24}} \prod_{n\in\mathbb{N}} (1 - e^{2\pi i z n}) = e^{\frac{2\pi i}{24}}\eta(z). \tag{34}$$

It is well-known that the matrices

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

generate the modular group $\mathrm{SL}_2(\mathbb{Z})$. The relations (33) and (34) are transformation formulae for $\eta(z)$ with respect to the generators T and S of $\mathrm{SL}_2(\mathbb{Z})$. They can be

written as $\eta(Tz) = e\left(\frac{1}{24}\right)\eta(z)$ and $\eta(Sz) = e\left(\frac{-1}{8}\right)\sqrt{z}\eta(z)$ (where $e(z) := e^{2\pi iz}$). Moreover, note that the function

$$\tilde{j} : \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z\right) \mapsto cz + d$$

satisfies

$$\tilde{j}(L_1L_2, z) = \tilde{j}(L_1, L_2z)\tilde{j}(L_2, z),$$

for all Möbius transformations $L_1, L_2 \in \mathrm{SL}_2(\mathbb{R})$ of $\mathcal{H}$. It follows that the eta function satisfies the relations

$$\eta(Lz) = v_\eta(L)(cz + d)^{\frac{1}{2}}\eta(z), \tag{35}$$

for all $L = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, with $v_\eta(L)$ only depending on L (and not on z).

One can also compute $v_\eta(L)$ explicitly:

Proposition 3.0.8. For $L = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ the *multiplier system* $v_\eta(L)$ of the Dedekind eta function is given by

$$v_\eta(L) = \begin{cases} \left(\frac{c}{|d|}\right) e\left(\frac{1}{24}((a+d)c - bd(c^2-1) - 3c)\right), & c \text{ odd}, \\ \left(\frac{c}{|d|}\right) r(c,d) \cdot e\left(\frac{1}{24}((a+d)c - bd(c^2-1) + 3d - 3 - 3cd)\right), & c \text{ even}, \end{cases}$$

where $r(c,d) := (-1)^{\frac{1}{4}(\mathrm{sgn}(c)-1)(\mathrm{sgn}(d)-1)}$.

Proof: See [Knopp] Section 1.1.

Proposition 3.0.9. The Jacobi theta function $\theta_1(z)$ is a modular form of weight $1/2$ for $\Gamma_0(4)$.

Proof: We start by giving the following more general statement:

Theorem 3.0.10 (***Jacobi triple product identity***)**.** Suppose that $q, w \in \mathbb{C}$ and $|q| < 1, w \neq 0$. Then

$$\prod_{n=1}^{\infty}(1-q^{2n})(1+q^{2n-1}w)(1+q^{2n-1}w^{-1}) = \sum_{n\in\mathbb{Z}} q^{n^2}w^n. \tag{36}$$

Proof: See [Kohl] Section 1, Theorem 1.1.

Now, choose $w := -1$ and multiply and divide the left side of (36) by $(1-q^{2n})$ to obtain

$$\prod_{n=1}^{\infty}(1-q^{2n})^2(1-q^{2n-1})^2(1-q^{2n})^{-1} = \sum_{n\in\mathbb{Z}}(-1)^n q^{n^2}.$$

Since $\prod_{n=1}^{\infty}(1-q^{2n})(1-q^{2n-1}) = \prod_{n=1}^{\infty}(1-q^n)$, we obtain

$$\frac{\eta(z)^2}{\eta(2z)} = \prod_{n=1}^{\infty}(1-q^n)^2(1-q^{2n})^2 = \sum_{n\in\mathbb{Z}}(-1)^n q^{n^2} = \theta_1(z).$$

Using transformation laws we obtained for the eta function above, we get

$$\theta_1\left(\frac{-1}{z}\right) = \frac{\eta(-1/z)^2}{\eta(-2/z)} = \frac{-iz\eta(z)^2}{\sqrt{-iz}\eta(2z)} = (-iz)^{\frac{1}{2}}\theta_1(z)$$
$$\theta_1(z+1) = \frac{\eta(z+1)^2}{\eta(2(z+1))} = \frac{e^{\frac{4\pi i}{24}}\eta(z)^2}{e^{\frac{4\pi i}{24}}\eta(2z)} = \theta_1(z).$$

Hence $\theta_1(z)$ is a modular form of weight $1/2$. □

3.1 The operator U_4

Definition 3.1.1. Define the following operator on formal q-expansions $\sum a_n q^n$: let $q = e^{2\pi iz}$, and define

$$(f|U_4)(z) = \sum a_{4n} q^n.$$

Lemma 3.1.2. If $f = \sum_{n=0}^{\infty} a_n q^n$ is a modular form of weight $k \in \frac{1}{2}\mathbb{Z}$, $\left(\begin{pmatrix} 1 & j \\ & 4 \end{pmatrix}, \phi(z)\right) = \gamma \in G$, then

$$(f|U_4)(z) = \frac{1}{4}\sum_{j=0}^{3} f\left(\frac{z+j}{4}\right) = \sum_{j=0}^{3} f(z)|[\gamma]_k$$

Proof: Note that if $\zeta_p = e^{\frac{2\pi i}{p}}$, $p \in \mathbb{Z}$, then

$$\sum_{j=0}^{p-1} \zeta_p^{nj} = \begin{cases} p, & p \mid n \\ 0, & p \nmid n \end{cases}$$

Now

$$\begin{aligned}
\sum_{j=0}^{3} f|[\gamma]_k &= 4^{k-1}4^{-k}t^{-\frac{k}{2}} \sum_{j=0}^{4-1} f\left(\frac{z+j}{4}\right) \\
&= \frac{1}{4}\sum_{j=0}^{3}\sum_{n=0}^{\infty} a_n e^{2\pi i n\frac{z+j}{4}} \\
&= \sum_{n=0}^{\infty} a_n e^{\frac{2\pi i n z}{4}} \left(\frac{1}{4}\sum_{j=0}^{3}\zeta_4^{nj}\right) \\
&= (f|U_4)(z).
\end{aligned}$$

□

For the modular forms θ and g, where

$$\theta(z) = \sum_{n\in\mathbb{Z}} q^{n^2},$$

and g is a modular form of weight $3/2$, we define the ***Cohen bracket*** as

$$[g,\theta](z) = 2\left(g'(z)\theta(z) - 3\theta(z)g'(z)\right), \tag{37}$$

where $' := \frac{d}{2\pi i dz}$.

Theorem 3.1.3 (***Derivatives of modular forms of different weight***)**.** Let $m \geq 2$ and let $\mathcal{M}_m$ be the vector space of modular forms of weight m for $\mathrm{SL}_2(\mathbb{Z})$. Then for $f \in \mathcal{M}_k$ and $g \in \mathcal{M}_l$ one has that

$$lf'g - kgf' \in \mathcal{M}_{l+k+2}. \tag{38}$$

Proof: See [Zag] pg. 60.

Thus $[g, \theta]$ is a holomorphic modular form of weight 4 on $\Gamma_0(4)$.

4 Traces of singular moduli

In this section we will introduce Zagier's result on traces of singular moduli. We mainly follow [Z] and rely on the results from previous chapters.

Let $d \in \mathbb{N}$ with $d \equiv 0$ or $3 \pmod 4$. Let $\mathcal{Q}_d$ be the set of positive definite binary quadratic forms $Q = [a, b, c] = aX^2 + bXY + cY^2$, $a, b, c \in \mathbb{Z}$ (so $a > 0$), of discriminant $b^2 - 4ac = -d$. To each $Q \in \mathcal{Q}_d$ we associate its unique root α_Q in $\mathcal{H}$ and we say that this root is the CM-point associated with Q.
Denote $\Gamma = \mathrm{PSL}(2, \mathbb{Z})$. Then the j-invariant of α_Q, $j(\alpha_Q)$ only depends on the Γ equivalence class of Q (by equation (4)). Moreover, recall from Section 2.3 that $j(\alpha_Q)$ is an algebraic integer.
Let $h(-d)$ denote the class number of $-d$. Then, $h(-d)$ is the number of Γ-equivalence classes of primitive quadratic forms (such that $\gcd(a, b, c) = 1$) in $\mathcal{Q}_d$. From the discussion in Chapter 2 we know that each of the corresponding $h(-d)$ values of $j(\alpha_Q)$ is an algebraic integer of degree $h(-d)$ and that they form a full set of Galois conjugates (by Theorem 2.3.10). Then we can take the sum of those $j(\alpha_Q)$'s and it will be the trace.

Computing a 'weighted' sum of the trace leaves us with integers that are equal (up to a sign) to coefficients of the Fourier expansion of a certain modular form of weight 3/2; and proving that relation is the main goal of this chapter.

On one hand we consider the function

$$t(d) := \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{1}{|\Gamma_Q|}(j(\alpha_Q) - 744), \tag{39}$$

called the ***modular trace function***, where $|\Gamma_Q|$ is equal to 2 or 3 if Q is Γ equivalent to $[a, 0, a]$ or $[a, a, a]$, and 1 otherwise.

On the other hand, we consider the modular form

$$g(z) := \theta_1(z)\frac{E_4(4z)}{\eta(4z)^6} = \frac{1}{q} - 2 + 248q^3 - 492q^4 + 4119q^7 - 7256q^8 + \dots \tag{40}$$

constructed from the modular forms E_4, θ_1 and η introduced in the previous Section. We will write

$$g(z) = \sum_{d \in \mathbb{Z}} B(d)q^d,$$

where $B(d)$ are the coefficients of the Fourier expansion of $g(z)$ and $B(d) = 0$ for $d < -1$.
Next, we want to show that $g(\tau)$ is a modular form of weight 3/2. Recall that E_4 has weight 4 and θ_1 has weight 1/2. We will now compute $g(\gamma\tau)$, for $\gamma = S, T$.

Using equation (33) for $\gamma = S$ one obtains

$$\begin{aligned}\eta\left(4\cdot\frac{-1}{z}\right)^6 &= -i^3z^3\eta(z)^6,\\ \theta_1\left(\frac{-1}{z}\right) &= \frac{\eta(-1/z)^2}{\eta(-2/z)} = (-i)^{\frac{1}{2}}z^{\frac{1}{2}}\theta_1(z),\\ E_4\left(4\cdot\frac{-1}{z}\right) &= z^4E_4(4z).\end{aligned}$$

Putting it all together:

$$g\left(\frac{-1}{z}\right) = \theta_1(z)\frac{E_4(4z)}{\eta(4z)^6} = (-i)^{\frac{3}{2}}z^{\frac{3}{2}}\theta_1(z)\frac{E_4(4z)}{\eta(4z)^6} = (-i)^{\frac{3}{2}}z^{\frac{3}{2}}g(z).$$

Now we turn to $\gamma = T$.

$$\begin{aligned}\eta(4(z+1))^6 &= i\cdot\eta(4z)^6,\\ \theta_1(z+1) &= \theta_1(z).\end{aligned}$$

Thus

$$g\left(z+1\right) = \theta_1(z+1)\frac{E_4(4(z+1))}{\eta(4(z+1))^6} = -iz^{\frac{3}{2}}g(z) = (-1)^{\frac{3}{2}}z^{\frac{3}{2}}g(z).$$

Hence, $g(z)$ is a modular form of weight $3/2$ on $\Gamma_0(4)$.

Theorem 4.0.1. Let $B(d)$ and $t(d)$ be defined as above. Then for all $d > 0$

$$t(d) = -B(d).$$

4.1 A recursion formula for $B(d)$

The idea is the following. First, using some properties from the theory of modular forms, we deduce recursion formulas for the coefficients $B(d)$ of $g(z)$. The idea is to then show that $t(d)$ can be computed using the same recursion formulas.

We start by considering the theta series

$$\theta(z) = \sum_{n\in\mathbb{Z}} q^{n^2},$$

and $g(z)$, given in (40). By comparing the exponents of the Fourier expansion of $\eta(4z)^{-6}$, $E_4(z)$ and $\theta_1(z)$ one can see that $g(z)$ has non-zero Fourier coefficients only for q^k, where $k \equiv 0$ or $3 \pmod 4$. To see this write

$$\begin{aligned}g(\tau) &= \theta_1(\tau)\frac{E_4(4\tau)}{\eta(4\tau)^6}\\ &= \left(\sum_{n\in\mathbb{Z}}(-1)^n q^{n^2}\right)\left(1+240\sum_{n=1}^{\infty}\frac{(4n)^3q^{4n}}{1-q^{4n}}\right)q^{-1}\prod_{n=1}^{\infty}(1-q^{4n})^{-6}\\ &= \left(\sum_{n\in\mathbb{Z}}(-1)^n q^{n^2-1}\right)\left(1+240\sum_{n=1}^{\infty}(4n)^3q^{4n}\sum_{l=0}^{\infty}q^{4l}\right)\prod_{n=1}^{\infty}\left(\sum_{m=0}^{\infty}q^{4lm}\right)^6.\end{aligned}$$

All coefficients q^k in the product have the form $k = 4n, 4l$ or $4lm$ (so are $\equiv 0 \pmod 4$), except q^{n^2-1}. Since $n^2 - 1 \equiv 0$ or $3 \pmod 4$, we see that the exponent q^d in the Fourier expansion of $g(\tau)$ is non-zero only for $d \equiv 0$ or $3 \pmod 4$.

Then $g\theta$ is a modular form of weight 2 and $(g\theta)|U_4$ is also a modular form of weight 2 on the full modular group $\mathrm{PSL}(2,\mathbb{Z})$, thus identically zero. Writing this in terms of Fourier coefficients yields:

$$\begin{aligned}
(g\theta)|U_4 &= \left(\sum_{d\geq -1} B(d)q^d \sum_{r\in\mathbb{Z}} q^{r^2}\right)\Bigg| U_4 \\
&= \left(\sum_{d\geq -1,\ r\in\mathbb{Z}} B(d)q^{d+r^2}\right)\Bigg| U_4, \quad d + r^2 =: n \\
&= \left(\sum_{n,\ r} B(n-r^2)q^n\right)\Bigg| U_4 \\
&= \sum_n q^n \left(\sum_{r\in\mathbb{Z}} B(4n-r^2)\right).
\end{aligned}$$

Thus we obtain the identity

$$\sum_{r\in\mathbb{Z}} B(4n-r^2) = 0, \quad \forall n \geq 0 \tag{41}$$

Next, we consider the image of the Cohen bracket

$$[g,\theta](z) = 2(g'(z)\theta(z) - 3\theta(z)g'(z))$$

under U_4. Since $[g,\theta]|U_4$ is a holomorphic modular form of weight 4, it is a multiple of E_4. We again compute the Fourier expansion:

$$\begin{aligned}
[g,\theta]|U_4(z) &= 2(g'(z)\theta(z) - 3g(z)\theta'(z))|U_4 \\
&= 2\left(\sum_{d\geq -1} dB(d)q^d \sum_{r\in\mathbb{Z}} q^{r^2} - 3\sum_{\tilde{d}\geq -1} \tilde{d}B(\tilde{d})q^{\tilde{d}} \sum_{\tilde{r}\in\mathbb{Z}} \tilde{r}^2 q^{\tilde{r}^2}\right)\Bigg| U_4 \\
&= 2\left(\sum_{d,r} (d-3r^2)B(d)q^{d+r^2}\right)\Bigg| U_4, \quad d + r^2 =: n \\
&= 2\left(\sum_{n,r} (n-4r^2)B(n-r^2)q^n\right)\Bigg| U_4 \\
&= 8\left(\sum_n \sum_{r\in\mathbb{Z}} (n-r^2)B(4n-r^2)q^n\right).
\end{aligned}$$

Since $\sum_n nq^n \sum_{r\in\mathbb{Z}} B(4n-r^2) = 0$, we get that

$$-16\sum_n q^n \sum_{r>0} r^2 B(4n-r^2)$$

is a multiple of $E_4(z) = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n$. Finally

$$\sum_{r>0} r^2 B(4n - r^2) = 240\sigma_3(n). \tag{42}$$

One can rewrite equations (41) and (42) as

$$B(4n-1) = 240\sigma_3(n) - \sum_{2\le r\le\sqrt{4n+1}} r^2 B(4n-r^2), \tag{43}$$

$$B(4n) = -2\sum_{1\le r\le\sqrt{4n+1}} B(4n-r^2). \tag{44}$$

which allow us to determine all the $B(d)$'s by recursion.
Note that $B(-1) = 240\sigma_3(0) = 1$, $B(0) = -2B(-1) = -2$ and $B(3) = 248$. Then

$$\begin{aligned}\sum_{|r|<2\sqrt{n}} B(4n-r^2) &= 2\sum_{1\le r\le\sqrt{4n+1}} B(4n-r^2) + B(4n) - 2\sum_{\sqrt{4n}\le r\le\sqrt{4n+1}} B(4n-r^2)\\ &= -2\sum_{\sqrt{4n}\le r\le\sqrt{4n+1}} B(4n-r^2)\\ &= \begin{cases} -2B(0) = 4, & \text{if } n \text{ is a square,}\\ -2B(-1) = -2, & \text{if } 4n+1 \text{ is a square,}\\ 0, & \text{otherwise.}\end{cases}\end{aligned}$$

Similarly one computes

$$\begin{aligned}\sum_{1\le r<2\sqrt{n}} r^2 B(4n-r^2) &= 2\sum_{\substack{2\le r\\ \le\sqrt{4n+1}}} B(4n-r^2) + B(4n-1) - 2\sum_{\substack{\sqrt{4n}\le r\\ \le\sqrt{4n+1}}} r^2 B(4n-r^2)\\ &= 240\sigma_3(n) - 2\sum_{\sqrt{4n}\le r\le\sqrt{4n+1}} r^2 B(4n-r^2)\\ &= 240\sigma_3(n) + \begin{cases} 8n, & \text{if } n \text{ is a square,}\\ -4n-1, & \text{if } 4n+1 \text{ is a square,}\\ 0, & \text{otherwise.}\end{cases}\end{aligned}$$

4.2 A recursion formula for $t(d)$

Next, we want to show that the same recursion formulas hold for $t(d)$.

Theorem 4.2.1. For all $n \in \mathbb{N}$ one has

$$\sum_{|r|<2\sqrt{n}} t(4n-r^2) = \begin{cases} -4, & \text{if } n \text{ is a square,}\\ 2, & \text{if } 4n+1 \text{ is a square,}\\ 0, & \text{otherwise,}\end{cases} \tag{45}$$

and

$$\sum_{1\le r<2\sqrt{n}} r^2 t(4n-r^2) = -240\sigma_3(n) + \begin{cases} -8n, & \text{if } n \text{ is a square,}\\ 4n+1, & \text{if } 4n+1 \text{ is a square,}\\ 0, & \text{otherwise.}\end{cases} \tag{46}$$

For that we consider the *modular polynomials* (recall (23))

$$\Phi_n(X, j(\tau)) = \prod_{\sigma \in C(n)} (X - j(\sigma\tau)) = \prod_{M \in \Gamma \backslash \mathcal{M}_n} (X - j(M\tau)), \ \ \tau \in \mathcal{H},$$

where $\mathcal{M}_n$ denotes the set of 2×2 integral matrices of determinant n, with M and $-M$ being identified. Also, recall from Section 2.3 the set

$$C(n) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = n, a > 0, 0 \leq b < d, \gcd(a, b, d) = 1 \right\}.$$

To prove equation (45) the idea is to compare Fourier coefficients of two different formulas for the modular polynomial $\Phi_n(j(\tau), j(\tau))$. In the case where n is a square Φ_n is divisible by Φ_1, so we will consider Φ_n/Φ_1 instead of Φ_n. For equation (46) the idea is to take the logarithmic derivative of Φ_n.

Proof: We start with equation (45). First assume $n \in \mathbb{N}$ is not a square. Then $\Phi_n(j(\tau), j(\tau))$ vanishes exactly at the points $\tau \in \mathcal{H}$ which are fixed by some $M \in \mathcal{M}_n$. These are the points α_Q with Q a positive definite quadratic form ($\mathrm{disc}(Q) > 0$). We can write $\mathrm{disc} = r^2 - 4n$ for some integer $r = \mathrm{tr}(M)$ satisfying $|r| < 2\sqrt{n}$. Define for $d > 0, \ \ d \equiv 0 \text{ or } 3 \pmod 4$

$$\mathcal{H}_d(X) := \prod_{Q \in \mathcal{Q}_d/\Gamma} (X - j(\alpha_Q))^{\frac{1}{w_Q}},$$

where $w_Q := |\Gamma_Q|$. This function is $X^{1/3}$ times a polynomial in X if $d/3$ is a square, $(X - 1728)^{1/2}$ times a polynomial in X if d is a square, and a polynomial otherwise. On one hand we get the identity

$$\Phi_n(X, X) = C \cdot \prod_{|r| < 2\sqrt{n}} \mathcal{H}_{4n-r^2}(X), \tag{47}$$

with $C := \pm 1$. We have the q-expansion

$$\mathcal{H}_d(j(\tau)) = \prod_{Q \in \mathcal{Q}_d/\Gamma} (q^{-1} + 744 - j(\alpha_Q) + \mathcal{O}(q))^{\frac{1}{w_Q}} \tag{48}$$

$$= q^{-H(d)}(1 - t(d)q + \mathcal{O}(q^2)), \quad H(d) := \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{1}{w_Q}. \tag{49}$$

On the other hand, take as representatives for $\Gamma \setminus \mathcal{M}_n$ the matrices $\begin{pmatrix} a & b \\ & d \end{pmatrix}$, with

$ad = n$ and $0 \le b < d$:

$$\begin{aligned}\Phi_n(j(\tau), j(\tau)) &= \prod_{ad=n} \prod_{b=1}^{d} \left(j(\tau) - j\left(\frac{a\tau + b}{d}\right)\right) \\ &= \prod_{ad=n} \prod_{b=1}^{d} \left(\frac{1}{q} - e^{-2\pi i b/d} q^{-a/d} + \mathcal{O}(q^{>0})\right) \\ &= \prod_{ad=n} (q^{-d} - q^{-a})(1 + \mathcal{O}(q^{>1})) \\ &= \prod_{ad=n} \pm q^{-\max\{a,d\}}(1 - \epsilon_a q + \mathcal{O}(q^2)),\end{aligned}$$

where $\epsilon_a = 1$ if $|a-d| = 1$ and 0 otherwise. Since

$$|a-d| = 1 \iff a^2 - n = \pm a \iff 4n+1 = (2a \pm 1)^2,$$

$\epsilon_a = 1$ if and only if $4n+1$ is a perfect square. Then $d = a \pm 1$ and $-\max\{a,d\} = -a-1$ or $d = -a$. Expanding the product

$$q^{-(2a+1)}(1 - q + \mathcal{O}(q^2))^2 \cdot \prod_{ad=n,\ |a-d|\neq 1} q^{-\max\{a,d\}}(1 + \mathcal{O}(q^2))$$

we see that the coefficient in front of q is -2. Comparing this to (48) we get the first recursion formula (45) for $t(d)$ and non-square n.
Now, let n be a square. Then $\Phi_n(X,Y)$ is divisible by $\Phi_1(X,Y) = X - Y$ and we replace $\Phi_n(X,Y)$ by $\Phi_n(X,Y)/\Phi_1(X,Y)$:

$$\begin{aligned}\left.\frac{\Phi_n(j(\tau),Y)}{\Phi_1(j(\tau),Y)}\right|_{Y=j(\tau)} &= C \cdot \prod_{|r|<2\sqrt{n}} \mathcal{H}_{4n-r^2}(j(\tau)) \left(\prod_{|r|<2} \mathcal{H}_{4-r^2}(j(\tau))\right)^{-1} \\ &= C \cdot \prod_{|r|<2\sqrt{n}} q^{-H(4n-r^2)}(1 - t(4n-r^2)q + \mathcal{O}(q^2)) \\ &\quad \cdot \left(q^{-2H(3)-H(4)}(1 - t(3)q + \mathcal{O}(q^2))^2(1 - t(4)q) + \mathcal{O}(q^2))\right)^{-1}.\end{aligned}$$

Similarly as before

$$\left.\frac{\Phi_n(j(\tau),Y)}{\Phi_1(j(\tau),Y)}\right|_{Y=j(\tau)} = \prod_{\substack{ad=n \\ a\neq\sqrt{n},\ d\neq\sqrt{n},\ b\neq 0}} \pm q^{\max\{a,d\}}(1 - \epsilon_a q + \mathcal{O}(q^2)), \tag{50}$$

but $\epsilon_a = 0$, since $4n+1$ is not a square. Comparing the coefficients we obtain

$$\sum_{|r|<2\sqrt{n}} t(4n-r^2) \left(\sum_{|r|<2} t(4-r^2)\right)^{-1} = 1,$$

and finally

$$\sum_{|r|<2\sqrt{n}} t(4n-r^2) = 2t(3) + t(4) = 2 \cdot (-248) + 492 = -4.$$

Next, we will show the second recursion formula (42) for $t(d)$. For $d \in \mathbb{N}$ such that $d \equiv 0$ or $3 \pmod 4$ define

$$\Lambda_d(\tau) = \frac{d}{d\tau} \log \mathcal{H}_d(j(\tau)) = \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{1}{w_Q} \frac{j'(\tau)}{j(\tau) - j(\alpha_Q)}. \tag{51}$$

The j-invariant has weight 0, so its derivative has weight 2 (simply by the chain rule; one can compute that j'/j is proportional to $-E_6/E_4$). Hence Λ_d is a modular form of weight 2, holomorphic at infinity and with a simple pole of residue $1/|\Gamma_\alpha|$ for $\alpha \in \mathcal{H}$ satisfying a quadratic equation over $\mathbb{Z}$ of discriminant $-d$. Since there are no holomorphic modular forms of weight 2 on Γ, Λ_d is uniquely characterised by these properties. Now, we would like to compute the logarithmic derivative of equation (47).

Proposition 4.2.2. Let $n \in \mathbb{N}$ not a square, $\tau \in \mathcal{H}$. Then

$$\frac{E_4(\tau)E_6(\tau)}{\Delta(\tau)} \sum_{M \in \Gamma \backslash \mathcal{M}_n} \frac{(E_4|M)(\tau)}{j(\tau) - j(M\tau)} = \frac{1}{4\pi i} \sum_{|r|<2\sqrt{n}} \left(r^2 - n\right) \Lambda_{4n-r^2}(\tau) \tag{52}$$

where $M\tau := \frac{a\tau+b}{c\tau+d}$ and $(E_4|M)(\tau) := n^3(c\tau+d)^{-4}E_4(M\tau)$ for $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_n$

With the help of Proposition 4.2.2 we can proceed similarly as before. Let $C_0 + C_1 q + \dots$ denote the expansion of the left hand side of (52) at infinity. From

$$\begin{aligned} -\frac{1}{2\pi i}\Lambda_d(\tau) &= \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{1}{w_Q} \frac{q^{-1} + \mathcal{O}(q)}{q^{-1} + 744 - j(\tau) + \mathcal{O}(q)} \\ &= H(d) + t(d)q + \mathcal{O}(q^2), \end{aligned}$$

we see

$$C_0 = \frac{1}{2} \sum_{|r|<2\sqrt{n}} (n - r^2) H(4n - r^2), \quad C_1 = \frac{1}{2} \sum_{|r|<2\sqrt{n}} (n - r^2) t(4n - r^2). \tag{53}$$

On the other hand, we can again take as a set of representatives for $\Gamma \setminus \mathcal{M}_n$ the set $C(n)$. Then the left hand side of (52) equals to

$$\sum_{ad=n} a^3 \cdot \frac{E_4(\tau)E_6(\tau)}{\Delta(\tau)} \frac{1}{d} \sum_{0 \le b < d} \frac{j((a\tau+b)/d)}{j(\tau) - j((a\tau+b)/d)} =: \sum_{ad=n} a^3 \cdot S_{a,d}(\tau).$$

Next, we write out $S_{a,d}(\tau)$:

(*Case I*) Assume $a < d$.

$$\begin{aligned} S_{a,d}(\tau) &= (q^{-1} - 240 + \mathcal{O}(q)) \cdot \frac{1}{d} \sum_{\zeta^d=1} \frac{1 + 240\zeta q^{a/d} + 240\sigma_3(2)\zeta^2 q^{2a/d} + \dots}{q^{-1} - \zeta^{-1} q^{-a/d} + \mathcal{O}(q^{a/d})} \\ &= A(q) \cdot \frac{1}{d} \sum_{\zeta^d=1} \frac{1}{1 - (\zeta^{-1} q^{1-a/d} + \mathcal{O}(q^{>1}))} \cdot \left(1 + 240 \sum_{l=1}^{\infty} \sigma_3(l) \zeta^l q^{l\frac{a}{d}}\right), \end{aligned}$$

where we write $A(q) := 1 - 240q + \mathcal{O}(q^2)$. Then expand the geometric series as

$$S_{a,d}(\tau) = A(q) \cdot \frac{1}{d} \sum_{\zeta^d=1} \left(\sum_{m=0}^{\infty} \zeta^{-m} q^{m(1-\frac{a}{d})} + \mathcal{O}(q^{>1}) \right) \cdot \left(1 + 240 \sum_{l=1}^{\infty} \sigma_3(l) \zeta^l q^{l\frac{a}{d}} \right)$$
$$= A(q) \cdot \frac{1}{d} \sum_{\zeta^d=1} \left(\sum_{m=0}^{\infty} \zeta^{-m} q^{m(1-\frac{a}{d})} + \sum_{\substack{m=0 \\ l=1}}^{\infty} \sigma_3(l) \zeta^{l-m} q^{m+(l-m)\frac{a}{d}} + \mathcal{O}(q^{>1}) \right).$$

To avoid the expression being 0, we need the powers of q to be integral, and hence $l \equiv m \pmod{d}$. Then $\zeta^{l-m} = 1$, for all $0 \leq b < d$. Thus

$$S_{a,d}(\tau) = (1 - 240q + \mathcal{O}(q^2)) \cdot \sum_{\substack{m=0,\ l=0 \\ l \equiv m \pmod{d}}}^{\infty} 240\sigma_3(l) q^{m+(l-m)\frac{a}{d}} + \mathcal{O}(q^2)$$
$$= 1 + (240\delta_{a,1}\sigma_3(n) + \delta_{a,d-1})q + \mathcal{O}(q^2),$$

since the only pairs (l, m) which contribute to the powers q^0 and q^1 are $(0,0), (1,1), (d,0)$ for $a = 1$ and $(0, d)$ for $a = d - 1$.

(*Case II*) Assume $a > d$.
A similar computation gives

$$S_{a,d}(\tau) = (1 - 240q + \mathcal{O}(q^2)) \cdot \sum_{\substack{m=0,\ l=0 \\ l \equiv -m \pmod{d}}}^{\infty} 240\sigma_3(l) q^{-m+(l-m)\frac{a}{d}} + \mathcal{O}(q^2)$$
$$= -\delta_{a,d+1} q + \mathcal{O}(q^2),$$

since only the pair $(l, m) = (0, d)$ contributes to the sum.
Summing over all divisors a of d, we see that the first two coefficients C_0 and C_1 are given by

$$C_0 = \sum_{\substack{0<a<\sqrt{n} \\ a|n}} a^3, \quad C_1 = 240\sigma_3(n) - \begin{cases} 3n+1, & 4n+1 \text{ is a square,} \\ 0, & \text{otherwise,} \end{cases}$$

where the last term comes from the two ways of factorising $n = ad$, where $|a-d| = 1$.

Comparing these formulas with the ones computed above (53) we obtain equation (46) in Theorem 4.2.1 for when n is not a square. When n is a square, we can proceed the same way, except that we have an additional case for the Fourier expansion of $S_{a,d}$ when $a = d$. □

Now it only remains to show Proposition 4.2.2.

Proof: Let $M \in \mathcal{M}_n$, $\tau \in \mathcal{H}$. We want to show

$$\frac{E_4(\tau)E_6(\tau)}{\Delta(\tau)} \sum_{M \in \Gamma \backslash \mathcal{M}_n} \frac{(E_4|M)(\tau)}{j(\tau) - j(M\tau)} = \frac{1}{4\pi i} \sum_{|r|<2\sqrt{n}} \left(r^2 - n\right) \Lambda_{4n-r^2}(\tau).$$

Since E_4 has weight 4, E_6 weight 6 and j weight 0, the left side of the equation is a modular form of weight $4+6-12+4-0=2$ (just like the right hand side). Moreover, both sides are holomorphic at infinity, and with only simple poles, so we only need to compare residues. Let $\alpha \in \mathcal{H}$ with $M\alpha = \alpha$. Write as usual $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and suppose $c > 0$. Then $c\alpha^2 + (d-a)\alpha - b = 0$ and $\lambda := c\alpha + d$ is an algebraic integer satisfying $\lambda^2 - (a+d)\lambda + (ad-bc) = 0$. We write $r := \mathrm{tr}(M)$ and $n = \det(M)$ for the norm of λ.
Now compute the residue

$$\mathrm{Res}_{\tau=\alpha}\left(\frac{E_4(\tau)E_6(\tau)}{\Delta(\tau)}\frac{(E_4|M)(\tau)}{j(\tau)-j(M\tau)}\right) = B(\alpha)\cdot\mathrm{Res}_{\tau=\alpha}\left(\frac{1}{j(\tau)-j(\alpha)+j(\alpha)-j(M\tau)}\right),$$

where $B(\alpha) := \dfrac{E_4(\alpha)E_6(\alpha)}{\Delta(\alpha)} n^3 E_4(\alpha)\lambda^{-4}$. Using $j(\alpha) = j(M\alpha)$ we compute

$$\begin{aligned}\mathrm{Res}_{\tau=\alpha}\left(\frac{1}{j(\tau)-j(M\tau)}\right) &= \lim_{\tau\to\alpha}\left(\frac{1}{\frac{j(\tau)-j(\alpha)}{\tau-\alpha} - \frac{j(M\tau)-j(M\alpha)}{\tau-\alpha}}\right)\\ &= \frac{1}{j'(\alpha)-(j\circ M)'(\alpha)}\\ &= \frac{1}{(1-\det(M)(cz+d)^{-2})j'(\alpha)},\end{aligned}$$

since $j'(\tau)$ has weight 2. Finally, using $j' = -2\pi i E_4^2 E_6/\Delta$, $r = \lambda + \bar\lambda$ and $n = \lambda\bar\lambda$

$$\mathrm{Res}_{\tau=\alpha}\left(\frac{E_4(\tau)E_6(\tau)}{\Delta(\tau)}\frac{(E_4|M)(\tau)}{j(\tau)-j(M\tau)}\right) = \frac{E_4(\alpha)E_6(\alpha)}{\Delta(\alpha)}\frac{n^3E_4(\alpha)\lambda^{-4}}{(1-n\lambda^{-2})j'(\alpha)} = \frac{1}{2\pi i}\frac{-\bar\lambda^3}{\lambda-\bar\lambda}.$$

Since the matrices M and nM^{-1} have the same fixed points, but conjugate values of λ, we replace the expression $-\bar\lambda^3/(\lambda-\bar\lambda)$ by $\frac{1}{2}(\lambda^3-\bar\lambda^3)/(\lambda-\bar\lambda) = \frac{1}{2}((\lambda+\bar\lambda)^2-\lambda\bar\lambda) = \frac{1}{2}(r^2-n)$. Then the residue of the left hand side of equation (52) has the form

$$\frac{1}{4\pi i}\sum_{\substack{r^2<4n\\ \alpha\in\Gamma\backslash\mathcal{Q}_{4n-r^2}}}(r^2-n),$$

which equals to the residue on the right hand side. □

4.3 Kronecker's class number relations

In the computations of Fourier coefficients above we stumbled upon a 'byproduct' result, namely:

Proposition 4.3.1 (***Kronecker's class number relation***)**.** Let $d \in \mathbb{N}$ with $d \equiv 0$ or $3 \pmod 4$. Then

$$\sum_{|r|<2\sqrt{n}} H\left(4n-r^2\right) = \sum_{d|n}\max\{d, n/d\} + \begin{cases} 1/6, & \text{if } n \text{ is a square}\\ 0, & \text{otherwise,}\end{cases}$$

where $H(d)$ is the ***Hurwitz-Kronecker class number***

$$H(d) = \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{1}{w_Q},$$

for $w_Q = |\Gamma_Q|$.

For non-square n the proof follows by comparing the exponent of $q^{-H(d)}$ in (48) to $\prod_{ad=n} q^{-\max\{a,d\}} = \prod_{d|n} q^{-\max\{d,n/d\}}$. For n a square we are off by $2H(3) - H(4) = 2 \cdot \frac{1}{3} - \frac{1}{2} = \frac{1}{6}$.

Considering the proof of the second recursion formula (46) for $t(d)$, one can very similarly deduce another identity for the Hurwitz-Kronecker class numbers:

Proposition 4.3.2. Let $n \in \mathbb{N}$. Then

$$\sum_{|r|<2\sqrt{n}} \left(n - r^2\right) H\left(4n - r^2\right) = \sum_{d|n} \min(d, n/d)^3 - \begin{cases} n/2, & \text{if } n \text{ is a square} \\ 0, & \text{otherwise.} \end{cases}$$

4.4 Fourier coefficients of the j-invariant

The aim of this section is to show a formula for computing the coefficients of the j-invariant using Zagier's result on traces of singular moduli. Here we follow [Kan], but also rely on the results from [Z] established in previous sections.

Let again

$$\theta_1(\tau) = \sum_{n \in \mathbb{Z}} (-1)^n q^{n^2}, \quad \theta(\tau) = \sum_{n \in \mathbb{Z}} q^{n^2}, \quad g(\tau) = \theta_1(\tau) \frac{E_4(4\tau)}{\eta(4\tau)^6}.$$

Consider the function

$$\mathcal{K}(\tau) := g(\tau)\theta(\tau) - \frac{1}{4}((g\theta_1)|U_4)\left(\tau + \frac{1}{2}\right) + \frac{1}{4}((g\theta_1)|U_4^2)(\tau),$$

which is a weakly holomorphic modular form of weight 2 on $\Gamma_0(4)$, since the translation $\tau \mapsto \tau + \frac{1}{2}$ sends a modular form to a modular form of the same weight. Using recursion formulas (4.2.1) for the Fourier expansion

$$g(\tau) = \sum_{\substack{d \geq -1 \\ d \equiv 0,3 \ (4)}} t(d) q^d,$$

we compute explicitly

$$\begin{aligned}
g(\tau)\theta(\tau) &= \sum_{d,r} t(d) q^{d+r^2} = \sum_{r,n} t(n-r^2) q^n, \quad d+r^2 = n, \\
\frac{1}{4}((g\theta_1)|U_4)\left(\tau+\frac{1}{2}\right) &= \frac{1}{4}\left(\left(\sum_{d,r} t(d)(-1)^r q^{d+r^2}\right)\middle| U_4\right)\left(\tau+\frac{1}{2}\right) \\
&= \frac{1}{4}\left(\left(\sum_{n,r} t(n-r^2)(-1)^r q^n\right)\middle| U_4\right)\left(\tau+\frac{1}{2}\right) \\
&= \frac{1}{4}\sum_{n,r} t(4n-r^2)(-1)^r e^{2\pi i n\tau + \pi i n} \\
&= \sum_{n,r} \frac{(-1)^{n+r}}{4} t(4n-r^2) q^n,
\end{aligned}$$

and finally

$$\begin{aligned}
\frac{1}{4}((g\theta_1)|U_4^2)(\tau) &= \frac{1}{4}\left(\left(\sum_{n,r} t(n-r^2)(-1)^r q^n\right)\middle| U_4^2\right)(\tau) \\
&= \sum_{n,r} \frac{(-1)^r}{4} t(16n-r^2) q^n.
\end{aligned}$$

Now, we consider the Fourier coefficients of $\mathcal{K}(\tau)$, and we set for $n \in \mathbb{N}$

$$\tilde{c}_n := \frac{1}{n}\sum_{r\in\mathbb{Z}}\left(t(n-r^2) - \frac{(-1)^{n+r}}{4} t(4n-r^2) + \frac{(-1)^r}{4} t(16n-r^2)\right). \tag{54}$$

Note that in each sum in equation (54) only finitely many terms are not 0. we can then rewrite $\tilde{c}_n$ as

$$\tilde{c}_n := \frac{1}{n}\left(\sum_{r\in\mathbb{Z}} t(n-r^2) - \sum_{r\geq 1,\ \text{odd}} \left((-1)^n t(4n-r^2) - t(16n-r^2)\right)\right). \tag{55}$$

Example 4.4.1. We can use equation (55) to compute a couple of $\tilde{c}_n$'s:

$$\begin{aligned}
\tilde{c}_1 &= 2t(0) - t(3) - t(15) - t(7) \\
&= 4 - (-248) - (-192513) - (-4119) \\
&= 196884, \\
\tilde{c}_2 &= \frac{1}{2}\left(t(7) + t(-1) - t(31) - t(23) - t(7)\right) \\
&= \frac{1}{2}\left(-1 - (-39493539) - (-3493982)\right) \\
&= 21493760.
\end{aligned}$$

As the reader might have already realised, these values of $\tilde{c}_n$'s look suspiciously similar to coefficients of the j-invariant.

Theorem 4.4.2. For all $n \geq 1$ and

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

one has $c_n = \tilde{c}_n$ (for $\tilde{c}_n$ given in (54), resp. (55)).

Proof: Compute the derivative of the j-invariant:

$$\frac{1}{2\pi i}\frac{\partial}{\partial \tau} j(\tau) = \frac{-1}{q} + 196884q + 2 \cdot 21493760q^2 + 3 \cdot 864299970q^3 + 4 \cdot 20245856256q^4 + \dots$$

Now compare the first few Fourier coefficients with values of $n\tilde{c}_n$. The derivative of j is a weakly holomorphic modular form of weight 2, which starts with $\frac{-1}{q}$. Since $\mathcal{K}(\tau)$ also starts with $\frac{-1}{q}$, their difference is a holomorphic modular form of weight 2, hence vanishes identically. $\square$

5 Appendix

5.1 Order in a quadratic field

Definition 5.1.1. An ***order*** $\mathcal{O}$ in a quadratic field K is a subset $\mathcal{O} \subset K$ such that the following hold:

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

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

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

Remark 5.1.2. The ***maximal order*** will be denoted by $\mathcal{O}_K$.

Next, recall that the *ideal class group* C is defined as the quotient of proper fractional ideals (denoted $\mathcal{I}$) over principal ideals (denoted $\mathcal{P}$). Hence for an order $\mathcal{O}$ one has

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

where the quotient is taken over all principal (resp. fractional) $\mathcal{O}$-ideals.

Lemma 5.1.3. Let $\mathcal{O}$ be an order in a quadratic field K of discriminant d_K. Then $\mathcal{O}$ has finite index in $\mathcal{O}_K$, and if we set $\mathfrak{f} = [\mathcal{O}_K : \mathcal{O}]$, then

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

with

$$w_K = \frac{d_K + \sqrt{d_K}}{2}$$

being the discriminant of K.

Proof: First, note that $\mathcal{O}$ and $\mathcal{O}_K$ are free $\mathbb{Z}$-modules of rank 2, so $[\mathcal{O}_K : \mathcal{O}] < \infty$. Setting $\mathfrak{f} = [\mathcal{O}_K : \mathcal{O}]$, we have $\mathfrak{f}\mathcal{O}_K \subset \mathcal{O}$, and then $\mathbb{Z} + \mathfrak{f}\mathcal{O}_K \subset \mathcal{O}$ follows. However, since $\mathcal{O}_K = [1, w_K]$, we get that $\mathbb{Z} + \mathfrak{f}\mathcal{O}_K = [1, \mathfrak{f}w_K]$. Hence, to prove the lemma, we have to show that $[1, \mathfrak{f}w_K]$ has index $\mathfrak{f}$ in $\mathcal{O}_K = [1, w_K]$. This last fact is obvious, so we are done. □

Definition 5.1.4. Given an order $\mathcal{O}$ in a quadratic field K, the index $\mathfrak{f} = [\mathcal{O}_K : \mathcal{O}]$ is called the ***conductor*** of the order.

5.2 Primes

Let K be any field and consider a valuation $|\cdot|$ on K such that for all $x, y \in K$ we have the inequality:

$$|x + y| \leq C \max\{x, y\}, \quad C \in \mathbb{R}_{\geq 0}. \tag{56}$$

We say that the valuation $|\cdot|$ is ***nonarchimedian*** if $C = 1$, and that it is ***archimedian*** if C is not *equivalent* to 1.

Definition 5.2.1. An equivalence class of valuations on a filed K is called a ***prime*** of K. An equivalence class of archimedian valuations is called an ***infinite prime*** and an equivalence class of nonarchimedian valuations is called a ***finite prime*** of K.

Theorem 5.2.2 (***Ostrowski***)**.** Let K be a field complete with respect to an archimedian valuation $|\cdot|$. Then K is isomorphic to either the real or complex field and the valuation is equivalent to the usual absolute value.

Ostrowski's theorem lets us deduce all the archimedian valuations of an algebraic number field.

Definition 5.2.3. Let K be a field. An infinite prime of K is called a ***real prime*** if the completion of K at the prime is the real field. An infinite prime is called a ***complex prime*** if the completion of K at the prime is the complex field.

Let K be an algebraic number field and let $\mathfrak{p}$ be a prime of K. Let L be a finite dimensional Galois extension with Galois group $G = G(L/K)$ and let $\mathfrak{b}_1, \ldots, \mathfrak{b}_g$ be primes of L extending $\mathfrak{p}$ so we may write

$$\mathfrak{p} = (\mathfrak{b}_1 \ldots \mathfrak{b}_g)^e,$$

where $e = (\mathfrak{b}_i/\mathfrak{p})$ if the ramification index.

If $\mathfrak{b}$ is one of the primes of L extending $\mathfrak{p}$, we set

$$G(\mathfrak{b}) := \{\sigma \in G(L/K) : \sigma(\mathfrak{b}) = \mathfrak{b}\},$$

and we will cal $G(\mathfrak{b})$ the ***decomposition group*** of $\mathfrak{b}$. We also define

$$T(\mathfrak{b}) := \ker\left(G(\mathfrak{b}) \longrightarrow G(R'/\mathfrak{b} \Big/ R/\mathfrak{p}), \quad \sigma \mapsto \bar{\sigma}\right)$$

as the ***inertia group*** of $\mathfrak{b}$, where $\mathfrak{p}$ is a finite prime of K, R is the valuation ring corresponding to $\mathfrak{p}$ ($\mathfrak{p}$ the maximal ideal of R), R' is the integral closure of R in L and $\mathfrak{b}$ is a prime ideal of R' with $\mathfrak{p} \subset \mathfrak{b}$ so that we have a map $\bar{\sigma}(x + \mathfrak{b}) = \sigma(x) + \mathfrak{b}$.

Proposition 5.2.4 (***conjugate primes***)**.** Let $\tau \in G(L/K)$. Then $G(\tau(\mathfrak{b})) = \tau G(\mathfrak{b})\tau^{-1}$ and

$$\left[\frac{L/K}{\tau(\mathfrak{b})}\right] = \tau \left[\frac{L/K}{\tau(\mathfrak{b})}\right] \tau^{-1}. \tag{57}$$

Proof: Any element in the ring of algebraic integers of L can be written as $\tau^{-1}(x)$ with x an algebraic integer.
Consider the automorphism

$$y \mapsto y^q, \quad y \in L.$$

Then there is a unique coset $\sigma T(\mathfrak{b}) \subset G(\mathfrak{b})$ all of whose elements satisfy

$$\left[\frac{L/K}{\mathfrak{b}}\right] \tau^{-1}(x) \equiv \tau^{-1}(x)^q \pmod{\mathfrak{b}}.$$

Apply τ to conclude

$$\tau \left[\frac{L/K}{\tau(\mathfrak{b})}\right] \tau^{-1}(x) \equiv x^q \pmod{\tau(\mathfrak{b})}.$$

The uniqueness of the Frobenius automorphism implies the equality (57). □

Definition 5.2.5. A prime $\mathfrak{p}$ of K ***splits completely*** in an extension L if

$$e(\mathfrak{b}/\mathfrak{p}) = f(\mathfrak{b}/\mathfrak{p}) = 1,$$

for any prime $\mathfrak{b}$ of L extending $\mathfrak{p}$.

Remark 5.2.6. An equivalent statement when L/K is Galois is that $\mathfrak{p}$ splits completely in L if $\mathfrak{p}$ has $[L : K]$ distinct extensions to primes of L.

Proposition 5.2.7 (***splitting***)**.** The unramified prime $\mathfrak{p}$ splits completely in L if and only if

$$\left[\frac{L/K}{\mathfrak{p}}\right] = 1.$$

Proof: See [J] Chapter III, 2.5.

References

[AL] Atkin, A.O.L., Lehner, *J. Hecke operators on* $\Gamma_0(m)$. Math. Ann. 185, 134–160 (1970)

[C] David A. Cox, *Primes of the form* $x^2 + ny^2$*: Fermat, class field theory, and complex multiplication.* John Wiley & Sons, Inc. (1989)

[DS] F. Diamond and J. Shurman, *A First Course in Modular Forms.* (2008)

[EF] Serge Lang, *Elliptic functions.* Graduate texts in mathematics, Springer-Verlag (1987)

[J] Gerald J. Janusz, *Algebraic number fields.* Second Edition, Graduate Studies in Mathematics, Volume 7, American Mathematical Society (1996)

[K] Neal Koblitz, *Introduction to Elliptic Curves and Modular Forms.* Second Edition, Graduate Texts in Mathematics, Springer-Verlag New York (1984)

[Kan] Masanobu Kaneko, *Traces of singular moduli and the Fourier coefficients of the elliptic modular function* $j(\tau)$. CRM Proceedings and Lecture Notes, Vol. 19. pp. 173-176. (1999)

[KH] Kohnen, W. *Modular forms of half-integral weight on* $\Gamma_0(4)$. Math. Ann. 248, 249–266 (1980)

[Knopp] M. I. Knopp, *Modular Functions in Analytic Number Theory.* Manhatan, Chicago (1970)

[Kohl] G. Köhler, *Eta Products and Theta Series Identities.* Springer Monographs in Mathematics (2010)

[Z] D. Zagier, *Traces of singular moduli.* Motives, polylogarithms and Hodge theory, Part I (Irvine, CA, 1998), Int. Press Lect. Ser., vol. 3, Int. Press, Somerville, MA, pp. 211-244 (2002)

[Zag] D. Zagier, *Modular forms and differential operators.* Proc. Indian Acad. Sci. (Math. Sci.), Voi. 104, No. 1, pp. 57-75. (1994)