Complex Elliptic Curves

Manuel Trachsler, Nikomedes Mojado

17.11.2020

Contents

1 Recap and the Basis Lemma

1.1 Introduction

This text follows mainly the third and fourth chapter of the first section of [1] and relies only so slightly on the first chapter of said section. Our starting point today will be lattices in the complex plane. For any two numbers ω_1 and ω_2 in $\mathbb{C}$ whose quotient does not lie in $\mathbb{R}$ we define the lattice of these two numbers as the set of points $\{a\omega_1 + b\omega_2 \in \mathbb{C}\}$ with $a, b \in \mathbb{Z}$. This lattice forms a subgroup of $\mathbb{C}$. The most common sign for a lattice is a capital Omega, Ω.

Remark 1.1. In some cases, a lattice is defined as a countable subgroup of any topological group so that its quotient has a finite Haar measure.

Definition 1.2. We call the ordered pair of (ω_1, ω_2) the **basis** of the lattice.

Remark 1.3. As $\mathbb{C}$ is abelian, the quotient of the lattice with the overlying group has itself a group structure.

Definition 1.4. For a Lattice Ω with basis ω_1, ω_2 and any given $u \in \mathbb{C}$ we denote the **tile of the lattice spanned at u** by

$$\Diamond(u, \omega_1, \omega_2) := \{u + a_1\omega_1 + a_2\omega_2\}$$

for $a_i \in [0, 1]$. In the case where $u = 0$ we omit the u and write $\Diamond(\omega_1, \omega_2)$.

Definition 1.5. The **diameter** of a lattice Ω with basis ω_1, ω_2 is denoted by δ and defined as follows:

$$\delta(\omega_1, \omega_2) := \sup\{|z - w|; z, w \in \Diamond(\omega_1, \omega_2)\}.$$

Definition 1.6. For any given $\rho > 0$ we set $\mathbf{A}_\rho(\mathbf{\Omega})$ to be the set of lattice points at least ρ-close to zero:

$$A_\rho(\Omega) = \#\{\omega \in \Omega : |\omega| \leq \rho\}$$

Definition 1.7. The **area** of a single tile is denoted by $Vol\Omega$.

1.2 The Basis Lemma

In this section we will state (and prove) a Lemma that gives us a way to determine whether two different bases span the same lattice.

Lemma 1.8. Let Ω be a lattice in $\mathbb{C}$ with basis $\omega := (\omega_1, \omega_2)$. For two other numbers $z := (z_1, z_2)$ we then have

(1) z_1 and z_2 lie in Ω if and only if there exists a $U \in \mathbb{Z}^{2\times 2}$ with $z = U\omega$.

(2) z is a basis of Ω if and only if the matrix U from Statement (1) lies in $GL(2, \mathbb{Z})$.

Proof. We proved this in the previous week. □

2 Eisenstein, Weierstrass and their Friends

2.1 Eisenstein

Lemma 2.1. We have the following (technical) inequality:

$$\frac{\pi}{Vol\Omega}(\rho-\delta)^2 \leq A_\rho(\Omega) \leq \frac{\pi}{Vol\Omega}(\rho+\delta)^2$$

for all $\rho \geq \delta$, where δ is the diameter (1.5) of Ω.

Proof. Let $K_\rho := \{z \in \mathbb{C} : |z| \leq \rho\}$ and $M_\rho := \bigcup_{\omega\in\Omega,|\omega|\leq\rho} \Diamond(\omega,\omega_1,\omega_2)$. Then we have

$$K_{\rho-\delta} \subset M_\rho \subset K_{\rho+\delta}.$$

Now we compute the volumes: $Vol(K_{\rho\pm\delta}) = \pi(\rho\pm\delta)^2$ and $Vol(M_\rho) = Vol\Omega \cdot A_\rho(\Omega)$. This then gives the inequality. □

Lemma 2.2. For a lattice Ω the following sequence converges if and only if $\alpha > 2$:

$$\sum_{0\neq\omega\in\Omega} |\omega|^{-\alpha}$$

Proof. Let $\alpha > 2$ and $E \subset \Omega \setminus \{0\}$ be a finite non-empty subset and let $M := \max\{|\omega|, \omega \in E\}$. Using the Lemma 2.1 we compute a first bound:

$$A_{n+1}(\Omega) - A_n(\Omega) \leq \frac{\pi}{Vol\Omega}\Big((n+1+\delta)^2 - (n-\delta)^2\Big) \leq c_2 n$$

for all $n \geq \delta$. Finally, by taking

$$c_1 := \sum_{0\neq|\omega|\leq\delta+1} |\omega|^{-\alpha}$$

we get

$$\begin{aligned}\sum_{\omega\in E} |\omega|^{-\alpha} &\leq c_1 + \sum_{n\in\mathbb{N},\delta<n<M} (A_{n+1}(\Omega) - A_n(\Omega))n^{-\alpha} \\ &\leq c_1 + c_2 \sum_{n=1}^{\infty} n^{1-\alpha} := C < \infty.\end{aligned}$$

This concludes the $\alpha > 2$ case. For $\alpha \leq 0$ the series must diverge for obvious reasons. Let now $\alpha \in (0, 2]$ and $\mathbb{N} \ni N > 2\delta$. We obtain a constant $c_3 > 0$ by setting

$$A_{kN}(\Omega) - A_{(k-1)N}(\Omega) \geq \frac{\pi}{Vol\Omega}\Big((kN-\delta)^2 - ((k-1)N+\delta)^2\Big) \geq c_3 k$$

for all integers $2 \leq k$. Setting $E_n := \{\omega \in \Omega : 0 < |\omega| \leq nN\}$ we have

$$\sum_{\omega\in E_n} |\omega|^{-\alpha} \geq \sum_{k=2}^{n} \big(A_{kN}(\Omega) - A_{(K-1)n}(\Omega)\big)(kN)^{-\alpha} \geq c_3 N^{-\alpha} \sum_{k>1} k^{1-\alpha}.$$

As the last sum diverges, the first sequence also diverges, yielding us the result. □

The main upshot of the above computations was to show that the so called Eisenstein series are indeed well defined:

Definition 2.3. We define the **Eisenstein series** G_k as

$$G_k \equiv G_k(\Omega) := \sum_{0\neq\omega\in\Omega} \omega^{-k}.$$

In particular, for $k \geq 3$ they are absolutely convergent series.

Lemma 2.4. If k is odd we have $G_k(\Omega) = 0$.

Proof. As $\omega \in \Omega$ if and only if $-\omega \in \Omega$ we have $G_k = (-1)^k G_k$ for all k, giving the result. □

2.2 Weierstrass

Lemma 2.5. Let K be a compact set contained in $\{(\omega_1, \omega_2) \in \mathbb{C} \times \mathbb{C}$ with $\omega_2 \neq 0$ and $\frac{\omega_1}{\omega_2} \notin \mathbb{R}\}$. Then there exist real constants $a, b > 0$ so that:

$$a|m_1 i + m_2| \leq |m_1\omega_1 + m_2\omega_2| \leq b|m_1 i + m_2|$$

for all $m_1, m_2 \in \mathbb{R}$ and all points in K.

We can think of this statement as "every compact set that does not touch lattice points can be scaled down to fit in the $1 + i$ lattice".

Proof. We can assume that $m_1 i + m_2$ lies on the unit sphere: $m_1^2 + m_2^2 = 1$. We then observe the continuous (non-negative) map given by

$$(\omega_1, \omega_2, m_1, m_2) \longmapsto |m_1\omega_1 + m_2\omega_2|.$$

This continuous map assumes a minimum a and a maximum b on the compact set $K \times \{(m_1, m_2) \in \mathbb{R} \times \mathbb{R}; m_1^2 + m_2^2 = 1\}$. As ω_1 and ω_2 are not linearly dependent over $\mathbb{R}$, the map does not have nontrivial roots. Therefore both a and b are greater than zero. □

Now we define a sequence $\wp(z, \omega_1, \omega_2)$. We will hold on to the three arguments for now but drop them later on:

Definition 2.6. The so-called **Weierstrass-p Function** of a lattice Ω is defined through the following sequence and has standard notation $\wp$:

$$\wp(z, \omega_1, \omega_2) := z^{-2} + \sum_{0 \neq \omega \in \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2} \big((z-\omega)^{-2} - \omega^{-2}\big).$$

Lemma 2.7. The sequence $\wp(z, \omega_1, \omega_2)$ converges absolutely on every compact set satisfying the following three assumptions:

- $\omega_2 \neq 0$
- $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$
- $z \notin \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

Casually speaking, this is to say that it converges whenever the lattice Ω with basis (ω_1, ω_2) is nice enough and z does not lie on it.

Proof. Let K be such a compact set. K is then contained in the product of two compact sets K_ρ and K', where $K_\rho := \{z \in \mathbb{C} : |z| \leq \rho\}$ is the closed ball around origin with radius $\rho > 0$ and $K' \subset \{(\omega_1, \omega_2) \in \mathbb{C} \times \mathbb{C}$ a compact subset as in the previous lemma, 2.5.

$$K \subset K_\rho \times K'.$$

For K' we pick an a as in the previous lemma 2.5 so that we have for all $(z, \omega_1, \omega_2) \in K$ and $m_1, m_2 \in \mathbb{Z}$ with $|m_1 i + m_2| \geq \frac{\rho+1}{a}$ the inequalities

$$|m_1\omega_1 + m_2\omega_2| =: |\omega| \geq \rho + 1.$$

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| = \left|\frac{2z\omega - z^2}{\omega^2(z-\omega)^2}\right| = \left|\frac{2 - z/\omega}{(1-z/\omega)^2}\right| \frac{|z|}{|\omega|} \ldots$$

$$\ldots \leq \frac{3}{(1-\rho/(\rho+1))^2} \frac{\rho}{|\omega|^3} \leq \frac{3\rho(\rho+1)^2}{a^3 |m_1 i + m_2|^3}$$

There are only finitely many pairs m_1, m_2 with $|m_1\omega_1 + m_2\omega_2| =: |\omega| \geq \rho + 1$ and therefore the claim of absolute convergence follows from the absolute convergence of the Eisenstein series of $G_3(\mathbb{Z}i + \mathbb{Z})$ from the convergence lemma 2.2. □

The following lemma has an analogous proof.

Lemma 2.8. Let Ω be a fixed lattice. Then for $k \in \mathbb{N}$ and $k \geq 3$ the series

$$\sum_{\omega \in \Omega} (z-\omega)^{-k}$$

converges absolutely and uniformly on every compact set in $\mathbb{C} \setminus \Omega$.

From now on we will denote the Weierstrass-$\wp$ function by

$$\wp(z) = \wp_\Omega(z) := z^{-2} + \sum_{0 \neq \omega \in \Omega} \left((z-\omega)^{-2} - \omega^{-2}\right), z \in \mathbb{C} \setminus \Omega,$$

which converges absolutely uniformly on every compact set disjoint to the lattice Ω as mentioned above in (2.7). For notations sake let us set $f_\omega(z)$ to be

$$f_\omega(z) := (z-\omega)^{-2} - \omega^{-2},$$

that is the "number we need to sum" in the sequence $\wp(z)$ at each lattice point.

The Weierstrass-$\wp$ function satisfies several other properties listed below.

Lemma 2.9. The $\wp$-function is a meromorphic function with poles of order 2 at every lattice point Ω.

Proof. Let $\rho > 0$. Then

$$\wp(z) = z^{-2} + \sum_{|\omega| < \rho+1} f_\omega(z) + \sum_{|\omega| \geq \rho+1} f_\omega(z).$$

The first sum is meromorphic on $\{|z| \leq \rho\}$ and the second sum is holomorphic on the same domain. Thus $\wp$ has poles on $\Omega \cap \{|z| \leq \rho\}$ of degree 2 with residue 0. □

Lemma 2.10. The function $\wp$ is an even function - that is that the Laurent series has only entries in the degrees $\{-2, 2, 4, ...\}$.

Proof. This statement follows from the fact that $\wp(-z) = \wp(z)$ and $f_\omega(0) = 0$. (Attention: $\wp(0) \neq 0$ as $0 \in \Omega$ and thus not defined). □

Lemma 2.11. We have $\wp(z+\omega) = \wp(z)$ for all $\omega \in \Omega$ and all $z \notin \Omega$.

Proof. Using lemma 2.8, we have the absolutely uniformly convergent series:

$$\wp'(z) = -2 \sum_{\omega \in \Omega} (z-\omega)^{-3}.$$

From this it follows that $\wp'(z+\omega) = \wp'(z)$ and thus if Ω is spanned by ω_1 and ω_2 then for $k = 1, 2$ we have $\wp(z+\omega_k) = \wp(z) + C_k$.

Next, if we take $z = -\omega_k/2$ then $C_k = 0$ as the function is even. This means $\wp(z+\omega_k) = \wp(z)$ for $k = 1, 2$ and $\wp$ has periods $\omega \in \Omega$. In other words, it's elliptic. □

These lemmas, together with the convergence lemma (2.7), make up the construction theorem for the $\wp$-function.

2.3 Linking Eisenstein and Weierstrass

Our main goal now is to use the Eisenstein Series in order to get a better insight to the $\wp$-function. Recall the Eisenstein Series

$$G_k := G_k(\Omega) := \sum_{0 \neq \omega \in \Omega} \omega^{-k}.$$

Additionally we set

$$\gamma = \gamma(\Omega) := \min\{|\omega| : 0 \neq \omega \in \Omega\}$$

and we get the following theorem.

Theorem 2.12. For all $z \in \mathbb{C}$ satisfying $0 < |z| < \gamma(\Omega)$ we have

$$\begin{aligned}\wp(z) &= z^{-2} + \sum_{n=2}^{\infty}(2n-1)G_{2n}z^{2n-2} \\ &= z^{-2} + 3G_4z^2 + 5G_6z^4 + ...\end{aligned}$$

Proof. In a first step we look at the derivative of the function $f(t) = \frac{1}{1-t}$. In the open unit ball we have $\frac{d}{dt}f = \frac{1}{(1-t)^2} = \sum_{m=1}^{\infty} mt^{m-1}$. We now extrapolate this to our context: For $\omega \neq 0, |z| < \gamma$ we have

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

This means we have:

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

Additionally we have that

$$\left|m\frac{z^{m-1}}{\omega^{m+1}}\right| \leq \gamma m\left(\frac{|z|}{\gamma}\right)^{m-1}|\omega|^{-3}$$

and due to the convergence lemma 2.2 we have that this sequence is absolutely convergent in m and ω. We are thus allowed to rearrange the sum which gives us

$$\wp(z) = z^{-2} + \sum_{m \geq 2} mG_{m+1}z^{m-1}.$$

□

Theorem 2.13. An important differential Equation. Set $g_2 := 60G_4$ and $g_3 = 140G_6$. The $\wp$-function satisfies the following differential equation:

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3.$$

Proof. This is a brute force proof so bear with me: We know

$$\wp(z) = z^{-2} + 3G_4 z^2 + 5G_6 z^4 + O(z^6).$$

We then compute the following:

$$\begin{aligned}
\wp^2(z) &= z^{-4} &&+ 6G_4 &&+ 10G_6 z^2 + O(z^3) \\
\wp^3(z) &= z^{-6} &&+ 9G_4 z^{-2} &&+ 15G_6 + O(z) \\
\wp'(z) &= -2z^{-3} &&+ 6G_4 z &&+ 20G_6 z^3 + O(z^5) \\
\wp'^2(z) &= 4z^{-6} &&- 24G_4 z &&- 80G_6 + O(z).
\end{aligned}$$

Now we compare and see that

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

The left hand side of this equation is smooth enough (lol ok) and if it has poles, then only where $\wp$ and $\wp'$ have poles. Additionally though, the left-hand side is holomorphic at 0 and thus everywhere. Therefore it is constant. But if it is $O(z)$, the constant must be zero, so our assertion holds. □

Remark 2.14. g_2 and g_3 are the so called **Weierstrass invariants** or **elliptic invariants**. They uniquely define a lattice and therefore so do G_4 and G_6.

2.4 The constants e_1, e_2, e_3

We now define three constants $e_k, k = 1, 2, 3$ and explore their properties. They will help us find some rather special invariants of a lattice.

Definition 2.15. Let Ω be a lattice spanned by the two numbers ω_1 and ω_2. Then we set

(1) $\omega_3 := \omega_1 + \omega_2$

(2) $e_k = \wp(\omega_k/2)$ for $k = 1, 2, 3$.

With these function values at half-periods of $\wp$, we can now formulate a second differential equation.

Theorem 2.16. For all $z \in C \setminus \Omega$ we have

$$\wp'^2(z) = 4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3)$$

Proving this would take a lot of time, so we skip its derivation.

$\wp$ assumes more than three different values. By taking any variable X over $\mathbb{C}$ we can use the new equation to get the following result.

Theorem 2.17. The following equality holds true for all $X \in \mathbb{C}$:

$$4X^3 - g_2X - g_3 = 4(X - e_1)(X - e_2)(X - e_3).$$

We can now express the lattice invariants in terms of the values e_k.

Corollary 2.18.

$$\begin{aligned} 0 &= e_1 + e_2 + e_3 \\ g_2 &= -4(e_1e_2 + e_2e_3 + e_3e_1) \\ g_3 &= 4e_1e_2e_3. \end{aligned}$$

Corollary 2.19.

$$g_2^3 - 27g_3^2 = 16(e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2 \neq 0 \tag{2.1}$$

Proof. This proof is rather technical and just uses the identities from the previous corollary (2.19), so we skip this here. □

2.5 Discriminant and j-Invariant

With the help of our e_k and the properties above we can finally define the aforementioned special invariants.

Definition 2.20. The left hand side of equation (2.1) is called the **Discriminant**. We denote

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

Definition 2.21. The **(absolute) j-invariant** of the Lattice Ω is denoted by j and defined as follows:

$$j = j(\Omega) := \frac{(12g_2)^3}{\Delta}.$$

Corollary 2.22.

$$j = -4(12)^3 \frac{\left(\sum_{i \neq j} e_i e_j\right)^3}{\sum_{i \neq j}(e_i - e_j)^2}$$

and setting $\lambda := \frac{e_2 - e_3}{e_1 - e_3}$ we get

$$j = 256 \frac{(1 - \lambda + \lambda^2)^3}{\lambda^2(1 - \lambda)^2}.$$

We will see in later talks, that these defined invariants of a lattice are several examples of modular forms.

3 The Interplay between $SL(2,\mathbb{Z})$ and...

3.1 The lattice

Remark 3.1. If Ω is a lattice, then $\lambda\Omega$ is also a lattice. We then have directly from (2.3) and (2.6):

$$\wp_{\lambda\Omega} = \lambda^{-2}\wp_\Omega$$

$$G_k(\lambda\Omega) = \lambda^{-k}G_k(\Omega).$$

for $k \geq 3$.
Using the definitions of g_2 and g_3 from theorem (2.13) as well as the definitions of the j-invariant (2.21) and the discriminant Δ (2.20) we then have:

$$\begin{aligned} g_2(\lambda\Omega) =& \lambda^{-4}g_2(\Omega) && (3.1)\\ g_3(\lambda\Omega) =& \lambda^{-6}g_3(\Omega) && (3.2)\\ \Delta(\lambda\Omega) =& \lambda^{-12}\Delta(\Omega) \\ j(\lambda\Omega) =& j(\Omega). && (3.3) \end{aligned}$$

In fact, for (3.3) the converse is true. Take a look at the following lemma.

Lemma 3.2. For two lattices Ω and Ω' the following two statements are equivalent

(i) There is a $0 \neq \lambda \in \mathbb{C}$ so that $\Omega' = \lambda\Omega$.

(ii) $j(\Omega) = j(\Omega')$.

Proof. (i) $\implies$ (ii): This is exactly the statement under equation (3.3).
(ii) $\implies$ (i): Let first $j(\Omega') = j(\Omega) \neq 0$. Then $g_2(\Omega) \neq 0$ and $g_2(\Omega') \neq 0$. Using equation (3.1) there must be a non-zero $\lambda \in \mathbb{C}$ so that

$$g_2(\Omega') = \lambda^{-4}g_2(\Omega) = g_2(\lambda\Omega).$$

Then using the definitions (2.20) and (2.21) and equation (3.2) we can see that

$$g_3(\Omega') = \pm\lambda^{-6}g_3(\Omega) = \pm g_3(\lambda\Omega).$$

Up to replacing λ with $i\lambda$ we have $g_2(\Omega') = g_2(\lambda\Omega)$ and $g_3(\Omega') = g_3(\lambda\Omega)$, yielding $\Omega' = \lambda\Omega$ by (2.14).

In the case that $j(\Omega')$ and thus also $j(\Omega)$ equals to zero, g_2 is zero too. But g_3 is always non-zero by (2.22). So the statement follows analogously. □

Recall that $\wp$ and G_k do only depend on the lattice Ω but not on its basis. Let $\omega = (\omega_1, \omega_2)$ and $\omega' = (\omega_1', \omega_2')$ be two bases of Ω. So for $k \geq 3$ we get by the basis lemma (1.8):

$$\wp(z;\omega_1',\omega_2') = \wp(z;\omega_1,\omega_2), \qquad G_k(\omega_1',\omega_2') = G_k(\omega_1,\omega_2), \qquad (3.4)$$

where

$$\begin{pmatrix}\omega_1'\\ \omega_2'\end{pmatrix} = U\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}, \qquad U = \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in GL(2;\mathbb{Z}),$$

scaled lattices, we can also write for a $0 \neq \lambda \in \mathbb{C}$ and $k \geq 3$:

$$\wp(\lambda z; \lambda\omega_1, \lambda\omega_2) = \lambda^{-2}\wp(z;\omega_1,\omega_2),$$
$$G_k(\lambda\omega_1, \lambda\omega_2) = \lambda^{-k}G_k(\omega_1,\omega_2). \tag{3.5}$$

As ω_1 and ω_2 are linearly independent over $\mathbb{R}$, multiplying ω_1 by -1 still spans the same lattice. We can thus conveniently assume that the quotient $\tau := \frac{\omega_1}{\omega_2}$ has positive imaginary part. We then apply equation (3.4) and (3.5) to get the following for $k \geq 3$:

$$\wp(z;\omega_1,\omega_2) = \omega_2^{-2}\wp(z/\omega_2;\tau,1), \qquad G_k(\omega_1,\omega_2) = \omega_2^{-k}G_k(\tau,1).$$

This allows us to restrict our attention entirely to lattices generated by $\tau\mathbb{Z}+\mathbb{Z}$ where τ lies in the upper half plane: $\mathbb{H} := \{\tau \in \mathbb{C} : Im(\tau) > 0\}$.

This raises the question, how we move between lattices Ω and Ω' with bases of the form $(\tau,1)$ and $(\tau',1)$ respectively. Consider

$$\tau' := \frac{\omega_1'}{\omega_2'} = \frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2} = \frac{a\tau+b}{c\tau+d}.$$

This has imaginary part $Im(\tau') = \frac{ad-bc}{|c\tau+d|^2}\cdot Im(\tau)$. So if we wish to move from Ω with basis $(\tau,1)$ to $\frac{1}{c\tau+d}\Omega$ with basis $(\tau',1)$ with $\tau' \in \mathbb{H}$, we are only allowed to use matrices $U = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$ from the **special linear group over** $\mathbb{Z}$, $SL(2;\mathbb{Z}) := \{U \in GL(2;\mathbb{Z}); det(U) = 1\}$.

Now by using (3.5) and our definitions of the bases we can write (3.4) in the following form:

$$\wp(\frac{z}{c\tau+d}; \tau' = \frac{a\tau+b}{c\tau+d}, 1) = (c\tau+d)^2 \cdot \wp(z;\tau,1)$$

respectively for $k \geq 4$

$$G_k(\frac{a\tau+b}{c\tau+d}, 1) = (c\tau+d)^k \cdot G_k(\tau,1). \tag{3.6}$$

Here are $a,b,c,d \in \mathbb{Z}$ and $ad-bc = 1$.

3.2 Eisenstein Series

Now that we can restrict our lattices, we redefine G_k for even $k \geq 4$ (recall that G_k was shown to be zero for odd k in lemma 2.4).

$$G_k(\tau) := G_k(\tau,1)$$
$$G_k(\tau) = \sum_{(m,n)\in\mathbb{Z}\times\mathbb{Z}\setminus(0,0)} (m\tau+n)^{-k}. \tag{3.7}$$

We look at the G_k as maps $G_k : \mathbb{H} \to \mathbb{C}$ with the definition above.

Lemma 3.3. For $\tau \in \mathbb{H}$ and integers $k \geq 2$ we have:

$$\sum_{n\in\mathbb{Z}} (\tau + n)^{-k} = \frac{(-2\pi i)^k}{(k+1)!} \sum_{r=1}^{\infty} r^{k-1} e^{2\pi i r\tau}$$

This lemma will be important in providing a Fourier expansion of the Eisenstein series.

Proof. From a different source (namely Remmert's book on complex analysis [2, Theorem 11.2.1]) we get the following partial fraction decomposition:

$$\left(\frac{\pi}{\sin \pi\tau}\right)^2 = \sum_{n\in\mathbb{Z}} (\tau + n)^{-2}, \tau \notin \mathbb{Z}.$$

The right hand side converges uniformly on every compact set disjoint from $\mathbb{Z}$. If we choose $\tau \in \mathbb{H}$, we get because of $|e^{2\pi i r}| = e^{-2\pi Im(\tau)} < 1$:

$$\left(\frac{\pi}{\sin \pi\tau}\right)^2 = \left(\frac{2\pi i}{e^{\pi i\tau} - e^{-\pi i\tau}}\right)^2 = (-2\pi i)^2 e^{2\pi i\tau} \frac{1}{(1 - e^{2\pi i\tau})^2} = (-2\pi i)^2 \sum_{r=1}^{\infty} r e^{2\pi i r\tau}.$$

This already shows the lemma for $k = 2$.

Since both sides converge uniformly in τ, we can easily get to the general case by repeatedly taking the derivative of τ on both sides. □

Notice that the left hand side is periodic in τ with period 1.

Theorem 3.4. For all $\tau \in \mathbb{H}$ and even integers $k \geq 4$ we have:

$$G_k(\tau) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!} \sum_{m=1}^{\infty} \sigma_{k-1}(m) \cdot e^{2\pi i m\tau} \tag{3.8}$$

where we define:

$$\zeta(s) := \sum_{m=1}^{\infty} m^{-s}$$

$$\sigma_k(m) := \sum_{d\in\mathbb{N}, d|m} d^k$$

For $\epsilon > 0$ the equation (3.8) converges on $\{\tau \in \mathbb{H} : Im(\tau) \geq \epsilon\}$ absolutely and uniformly. Additionally, all G_k are holomorphic on $\mathbb{H}$ and satisfy:

$$G_k\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k G_k(\tau)$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z})$.

This theorem is useful in multiple ways: It characterizes the Eisenstein series on our model lattice in form of a Fourier sequence, shows how it behaves under $SL(2,\mathbb{Z})$ actions and additionally we can follow that the G_k are nontrivial modular forms of weight k.

Proof. Due to the convergence lemma 2.2 we can manipulate equation (3.7):

$$G_k(\tau) = \sum_{n\neq 0} n^{-k} + \sum_{m\neq 0}\sum_{n\in\mathbb{Z}} (m\tau+n)^{-k} = 2\zeta(k) + 2\sum_{m=1}^{\infty}\sum_{n\in\mathbb{Z}} (m\tau+n)^{-k}.$$

The conditions $m = 0$ and $n \neq 0$ are covered in the first summation and the other summation runs over the rest of the cases. In the second step we only consider positive m and n but then double the sum. We now plug in lemma 3.3 and get:

$$G_k(\tau) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{s=1}^{\infty}\sum_{r=1}^{\infty} r^{k-1}e^{2\pi irs\tau}$$

Now by taking $rs = m$ we obtain (3.8). Holomorphy follows from the local uniform convergence of lemma 3.3 and finally the last equation is just another way of writing equation (3.6). □

Remark 3.5. Using the facts that $\zeta(4) = \frac{\pi^4}{90}$ and $\zeta(6) = \frac{\pi^6}{945}$ we obtain two explicit Eisenstein series:

$$G_4(\tau) = \frac{\pi^4}{45}\left(1 + 240\sum_{m=1}^{\infty}\sigma_3(m)\cdot e^{2\pi im\tau}\right)$$
$$G_6(\tau) = \frac{2\pi^6}{945}\left(1 - 504\sum_{m=1}^{\infty}\sigma_5(m)\cdot e^{2\pi im\tau}\right)$$

3.3 The Discriminant

Recall the definitions in Theorem 2.13 and Definition 2.20:

$$g_2(\tau) := 60G_4(\tau)$$
$$g_3(\tau) := 140G_6(\tau)$$
$$\Delta(\tau) := g_2^3(\tau) - 27g_3^2(\tau)$$

Using Remark 3.5 we have the identities

$$g_2(\tau) = \frac{(2\pi)^4}{12}\left(1 + 240\sum_{m=1}^{\infty}\sigma_3(m)e^{2\pi im\tau}\right) \tag{3.9}$$
$$g_3(\tau) = \frac{(2\pi)^6}{216}\left(1 - 504\sum_{m=1}^{\infty}\sigma_5(m)e^{2\pi im\tau}\right). \tag{3.10}$$

Theorem 3.6. The Fourier series of the discriminant Δ is defined as follows for $\tau \in \mathbb{H}$:

$$\Delta(\tau) = (2\pi)^{12} \sum_{m=1}^{\infty} \tau_m e^{2\pi i m \tau}.$$

Additionally, τ_m lies in $\mathbb{Z}$ with $\tau_1 = 1$. Therefore, $\Delta : \mathbb{H} \to \mathbb{C}$ can be viewed as a holomorhphic, non-zero function. Finally, we observe its behaviour under $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z})$:

$$\Delta\Big(\frac{a\tau + b}{c\tau + d}\Big) = (c\tau + d)^{12} \Delta(\tau).$$

Proof. We set the abbreviations A and B:

$$A := \sum_{m=1}^{\infty} \sigma_3(m) e^{2\pi i m \tau}$$
$$B := \sum_{m=1}^{\infty} \sigma_5(m) e^{2\pi i m \tau}.$$

By plugging in the abbreviations into equations (3.9) and (3.10) we get

$$\Delta(\tau) = \frac{(2\pi)^{12}}{1728}\big((1 + 240A)^3 - (1 - 504B)^2\big) = (2\pi)^{12}\big(e^{2\pi i \tau} + ...\big) \qquad (3.11)$$

Tis notation suggests that we can write the discriminant as a power series in $q = e^{2\pi i r}$. We now want to show that the coefficients of such a power series lie in $\mathbb{Z}$ as claimed by the statement.

Observe that for $d \in \mathbb{Z}$ we have $d^3 \equiv d^5$ in $\mathbb{Z}/12\mathbb{Z}$ (see the below Lemma 3.7). So therefore $\sigma_3(m) \equiv \sigma_5(m)$ in $\mathbb{Z}/12\mathbb{Z}$. Thus $A \equiv B \mod 12$ and lastly; modulo 1728 we have

$$(1 + 240)^3 - (1 - 504B)^2 \equiv 12^2(5A + 7B) \equiv 0.$$

This means that the 1728 in (3.11) is cancelled out in all coefficients of the power series yielding it an power series with integer coefficients as claimed. □

Lemma 3.7. For any integer $d \in \mathbb{Z}$ we have

$$d^3 \equiv d^5 \mod 12$$

Proof. First we show that we can consider numbers a that are smaller than 12. Set $d = 12k + a$ then

$$\begin{aligned} d^3 &= (12k + a)^3 \\ &= 12^3k^3 + 3(12^2k^2a) + 3(12ka^2) + a^3 \\ d^3 &\equiv a^3 \end{aligned}$$

and

$$\begin{aligned} d^5 &= (12k+a)^5 \\ &= 12^5k^5 + 5(12^4k^4a) + 10(12^3k^3a^2) + 10(12^2k^2a^3) + 5(12ka^4) + a^5 \\ d^5 &\equiv a^5 \end{aligned}$$

Now we brute force it:

- For $a = 1$ the statement is clear
- For $a = 2$ we have $32 \equiv 8$.
- For $a = 3$ we have $27 = 24 + 3$ and $243 = 240 + 3$
- The cases $a = 4$ and $a = 8$ work the same way as $a = 2$
- The cases $a = 5$, $a = 7$ and $a = 11$ have the common property that $a^2 \equiv 1$ and thus $a^5 = a^3a^2$ yields the result.
- For $a = 6$, we have 0 in both powers
- Finally $a = 9$ and $a = 10$ can be concluded from their divisors.

□

3.4 The j-Invariant

Last but not least, we take a closer look at the j-invariant. Recall its definition—in a new dress, now that we can restrict the lattices we study:

$$j(\tau) := \frac{\big(12g_2(\tau)\big)^3}{\Delta(\tau)}$$

Remark 3.8. In the theorem above we defined $\Delta(\tau)$ for all $\tau \in \mathbb{H}$ allowing us to write $\Delta(\tau)$ as a Fourier series. We will use a convergence lemma, 3.9, stated below to show that in our case the quotient of the two power series is still a converging power series with coefficients in $\mathbb{Z}$.

Lemma 3.9. Let $f = \sum_{n\geq 0} a_n q^n$ and $g \sum_{n\geq 0} b_n q^n$ be power series which converge for $|q| < 1$ and satisfy $a_n, b_n \in \mathbb{Z}$. Additionally, assume $b_0 = 0$ and $g(q) \neq 0$. Then the quotient $\frac{f}{g}$ also converges in the same domain and has integer coefficients.

Theorem 3.10. The j-invariant can be seen as a holomorphic map: $j : \mathbb{H} \to \mathbb{C}$ admitting a Fourier series with integer coefficients:

$$\begin{aligned} j(\tau) &= e^{-2\pi i\tau} + \sum_{m\geq 0} j_m e^{2\pi i m\tau} \qquad (3.12) \\ &= e^{-2\pi i\tau} + 744 + 196884e^{2\pi i\tau} + ... \end{aligned}$$

Again, we have its behaviour under $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z})$:

$$j\Big(\frac{a\tau+b}{c\tau+d}\Big) = j(\tau).$$

Proof. Holomorphy follows from the previous statements: We know from theorem 3.6 that the discriminant is holomorphic and we have established at the latest in Theorem 3.4 that $g_2(\tau) = 60G_4(\tau)$ can be viewed as holomorphic map. Additionally, we get the claimed formula in equation (3.12) by brute force computing it through the Fourier series of $g_2(\tau)$ and the Fourier series of the discriminant, both in Theorem 3.6.

Last but not least, the invariance under $SL(2,\mathbb{Z})$ arises from the respective $SL(2,\mathbb{Z})$ - statements of Theorems 3.4 and 3.12. □

Proposition 3.11. For all $c \in \mathbb{C}$ there exists a $\tau \in \mathbb{H}$ with $j(\tau) = c$.

Proof. Assume for the sake of a contradiction that $j(\tau) \neq c$ for all $\tau \in \mathbb{H}$. Then $F(\tau) := \frac{j'(r)}{j(r)-c}$ is holomorph on $\mathbb{C}$. Using a clever path integral we conclude that the first term of the Fourier Series of F is $-2\pi i$ which yields a contradiction. □

Corollary 3.12. For c_2 and c_3 with $c_2^3 - 27c_3^2 \neq 0$ there is exactly one lattice Ω with $c_2 = g_2(\Omega)$ and $c_3 = g_3(\Omega)$.

Proof. Using the first part of the remark we have a lattice Ω with $j(\Omega) = \frac{(12c_2)^3}{c_2^3-27c_3^2}$.

- In the case that $c_2 = 0$ we have $g_2(\Omega) = 0$ and $g_3(\Omega) \neq 0$. Pick a $\lambda \in \mathbb{C}$ with $g_3(\Omega) = \lambda^6 c_3$. Using Remark 3.1 we have $g_3(\lambda\Omega) = \lambda^{-6} g_3(\Omega) = c_3$. Finally $g_2(\lambda\Omega) = 0 = c_2$.
- In the case that $c_2 \neq 0$,we have $j(\Omega) \neq 0$ and thus $g_2(\Omega) \neq 0$. Pick a $\lambda \in \mathbb{C} \setminus 0$ satisfying $g_2(\Omega) = \lambda^4 c_2$. Then $g_2(\lambda\Omega) = c_2$ and due to the in variance of the j-invariant we have $c_3^2 = g_3^2(\lambda\Omega)$.

Uniqueness is then a consequence of the fact that the $\wp$ is the unique solution of the elliptical differential equation, see the talk of last week.

□

4 Complex Elliptic curves

4.1 The Addition Law

Recall the Definition of the $\wp$-function as stated in Chapter (2.2): For a lattice Ω defined as $\Omega := (\omega_1\mathbb{Z} + \omega_1\mathbb{Z}) \in \mathbb{C}$ we defined the $\wp$ function as

$$\wp(z) \equiv \wp(z, \omega_1, \omega_2) := z^{-2} + \sum_{0 \neq \omega \in \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2} \big((z-\omega)^{-2} - \omega^{-2}\big).$$

In this chapter we will fix the lattice Ω and thus allow ourselves to write simply $\wp(z)$.

Theorem 4.1. Let $z, w \in \mathbb{C}$ (this is a small "W" and not a small "Ω") satisfying $z, w, z \pm w \notin \Omega$. Then we have the following additive identity:

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

4.2 The elliptic curves of lattices

Definition 4.2. Recall the factor group $\mathbb{C}/\Omega = \{z + \Omega \text{ with } z \in \mathbb{C}\}$. We call the set

$$\mathbb{E} \equiv \mathbb{E}(\Omega) := \{(x, y) \in \mathbb{C}^2 : y^2 = 4x^3 - g_2 x - g_3\}$$

the **elliptic curve of Ω**.

The $\wp$ function allows for a nice parametritzation of $\mathbb{E}$:

Lemma 4.3. The map Φ is a bijection.

$$\begin{aligned} \Phi : (\mathbb{C}/\Omega) \setminus \Omega \to & \qquad \mathbb{E}(\Omega) \\ z + \Omega \longmapsto & \qquad \Phi(z+\Omega) := (\wp(z), \wp'(z)) \end{aligned}$$

Proof. From the first important differential equation in the talk of last week ($\wp'^2 = 4\wp^3 - g_2\wp - g_3$) we can follow that the image of Φ is contained in $\mathbb{E}$. For a $(x, y) \in \mathbb{E}$ we pick a z in $\mathbb{C}$ with $\wp(z) = x$.

We might have also seen in the last talk that for a $z \in \mathbb{C}$ satisfying $z \neq \wp(\omega/2)$ for $\omega \in \Omega$ and $\omega/2 \notin \Omega$ there are exactly two different numbers u, v in any tile of Ω that satisfy $u + v \in \Omega$.

Then we have $y^2 = 4x^3 - g_2 x - g_3 = \wp'(z)^2$ again due to the differential equation. After taking the square root, up to signs we have $\wp(z) = y$ meaning that (x, y) lies in the image of Φ. Therefore Φ is surjective.

Let $z_1, z_2 \in \mathbb{C}$ satisfy $\Phi(z_1) = \Phi(z_2)$. In the case that $\wp'(z_1) \neq 0$ we have $z_1 \equiv z_2 \bmod \Omega$ as $\wp(z) - \omega$ has two simple roots in a tile given that $w \neq e_1, e_2, e_2$.

In the case that $\wp'(z) = 0$ we have $z_1, z_2 \equiv \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_3}{2} \bmod \Omega$. This is due to the fact that $\wp(z) - e_k$ has a double root in a tile.

We see that $\wp(\omega_k/2)$ are all different numbers for $k = 1, 2, 3$ so we also have $z_1, z_2 \equiv \frac{\omega_1}{2}$. Therefore Φ is also injective. $\square$

Definition 4.4. The one point compactification of $\mathbb{E}$ is denoted $\bar{\mathbb{E}}$ and allows us to extend the map Φ to Ω by defining $\Phi(\Omega) := \{\infty, \infty\} \equiv \infty$.

This expansion will allow us to push forward the group structure of $\mathbb{C}/\Omega$ to $\bar{\mathbb{E}}$ in a natural way:

Definition 4.5. Taking into account the usual addition on $\mathbb{C}/\Omega$, we have for $P, Q \in \bar{\mathbb{E}}$ satisfying $P \neq Q$ the following **addition formula**.

$$P + Q := \Phi(\Phi^{-1}(P) + \Phi^{-1}(Q))$$

In case of this diagram we can think of the addition of going up, then to the right and then down again.

$$\begin{array}{ccc} \mathbb{C}/\Omega \times \mathbb{C}/\Omega & \xrightarrow{\text{usual + in } \mathbb{C}} & \mathbb{C}/\Omega \\ {\scriptstyle \Phi^{-1}\times\Phi^{-1}}\uparrow & & \downarrow{\scriptstyle \Phi} \\ \mathbb{E} \times \mathbb{E} & \xrightarrow{\text{new +}} & \mathbb{E} \end{array}$$

Theorem 4.6. Together with the addition we just defined in Definition (4.5), the set $\bar{\mathbb{E}}$ becomes an abelian group with neutral element ∞.

Proof. We check that $P + \infty = P$:

$$\begin{aligned} P + \infty &= \Phi(\Phi^{-1}(P) + \Phi^{-1}(\infty)) \\ &= \Phi(\Phi^{-1}(P) + \Omega) \\ &= \Phi(\Phi^{-1}(P)) \\ &= P \end{aligned}$$

We have $\Phi(z + \Omega) = \Phi(z)$. The other group axioms work equivalently □

Remark 4.7. The addition of the ∞-point can be circumnavigated by considering projective elliptic curves.

Definition 4.8. Let P and Q be any two points in $\mathbb{C}^2$ with $X_P \neq Y_P$. **The complex line** through P and Q is denoted Γ_{PQ} and after defining

$$a_{PQ} := \frac{Y_P - Y_Q}{X_p - X_Q} \tag{4.1}$$

and

$$b_{PQ} = \frac{X_P Y_Q - X_Q Y_P}{X_P - X_Q} \tag{4.2}$$

we see that

$$\Gamma_{PQ} = \{Y = a_{PQ}X + b_{PQ}\} \subset \mathbb{C}^2.$$

If now P and Q lie on $\mathbb{E}$ then the line Γ_{PQ} will intersect $\mathbb{E}$ again at a third point. (As algebraic geometry students will *of course* know that a line intersects a cubic curve in $\mathbb{P}^2$ exactly twice. This then boils down to our case.) We call that point $P \cdot Q$.

More precisely we have:

$$X_{P\cdot Q} = \frac{1}{4}a_{P,Q}^2 - X_p - X_q \tag{4.3}$$

$$Y_{P\cdot Q} = a_{P,Q}X_{P\cdot Q} + b_{P,Q}. \tag{4.4}$$

Lemma 4.9. For all $X \in \mathbb{C}$ we have:

$$4X^3 - g_2X - g_3 = 4(X - X_P)(X - X_Q)(X - X_{P\cdot Q}) + (a_{P,Q}X + b_{P,Q})^2$$

Proof. The coefficients of the X^3 entry agree obviously. Computation using ((4.3)) and ((4.4)) yields the same coefficients (zero) for the X^2 entry. Finally we have $g_2X + g_3 = mX + c$. As the equation holds if we set $X = X_P$ and $X = X_Q$ we are done. □

This result gives us:

Corollary 4.10. If $P, Q \in \mathbb{E}$ with $X_P \neq Y_Q$ then $P \cdot Q \in \mathbb{E}$.

In the case that $P = Q$ we work analogously. We take the tangent through a point $P \in \mathbb{E}$ assuming $Y_P \neq 0$. Set $a_P := \frac{X_P^2 - g_2}{2Y_P}$ and $b_P = Y_P - a_PX_P$. The tangent is then given by $\{Y = a_PX + b_P\}$. The point $P \cdot P$ can then be written as

$$X_{P\cdot P} = \frac{1}{4}a_P^2 - 2X_P$$
$$Y_{P\cdot P} = a_pX_{P\cdot P} + b_P.$$

We have similar statements as before.

Lemma 4.11. For all $X \in \mathbb{C}$ we have

$$4X^3 - g_2X - g_3 = 4(X - X_P)^2(X - X_{P\cdot P}) + (a_PX + b_P)^2$$

Corollary 4.12. For $P \in \mathbb{E}$ satisfying $Y_p \neq 0$ we have $P \cdot P \in \mathbb{E}$.

The question now arises how this "$\cdot$" links to the rest of the content we presented.

Lemma 4.13. Let $u, v, w \in \mathbb{C} \setminus \Omega$ with $u + v + w \in \Omega$ and $u + \Omega$, $v + \Omega$, $w + \Omega$ distinct. Define $\bar{\mathbb{E}} \ni P := \Phi(u + \Omega)$ and $\bar{\mathbb{E}} \ni Q := \Phi(v + \Omega)$. Then we have

$$P \cdot Q = \Phi(w + \Omega).$$

Proof. The elliptic function $f(z) := \wp'(z) - a_{P,Q}\wp(z) + b_{P,Q}$ has a pole of third degree in zero. Therefore it also has three roots in $\mathbb{C}/\Omega$. By construction we have $f(u) = 0 = f(v)$ and due to some function theory magic we know that $f(w) = 0$.

Therefore P, Q and $R := \Phi(w + \Omega)$ form the intersection of the line spanned by P and Q with $\mathbb{E}$. We now want to show that $P \cdot Q = R$. If $P \cdot Q = P$ then we would obtain $a_{P,Q} = a_P$ and $b_{P,Q} = b_P$ by using the formulas computed in ((4.1)) and ((4.2)). This would mean that the line is a tangent to the curve $\mathbb{E}$. As P, Q, R are distinct, this is impossible. So $P \cdot Q = R$. □

Proof. Of the Addition Law. From the Lemma above and the equations describing $P \cdot Q$ we have for $u, v, w \in C/\Omega$ satisfying $u + v + w = 0$ and $u + \Omega$, $v + \Omega$, $w + \Omega$ pairwise distinct:

$$\begin{aligned}\wp(u+v) = \wp(w) = -\wp(w) &= \frac{1}{4}a_{P,Q}^2 - X_P - Y_Q \\ &= \frac{1}{4}\left(\frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)}\right)^2 - \wp(u) - \wp(v)\end{aligned}$$

Therefore we have

$$\wp(u+v) + \wp(u) + \wp(v) = \frac{1}{4}\left(\frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)}\right)^2$$

Which was the statement we desired to prove. □

For $P \in \mathbb{C}^2$ we define a sort of conjugation as follows:

$$P^* := (X_P, -Y_P)$$

The final result then is:

Theorem 4.14. The addition $P + Q$ on $\mathbb{E}$ is defined by

$$P + Q = (P \cdot Q)^*$$

for $X_P \neq X_Q$ and for $Y_p \neq 0$

$$2P = (P \cdot P)^*$$

In particular we have $-P = P^*$

Proof. For $\wp(u) \neq \wp(v)$ we have

$$\begin{aligned}P + Q &= \Phi(\Phi^{-1}(P) + \Phi^{-1}(Q)) \\ &= \Phi(u + v + \Omega) \\ &= \Phi(-w + \Omega) \\ &= (\wp(w), -\wp'(w)) \\ &= (\Phi(w + \Omega))^* \\ &= (P \cdot Q)^*\end{aligned}$$

□

Remark 4.15. There is a less geometric proof of the addition law involving the differential equations from last talk, however this proof gives a nicer picture and makes thus —in my eyes— more sense to present.

4.3 Classifying Complex Elliptic Curves

The Basis Lemma 1.8 showed us that two lattices agree if and only if the basis can be transformed to each other through an element in $SL(2,\mathbb{Z})$. Additionally, we showed that any lattice can be described by a lattice of the form $\tau\mathbb{Z}+\mathbb{Z}$. Lastly the last section showed that there is a bijection between any given lattice and its Elliptic curve which we denoted Φ. Now the question arises if there is a way to push this Φ forward in order to get some sort of relation between complex elliptic curves and $SL(2,\mathbb{Z})$-distinguished lattices.

$$\begin{array}{ccc} \mathbb{H}/SL(2,\mathbb{Z}) & \longrightarrow^{\Theta} & K(\Omega) \\ \text{"}\cup\text{"} & & \cup \\ \mathbb{C}/\Omega & \longrightarrow^{\Phi} & \bar{\mathbb{E}}(\Omega) \\ \cup & & \cup \\ z+\Omega & \longmapsto^{\Phi} & \big(\wp(z),\wp'(z)\big) \end{array}$$

The steps we applied to Ω in Definition 4.2 that ended up giving us $\bar{\mathbb{E}}$ can be made into a map Θ which assign to every lattice Ω an Elliptic curve. Using Proposition 3.11 we can follow that there is indeed a unique lattice for every elliptic curve and vice versa.

Definition 4.16. The map $\Theta : \mathbb{H}/SL(2,\mathbb{Z}) \to K(\Omega)$ assigns to every $SL(2,\mathbb{Z})$-unique lattice Ω an Elliptic curve Θ_Ω.

$$\Theta_\Omega := \{(x,y) \in \mathbb{C}\times\mathbb{C}; y^2 = 4x^3 - g_2x - g_3\}$$

We have seen that both g_2 and g_3 will change as soon as the underlying lattice changes. This is die to the Eisenstein Series which G_k define modular forms and g_2 and g_3 being multiples of G_4 and G_6.

Every elliptic curve is a Riemann surface, a one dimensional complex manifold. Additionally the map we just shined light on showed us that the set of all Elliptic curves is itself also a Riemann surface.

References

[1] M. Koecher and A. Krieg, *Elliptische Funktionen und Modulformen*, Springer-Verlag, Berlin, revised ed., 2007.

[2] R. Remmert, *Funktionentheorie 1*, Springer-Verlag, Berlin, 4 ed., 1995.