Elliptic Curves

Dr. Joerg Zintl

University of Kaiserslautern, Germany

Review Course given at AIMS, South Africa

May 2017

PART I: Plane Cubic Curves

PART II: Elliptic Curves in Cryptography

PART III: Elliptic Functions

8. Basics on holomorphic functions

Definition 8.1. *Let $U \subseteq \mathbb{C}$ be an open subset. A function $f : U \to \mathbb{C}$ is called* holomorphic, *if the* complex derivative

$$\frac{df}{dz}(z_0) = \lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0}$$

exists for any $z_0 \in U$.

There are many equivalent characterizations of holomorphic functions, like for example as solutions of the Cauchy-Riemann differential equations. For us, the following is the most important:

Proposition 8.2. *Let $U \subseteq \mathbb{C}$ be an open subset. A function $f : U \to \mathbb{C}$ is holomorphic, if and only if for any $z_0 \in U$ there exists an $r > 0$ with*

$$U_r(z_0) := \{z \in \mathbb{C} : |z - z_0| < r\} \subseteq U$$

together with complex numbers $a_0, a_1, a_2, \ldots \in \mathbb{C}$ such that

$$f(z) = \sum_{n=0}^{\infty} a_n (z - z_0)^n$$

holds for all $z \in U_r(z_0)$.

A function which can be written everywhere locally as a converging power series is called *complex analytic*. In fact, the power series is obtained as the *Taylor expansion* by iterated computing of complex derivatives.

One example is the complex *exponential function*

$$\exp(z) := \sum_{n=0}^{\infty} \frac{1}{n!} z^n.$$

Remark 8.3. Properties of a holomorphic function $f : U \to \mathbb{C}$

- f is a continuous map
- if f is non-constant, then f is an open map (i.e. f maps open sets to open sets)
- $f' := \frac{df}{dz}$ is holomorphic
- **Identity theorem:**

  If $g : U \to \mathbb{C}$ is holomorphic, and $W \subseteq U$ a non-discrete subset such that $f|W = g|W$, then $f = g$.

This few basic properties have very important consequences for holomorphic functions. Here are a few examples.

Lemma 8.4. *Let $f : U \to \mathbb{C}$ be a holomorphic function, which is not constantly* 0*. Then the* vanishing locus

$$V(f) := \{z \in U : f(z) = 0\}$$

is a discrete subset.

Proof. Assume that the vanishing locus is not discrete. Put

$$W := V(f) \text{ and } g \equiv 0.$$

Now apply the identity theorem to

$$f|W \;=\; 0|W$$

and obtain a contradiction.

Theorem 8.5. (Liouville) *Let $f : \mathbb{C} \to \mathbb{C}$ be holomorphic. If there exists an upper bound $R > 0$ such that $|f(z)| < R$ for all $z \in \mathbb{C}$, then f is constant.*

The main object of complex analysis is the following generalization of holomorphic functions.

Definition 8.6. *Let $U \subseteq \mathbb{C}$ be an open subset, and let $\Delta \subset U$ be a discrete subset. A function $f : U \smallsetminus \Delta \to \mathbb{C}$ is called a* meromorphic function on U *if for any $z_0 \in U$, there exists an $r > 0$ with*

$$U_r(z_0) := \{z \in \mathbb{C} : |z - z_0| < r\} \;\subseteq\; U$$

together with some $k \in \mathbb{Z}$ and complex numbers $a_k, a_{k+1}, a_{k+2}, \ldots \in \mathbb{C}$ such that

$$f(z) = \sum_{n=k}^{\infty} a_n (z - z_0)^n$$

holds for all $z \in U_r(z_0) \setminus \Delta$.

Example 8.7. Consider the function

$$f(z) := \frac{\exp(z)}{z} = \sum_{n=0}^{\infty} \frac{1}{n!} \frac{z^n}{z} = \sum_{n=-1}^{\infty} \frac{1}{(n+1)!} z^n$$

as a meromorphic function on $\mathbb{C}$, with $\Delta = \{0\}$.

Example 8.8. Consider the rational function on $\mathbb{C}$

$$f(z) := \frac{z-1}{z^3 - z^2}$$

By factorization of the denominator

$$z^3 - z^2 = z(z+1)(z-1)$$

we find for the exceptional set $\Delta = \{-1, 0, 1\}$.

Note that f is complex differentiable at $z_0 = 1$, since by cancellation

$$f(z) = \frac{1}{z(z+1)}.$$

One says that $f : \mathbb{C} \setminus \Delta \to \mathbb{C}$ *extends holomorpically over* $z_0 = 1$.

Recall the formula

$$\frac{1}{z+1} = \sum_{n=0}^{\infty} (-z)^n,$$

which is valid as long as $|z| < 1$, i.e. for $z \in U_1(z_0)$.

Using this, we obtain for the case $z_0 = 0$:

$$\begin{aligned} f(z) &= \tfrac{1}{z(z+1)} \\ &= \tfrac{1}{z} \sum_{n=0}^{\infty} (-1)^n z^n \\ &= \sum_{n=-1}^{\infty} (-1)^{n+1} z^n \end{aligned}$$

This formula holds for $z \in U_1(0) \setminus \{0\}$.
Similarly, we compute for $z_0 = -1$:

$$\begin{aligned} f(z) &= \tfrac{1}{z(z+1)} \\ &= \tfrac{1}{z+1} \, \tfrac{-1}{1-(z+1)} \\ &= \tfrac{1}{z+1} \, (-1) \sum_{n=0}^{\infty} (z+1)^n \\ &= \sum_{n=-1}^{\infty} (-1)(z+1)^n \end{aligned}$$

Here we need the condition $z \neq -1$ and $|z+1| < 1$, which is equivalent to $z \in U_1(-1) \setminus \{-1\}$.

Remark 8.9. Is has become an accepted habit to write for a meromorphic function

$$f : U \to \mathbb{C}$$

even though strictly speaking there may be some points in U (contained in Δ), where the map f is not defined.

Definition 8.10. Let $f : U \to \mathbb{C}$ be a meromorphic function. Let $z_0 \in U$, and let

$$f(z) = \sum_{n=k}^{\infty} a_n (z - z_0)^n$$

for all $z \in U_r(z_0)$ for a suitable $r > 0$. Let $a_k \neq 0$.
We call

$$\mathrm{ord}_{z_0}(f) := k$$

the *order of f at z_0*.
We say that

f has a *pole of order k* at z_0, if $k < 0$

and

f has a *zero of order k* at z_0, if $k > 0$

Note: $\mathrm{ord}_{z_0}(f) = 0 \quad \Leftrightarrow \quad f(z_0) \in \mathbb{C} \setminus \{0\}$.
More generally, for a complex number $v \in \mathbb{C}$, we say that f *assumes the value v to the order k at z_0*, if the meromorphic function

$$f_v(z) := f(z) - v$$

has a zero of order k at z_0.

Exercise 8.11. Show that for a meromorphic function f holds

$$\mathrm{ord}_{z_0}(f) = k$$

if and only if

$$g(z) := \frac{f(z)}{z^k}$$

extends holomorphically over z_0, with $g(z_0) \neq 0$.

Remark 8.12. Meromorphic functions on U are such holomorphic functions f on U minus some discrete subset Δ_f, where for any $z_0 \in \Delta_f$ the limit

$$\lim_{z \to z_0} f(z)$$

has a "controlled behavior": either the limit exists in $\mathbb{C}$, in which case f extends holomorphically over z_0 ($\Leftrightarrow$ $\mathrm{ord}_{z_0} \geq 0$), or the limit is ∞ ($\Leftrightarrow$ $\mathrm{ord}_{z_0} < 0$).

There are examples of holomorphic functions $f : U \setminus \{z_0\} \to \mathbb{C}$, where no well-defined limit exists. Such a function is not meromorphic.

Notation 8.13. Let $U \subseteq \mathbb{C}$ be open. We write

$$\mathcal{O}(U) := \{f : U \to \mathbb{C} \text{ such that } f \text{ is holomorphic on } U\}$$

and

$$\mathcal{M}(U) := \{f : U \to \mathbb{C} \text{ such that } f \text{ is meromorphic on } U\}$$

Remark 8.14. For the algebraically interested:

Let $f, g \in \mathcal{O}(U)$. By defining $f + g$ and $f \cdot g$ pointwise, we see that $\mathcal{O}(U)$ has the structure of a *commutative ring*.

Let $f, g \in \mathcal{M}(U)$. Let Δ_f and Δ_g be their exceptional sets, and let V_g be the set of points, where g vanishes. By 8.4, the set V_g is discrete. Therefore

$$\frac{f}{g}$$

is meromorphic over U, with exceptional set contained in $\Delta_f \cup V_g$. (In fact, $\frac{1}{g}$ extends holomorphically over all points of Δ_g.)

In particular, for the quotient holds $\frac{f}{g} \in \mathcal{M}(U)$.

This makes $\mathcal{M}(U)$ into a field!

Definition 8.15. The *Riemann sphere* is the set $\hat{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$, together with the following topological structure:

For any point $p \in \hat{\mathbb{C}}$, and any $r > 0$, we define circular neighbourhoods

$$U_r(p) := \begin{cases} \{z \in \mathbb{C} : |z - p| < r\} & \text{if } p \in \mathbb{C} \\ \{z \in \mathbb{C} : |z| > \frac{1}{r}\} \cup \infty & \text{if } p = \infty \end{cases}$$

A subset $V \subseteq \hat{\mathbb{C}}$ is called *open*, if for any point $p \in V$ there exists a circular neighbourhood contained in V.

Exercise: $\hat{\mathbb{C}}$ is compact.

Remark 8.16. Let $f \in \mathcal{M}(U)$ be a meromorphic function on an open subset $U \subseteq \mathbb{C}$. By defining $f(z) := \infty$, if z is a pole of f, we can view f as a map

$$f : U \to \hat{\mathbb{C}}$$

By remark 8.12, we make an identification

$$\mathcal{M}(U) = \left\{ \begin{array}{c} f : U \to \hat{\mathbb{C}} \text{ such that} \\ f \text{ is continuous and} \\ f \text{ is holomorphic on } f^{-1}(\hat{\mathbb{C}} \setminus \{\infty\}) \end{array} \right\}$$

9. Elliptic functions

Definition 9.1. Let $f \in \mathcal{M}(\mathbb{C})$. A complex number $w \in \mathbb{C}$ is called a *period* on f, if for all $z \in \mathbb{C}$ holds

$$f(z + w) = f(z).$$

The set of all periods of f is denoted by

$$\mathrm{Per}(f) := \{w \in \mathbb{C} : \ w \text{ is a period of } f\}.$$

Example 9.2. Consider the exponential function $f(z) = \exp(z)$. We find

$$\mathrm{Per}(\exp) = \{2\pi i m : \ m \in \mathbb{Z}\} = 2\pi i \, \mathbb{Z}.$$

Proposition 9.3. *Let $f \in \mathcal{M}(\mathbb{C})$ be a non-constant meromorphic function. Then $(Per(f), +)$ is a discrete subgroup of $(\mathbb{C}, +)$.*

Proof. (i) It is easy to see that $\mathrm{Per}(f)$ is an Abelian group with respect to "+".

Clearly, $0 \in \mathrm{Per}(f)$.

For $w_1, w_2 \in \mathrm{Per}(f)$, we find

$$f(z + w_1 + w_2) = f(z + w_1) = f(z)$$

for all $z \in \mathbb{C}$, and thus $w_1 + w_2 \in \mathrm{Per}(f)$.

For the inverse of a period $w \in \mathrm{Per}(f)$, consider

$$f(z) = f(z - w + w) = f(z - w)$$

and thus $-w \in \mathrm{Per}(f)$, too.
(ii) By definition,

$$f(w) = f(0)$$

for all $w \in \mathrm{Per}(f)$. If we write $c := f(0)$, then

$$f|\mathrm{Per}(f) \equiv c$$

is constant. If $\mathrm{Per}(f)$ is not a discrete subset, then the identity theorem 8.3 implies that f is constant, a contradiction. $\square$

Proposition 9.4. *Let $(\Omega, +)$ be a discrete subgroup of $(\mathbb{C}, +)$. Then Ω is exactly one of the following:*

- $\Omega = \{0\}$
- $\Omega = \omega\,\mathbb{Z} = \{\omega m : \ m \in \mathbb{Z}\}$, *where* $0 \neq \omega \in \mathbb{C}$
- $\Omega = \omega_1\,\mathbb{Z} + \omega_2\,\mathbb{Z} = \{\omega_1 m_1 + \omega_2 m_2 : \ m_1, m_2 \in \mathbb{Z}\}$, *where ω_1 and ω_2 are linearly independent over $\mathbb{R}$.*

Remark 9.5. We say that the discrete subgroup Ω is of *rank* 0, 1 or 2, respectively.

A discrete subgroup of rank 2 in $\mathbb{C}$ is called a *lattice*.

Proof. of proposition 9.4

Note that by assumption, Ω is discrete. So $\mathbb{C} \setminus \Omega$ is open, and hence Ω is closed.

We may assume $\Omega \neq \{0\}$. For the proof we view $\mathbb{C}$ as a 2-dimensional vector space over $\mathbb{R}$.

Case 1. Suppose that Ω is contained in a line. This is equivalent to saying that any 2 elements of Ω are linearly equivalent over $\mathbb{R}$.

Note that the line must necessarily contain the origin 0.

Since Ω is discrete, we can find a period $0 \neq \omega_0 \in \Omega$, for which $|\omega_0|$ is minimal.

For any other $0 \neq \omega \in \Omega$, there exists a scalar $\lambda \in \mathbb{R}$, such that $\omega = \lambda\omega_0$.

Claim: $\lambda \in \mathbb{Q}$.

Otherwise, there exists sequences of integers $(p_n)_{n\in\mathbb{N}}$ and $(q_n)_{n\in\mathbb{N}}$ in $\mathbb{Z}$, such that

$$\lim_{n\to\infty} \frac{p_n}{q_n} = \lambda$$

such that $\frac{p_n}{q_n} \neq \lambda$ for all $n \in \mathbb{N}$.

Since Ω is an Abelian group, we have

$$p_n\omega_0 - q_n\omega \in \Omega$$

for all $n \in \mathbb{N}$. In particular,

$$(p_n\omega_0 - q_n\omega)_{n\in\mathbb{N}}$$

is a sequence of points in $\mathrm{Per}(f) \setminus \{0\}$, which converges to the point $0 \in \mathrm{Per}(f)$. But this contradicts the discreteness of $\mathrm{Per}(f)$.

Claim: $\lambda \in \mathbb{Z}$.

Otherwise, we can write λ as a fraction $\lambda = \frac{p}{q}$ with $\gcd(p, q) = 1$ and $q \notin \{-1, 1\}$. We can to thus find $a, b \in \mathbb{Z}$ such that

$$aq + bp = 1.$$

We compute

$$\omega = (ap + bq)\omega = ap\omega_0 + bp\omega.$$

Since by definition $\omega = \frac{p}{q}\omega_0$, this implies

$$\frac{1}{q}\omega_0 = \frac{1}{p}\omega = a\omega_0 + b\omega \in \Omega.$$

This, however, contradicts the minimality of ω_0.

Case 2. Suppose that Ω contains two elements ω_1 and ω_2, which are linearly independent over $\mathbb{R}$. We may assume that $|\omega_1|$ in minimal among the elements $\Omega \setminus \{0\}$ and $|\omega_2|$ is minimal among the elements not linearly equivalent to ω_1.

For any $0 \neq \omega \in \Omega$, there exist unique $\lambda_1, \lambda_2 \in \mathbb{R}$, such that

$$\omega = \lambda_1\omega_1 + \lambda_2\omega_2$$

We find

$$w - \lambda_2\omega_2 = \lambda_1\omega_1 \in \Omega'$$

where

$$\Omega' := \Omega \cap L \text{ for the line } L := \omega_1\mathbb{R}$$

Note that Ω' is a discrete subgroup of $\mathbb{C}$. By case 1, we must have $\lambda_1 \in \mathbb{Z}$.

Analogously, we conclude $\lambda_2 \in \mathbb{Z}$.

Definition 9.6. *Let $\Omega \subset \mathbb{C}$ be a lattice. An* elliptic function with respect to Ω *is a meromorphic function $f \in \mathcal{M}(\mathbb{C})$ such that*

$$\Omega \subseteq Per(f).$$

The set

$$\mathcal{K}(\Omega) := \{f \in \mathcal{M}(\mathbb{C}) \text{ such that } f \text{ is elliptic w.r.t. } \Omega\}$$

is called the field of elliptic functions with respect to Ω.

Note. It is not hard to verify the field axioms for $\mathcal{K}(\Omega)$.

Remark 9.7. For a constant function f clearly holds $\mathrm{Per}(f) = \mathbb{C}$. Therefore, a constant function f is elliptic with respect to any lattice Ω.

Proposition 9.8. *Let $\Omega \subset \mathbb{C}$ be a lattice, and let f be holomorphic on $\mathbb{C}$ and elliptic with respect to Ω.*

Then f is constant.

Before we prove this proposition, let us introduce some notation.

Notation 9.9. Let $\Omega \subset \mathbb{C}$ be a lattice.

A *semi-open parallelogram of periods of* Ω is a set

$$P_{\omega_1,\omega_2} := \{t_1\omega_1 + t_2\omega_2 \in \mathbb{C} \text{ for } 0 \leq t_1, t_2 < 1\}$$

where $\omega_1, \omega_2 \in \mathbb{C}$ are $\mathbb{R}$-linearly independent generators of the lattice $\Omega = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$.

The set

$$\overline{P}_{\omega_1,\omega_2} := \{t_1\omega_1 + t_2\omega_2 \in \mathbb{C} \text{ for } 0 \leq t_1, t_2 \leq 1\}.$$

is called a *closed parallelogram of periods of* Ω.

Proof. of proposition 9.8.

Let $\Omega = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ and $f \in \mathcal{O}(\mathbb{C}) \cap \mathcal{K}(\Omega)$.

The function f being elliptic means that f is *periodic* with respect to Ω.

Therefore we have

$$f(\mathbb{C}) = f(P_{\omega_1,\omega_2}) = f(\overline{P}_{\omega_1,\omega_2}).$$

As a holomorphic function is in particular a continuous function.

Hence it maps compact subsets of $\mathbb{C}$ to compact subsets.

Since $\overline{P}_{\omega_1,\omega_2}$ is compact, so is $f(\overline{P}_{\omega_1,\omega_2})$. Therefore, by the above identity, $f(\mathbb{C})$ is compact.

In particular, the values of f are bounded.

Now the theorem of Liouville implies that f must be constant. $\square$

Theorem 9.10. *Let $f \in \mathcal{K}(\Omega)$ be a meromorphic function, which is not constantly zero, and elliptic with respect to a lattice Ω.*

Let $P = P_{\omega_1,\omega_2}$ be a semi-open parallelogram of periods of Ω.

For a point $z \in P$ let $\mathrm{ord}_z(f)$ denote the order of f at z.

Then there are at most finitely many points $z \in P$, such that $\mathrm{ord}_z(f) \neq 0$, and

$$\sum_{z \in P} \mathrm{ord}_z(f) = 0.$$

The proof of this statement is a consequence of the very strong *Residue Theorem* on meromorphic functions.

Remark 9.11. Note that $\mathrm{ord}_z(f) \neq 0$ if and only if z is either a pole or a zero of f.

If $f(z) = 0$, for some $z \in P$, then $\mathrm{ord}_z(f) > 0$. Thus the sum

$$n(f) := \sum_{z \in P \text{ such that } f(z)=0} \mathrm{ord}_z(f) \ \geq 0$$

counts the number of zeroes of f inside P with *multiplicities* given by the order of f at the respective points.

Conversely, if z is a pole of f, then $\mathrm{ord}_z(f) < 0$. By definition, the order of the pole is given by $-\mathrm{ord}_z(f)$, and therefore the sum

$$p(f) := \sum_{z \in P \text{ such that } z \text{ is a pole}} (-\mathrm{ord}_z(f)) \ \geq 0$$

is counting poles in P with multiplicities.

The essence of the above theorem is the important fact, that these two sums

$$n(f) = p(f)$$

are in fact the same!

Definition 9.12. *Let $f \in \mathcal{K}(\Omega) \setminus \{0\}$ for some lattice Ω. The* order of f *is defined by*

$$\operatorname{ord}(f) := n(f).$$

Remark 9.13. (i) Note that $n(f) = 0$ is equivalent to $p(f) = 0$. Hence $\operatorname{ord}(f) = 0$ is equivalent to f being holomorphic on P_{ω_1,ω_2}, and therefore, by periodicity, on all of $\mathbb{C}$.
From proposition 9.8 it follows that this is the case if and only if f is constant.

(ii) One can show that there exists no elliptic function of order 1.

10. The Weierstrass function

Throughout this section let $\Omega = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ be a lattice, with $\omega_1, \omega_2 \in \mathbb{C}$ linearly independent over $\mathbb{R}$.

Definition 10.1. *Let $k \in \mathbb{N}$. The* Eisenstein series of weight k *with respect to Ω is*

$$G_k(\Omega) := \sum_{\omega \in \Omega \setminus \{0\}} \frac{1}{\omega^k}.$$

Proposition 10.2. *The Eisenstein series $G_k(\Omega)$ converges absolutely for all $k \geq 3$.*

Proof. For $m \in N$, consider the two finite sums

$$S_m := \sum_{\substack{\omega = m_1\omega_1 + m_2\omega_2 \\ -m \le m_1, m_2 \le m}} \frac{1}{|\omega|^k}$$

and

$$T_{m=1} := S_{m+1} - S_m.$$

Note that S_m consists of $(2m+1)^2$ summands, and T_m of $8m$ summands.

As formal sums,

$$\sum_{\omega \in \Omega \setminus \{0\}} \frac{1}{|\omega|^k} = \sum_{m+1}^{\infty} T_m$$

Therefore to show the absolute convergence of $G_k(\Omega)$, it suffices to show the (absolute) convergence of the sum on the right hand side.

Define

$$a := \min\{|\omega_1|, |\omega_2|, |\omega_1 + \omega_2|, |\omega_1 - \omega_2|\}$$

and

$$b := \max\{|\omega_1|, |\omega_2|, |\omega_1 + \omega_2|, |\omega_1 - \omega_2|\}.$$

For an element $\omega = m_1\omega_1 + m_2\omega_2$ with $-m \le m_1, m_2 \le m$ we obtain the estimates

$$ma \le |\omega| \le mb$$

and therefore

$$\frac{1}{(ma)^k} \ge \frac{1}{|\omega|^k} \ge \frac{1}{(bm)^k}.$$

From this we conclude

$$\frac{8m}{(ma)^k} \geq T_m \geq \frac{8m}{(bm)^k}.$$

Now the series we are interested in is bounded by two series, which converge for $k \geq 3$:

$$\frac{8}{(a)^k} \sum_{m=1}^{\infty} \frac{1}{m^{k-1}} \geq \sum_{m=1}^{\infty} T_m \geq \frac{8}{(b)^k} \sum_{m=1}^{\infty} \frac{1}{m^{k-1}}.$$

Hence it must be converging, too. □

Remark 10.3. For any odd number $k \in N$ holds $G_k(\Omega) = 0$.

Indeed, by the absolute convergence of the series, we may group the summands into pairs

$$\frac{1}{\omega^k} + \frac{1}{(-\omega)^k} = 0$$

Proposition 10.4. *The series*

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

defines an elliptic function with respect to Ω.

Definition 10.5. $\wp$ *is called the* Weierstraß $\wp$-function.

Remark 10.6. Note that $\wp$ is a symmetric function.

Indeed, for all $z \in \mathbb{C}$ and all $\omega \in \Omega$ we have

$$\frac{1}{(z-\omega)^2} = \frac{1}{(-z+\omega)^2}.$$

Once we have established that $\wp$ is a meromorphic function, we may reorder the series by interchanging ω with $-\omega$, and thus obtain $\wp(-z) = \wp(z)$ for all $z \in \mathbb{C}$.

Proof. of proposition 10.4

(i) Let $R > 0$. We can split the above series as

$$\wp(z) = g(z) + f(z),$$

where

$$g(z) := \frac{1}{z^2} + \sum_{\substack{\omega \in \Omega \setminus \{0\} \\ |\omega| \leq 2R}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

and

$$f(z) := \sum_{\substack{\omega \in \Omega \setminus \{0\} \\ |\omega| > 2R}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Note that g is just a finite sum, so it is clearly a meromorphic function on the open disc $U_R(0)$.

We claim that f is holomorphic on $U_R(0)$.

From this it then follows that $\wp$ is meromorphic on $U_R(0)$, and since this holds true for any $R > 0$, the function $\wp$ is meromorphic on all of $\mathbb{C}$.

To prove the claim, we need to show, that f converges absolutely and uniformly on the disc $U_R(0)$, where $R > 0$ is fixed.

For a point $z \in U_R(0)$ and an element $\omega \in \Omega$ with $|\omega| > 2R$, we have the following two inequalities:

$$|2\omega - z| \leq |2\omega| + |z| \leq 3|\omega|$$

and

$$|z-\omega| \geq |\omega| - |z| \geq |\omega| - \frac{|\omega|}{2} = \frac{|\omega|}{2}.$$

From this we derive the following estimate for the summands of f.

$$\begin{aligned}
\left|\tfrac{1}{(z-\omega)^2} - \tfrac{1}{\omega^2}\right| &= \left|\tfrac{\omega^2 - z^2 + 2z\omega - \omega^2}{(z-\omega)^2\omega^2}\right| \\
&= \tfrac{|z|\,|2\omega - z|}{|z-\omega|^2|\omega|^2} \\
&\leq \tfrac{R\cdot 3|\omega|}{\frac{|\omega|^2}{4}|\omega|^2} \\
&= 12R\,\tfrac{1}{|\omega|^3}
\end{aligned}$$

Summing up gives the bound

$$\begin{aligned}
\sum_{\substack{\omega \in \Omega \setminus \{0\} \\ |\omega| > 2R}} \left|\tfrac{1}{(z-\omega)^2} - \tfrac{1}{\omega^2}\right| &\leq 12R \sum_{\substack{\omega \in \Omega \setminus \{0\} \\ |\omega| > 2R}} \tfrac{1}{|\omega|^3} \\
&\leq 12R \cdot G_3(\Omega)
\end{aligned}$$

which proves absolute convergence.

Since the Eisenstein series in independent of z, the convergence is uniformly as well.

We have thus shown that $\wp$ is a meromorphic function. We still need to see that $\wp$ is elliptic, i.e. periodic with respect to Ω.

(ii) Note that because of the summands $\frac{1}{(z-\omega)^2}$ we will have a pole for any $z \in C$ with $z \in \Omega$.

So consider $z \in \mathbb{C} \setminus \Omega$. We compute the first derivative $\wp'$ of $\wp$ by differentiating the summands of the series:

$$\wp'(z) = \frac{-2}{z^3} + \sum_{\omega \in \Omega \setminus \{0\}} \frac{-2}{(z-\omega)^3} = \sum_{\omega \in \Omega} \frac{-2}{(z-\omega)^3}.$$

Note that since $\wp$ is meromorphic, so is $\wp'$, and hence the series on the right is absolutely convergent. We therefore may reorder the summands, to obtain

$$\sum_{\omega \in \Omega} \frac{-2}{(z-\omega)^3} = \sum_{\omega \in \Omega} \frac{-2}{(z-\omega+\omega_0)^3}$$

for any element $\omega_0 \in \Omega$. This implies

$$\wp'(z) = \wp'(z+\omega_0)$$

or, equivalently,

$$\wp' \in \mathcal{K}(\Omega).$$

We now need to go back from the first derivative to the original function.

For any $\omega_0 \in \Omega$ we know by now that

$$(\wp(z) - \wp(z+\omega_0))' = 0 \text{ for all } z \in \mathbb{C} \setminus \Omega.$$

This is in particular true for the two generators ω_1, ω_2 of Ω.

By the standard rules for differentiation there must therefore exist constants $c_1, c_2 \in \mathbb{C}$ such that

$$\wp(z) = \wp(z + \omega_i) + c_i \text{ for all } z \in \mathbb{C} \setminus \Omega,\ i = 1, 2$$

The function $\wp$ is periodic if and only if $c_1 = c_2 = 0$.

To compute c_1, it suffices to consider one point of $\mathbb{C} \setminus \Omega$.

We choose $z := -\frac{\omega_1}{2}$.

Since ω_1 is a generator of Ω, we have $z \in \mathbb{C} \setminus \Omega$. We compute

$$\wp(-\frac{\omega_1}{2}) = \wp(\frac{\omega_1}{2}) + c_1 = \wp(-\frac{\omega_1}{2}) + c_1$$

For the last equality, we are using that $\wp$ is a symmetric function, as noted in 10.6.

From this immediately follows $c_1 = 0$, and analogously for c_2. $\square$

Lemma 10.7. *The poles of f are precisely the elements of the lattice Ω. All poles are of order 2. In particular, we have*

$$\operatorname{ord}(\wp) = 2.$$

Proof. Note that the semi-open parallelogram of periods P_{ω_1,ω_2} contains exactly one point of Ω, which is 0.

From calculus, we have the power series expansion at $z_0 = 0$

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

for all $\omega \neq 0$ and $|z| < |\omega|$. Thus

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + \sum_{\omega\in\Omega\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right) \\
&= \frac{1}{z^2} + \sum_{\omega\in\Omega\setminus\{0\}} \left(\sum_{j=2}^{\infty} \frac{jz^{j-1}}{\omega^{j+1}}\right) \\
&= \frac{1}{z^2} + \sum_{j=2}^{\infty} \left(j \cdot \sum_{\omega\in\Omega\setminus\{0\}} \frac{1}{\omega^{j+1}}\right) z^{j-1} \\
&= \frac{1}{z^2} + \sum_{\nu=1}^{\infty} (2\nu+1)\, G_{2\nu+2}(\Omega)\, z^{2\nu}
\end{aligned}$$

For the last equality recall that the Eisenstein series of odd weight are constantly zero. □

Remark 10.8. We have seen that the Weierstrass $\wp$-function is an even function of order 2, with a pole of order 2 at all points of the lattice Ω.

By differentiating the power series expansion of $\wp$, as we found it in the proof of lemma 10.7, we immediately see that $\wp'$ is an odd function

$$\wp'(-z) = -\wp(z) \text{ for all } z \in \mathbb{C}$$

of order 3, with poles of order 3 exactly at the elements of Ω.

Theorem 10.9. (Differential equation of the $\wp$-function)
For all $z \in \mathbb{C} \setminus \Omega$ holds

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

where

$$\begin{aligned} g_2 &:= 60\, G_4(\Omega), \\ g_3 &:= 140\, G_6(\Omega). \end{aligned}$$

Proof. Consider the meromorphic function

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

Note that $f \in \mathcal{K}(\Omega)$, and the only points, where f may possibly have poles, are the points of Ω.

In the proof of lemma 10.7, we computed the power series expansion of $\wp$, centered at 0 as

$$\wp(z) = \frac{1}{z^2} + 3G_4(\omega)z^2 + 5G_6(\Omega)z^4 + \dots$$

From this we get

$$4\wp(z)^3 = \frac{4}{z^6} + \frac{36}{z^2}G_4(\Omega) + 60G_6(\Omega)z^0 + 36G_4(\Omega)^2z^2 + \dots$$

Analogously, we get by differentiation

$$\wp'(z) = -\frac{2}{z^3} + 6G_4(\Omega)z + 20G_6(\Omega)z^3 + (\dots)z^5 + \dots$$

and thus

$$\wp'(z)^2 = \frac{4}{z^6} - \frac{24}{z^2}G_4(\Omega) - 80G_6(\Omega)z^0 + (\dots)z^2 + \dots$$

If we combine these power series expansions, and sort them by powers of z, then we obtain

$$\begin{aligned} f(z) = \quad & (4-4)\tfrac{1}{z^6} \\ & + \ (-24G_4(\omega) - 36G_4(\Omega) + g_2)\tfrac{1}{z^2} \\ & + \ (-80G_6(\Omega) - 60G_6(\Omega) + g_3)z^0 \\ & + \ (\ldots)z^2 \\ & + \ \ldots \end{aligned}$$

From this we see immediately that f can be extended over the point $z_0 = 0$ by $f(0) := 0$.

Since f is periodic, it extends over all points of Ω, so

$$f \in \mathcal{O}(\mathbb{C}) \cap \mathcal{K}(\Omega).$$

By proposition 9.8, the function f must be constant, and since we know $f(0) = 0$, we must have $f \equiv 0$.
Therefore the differential equation holds true. □

Lemma 10.10. (*i*) *The first derivative $\wp'$ of the Weierstrass $\wp$-function has exactly* 3 *zeroes on the semi-open parallelogram of periods P_{ω_1,ω_2}, which are*

$$\rho_1 = \frac{\omega_1}{2}, \quad \rho_2 = \frac{\omega_2}{2}, \quad \textit{and} \quad \rho_3 = \frac{\omega_1 + \omega_2}{2}.$$

Each of them has order 1.

(*ii*) *The values $e_i := \wp(\rho_i)$, $i = 1, 2, 3$ are pairwise different.*

Proof. (i) Since $\wp'$ is an odd and a periodic function, we have

$$\wp'(z) = -\wp'(-z) = -\wp'(\omega - z)$$

for all $\omega \in \Omega$ and all $z \in \mathbb{C} \setminus \Omega$.

In particular, for $z := \frac{\omega_1}{2}$ and $\omega := \omega_1$ we obtain

$$\wp'(\frac{\omega_1}{2}) = -\wp'(\frac{\omega_1}{2}).$$

Therefore $\wp'(\rho_1) = \wp'(\frac{\omega_1}{2}) = 0$.

Analogously we obtain $\wp'(\rho_2) = \wp'(\rho_3) = 0$.

The order of $\wp'$ equals 3 by 10.8.

Therefore, by theorem 9.10, the elliptic function $\wp'$ has exactly three zeroes, counted with orders, on the semi-open parallelogram of periods $\mathbb{P}_{\omega_1,\omega_2}$.

Since we found three distinct points ρ_1, ρ_2, ρ_3, where $\wp'$ vanishes, the vanishing order at each point must be equal to 1.

(ii) As an easy consequence of theorem 9.10, each value of $\wp$ is assumed in exactly $\mathrm{ord}(\wp) = 2$ points on the semi-open parallelogram of periods P_{ω_1,ω_2}, where we count with multiplicities.

By part (i) of the proof, we know that $\wp'(\rho_1) = 0$, so the value $e_1 = \wp(\rho_1)$ is assumed with multiplicity greater than 1.

So the multiplicity of the value e_1 at ρ_1 must equal 2, and there can be no other point, where this value is assumed.

In particular, $e_1 \neq e_2$ and $e_1 \neq e_3$.

The proof of $e_2 \neq e_3$ is analogous. $\square$

Proposition 10.11. *The Weierstrass $\wp$-function satisfies the differential equation*

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

Proof. Consider the elliptic function

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

Suppose that f is not constant.
Writing down the power series expansion as before, we get

$$f(z) = (4 - 4)\frac{1}{z^6} + (\dots)\frac{1}{z^4} + \dots$$

So f can have at most one pole of order 4 at $z_0 = 0$, and it has no other poles on the semi-open parallelogram of periods.

In particular, we must have $\mathrm{ord}(f) \leq 4$.
Let us count the zeroes of f.

Clearly, $f(\rho_i) = 0$ for $i = 1, 2, 3$, as these are the zeroes of $\wp'$.
Let us compute the first derivative of f

$$\begin{aligned} f'(z) = 2\wp'(z)\wp''(z) \; &- \; 4\wp'(z)(\wp(z) - e_2)(\wp(z) - e_3) \\ &- \; 4\wp'(z)(\wp(z) - e_1)(\wp(z) - e_3) \\ &- \; 4\wp'(z)(\wp(z) - e_1)(\wp(z) - e_3) \end{aligned}$$

Thus $f'(\rho_i) = 0$ for all $i = 1, 2, 3$. Therefore the order of each of the zeroes ρ_1, ρ_2, ρ_3 of f is at least 2.

This implies that the total number of zeroes on the semi-open parallelogram of periods, counted with multiplicities, is at least 6, contradicting the bound $\mathrm{ord}(f) \leq 4$.

Therefore, f must be constant.

Since $f(\rho_1) = 0$, we must have $f \equiv 0$. $\square$

Remark 10.12. Recall from Algebra, that a quadratic equation

$$ax^2 = bx + c = 0$$

with $a \neq 0$ admits exactly two different solutions

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

if and only if the *discriminant*

$$D := b^2 - 4ac$$

is different from zero.

In the same way, a cubic equation

$$ax^3 + 3bx^2 + 3cx + d = 0$$

with $a \neq 0$ has exactly three pairwise different solutions, if its *discriminant*

$$\Delta := a^2d^2 - 6abcd + 4ac^3 + 4b^3d - 3b^2c^2$$

is not equal to zero.

Corollary 10.13. *For a fixed lattice Ω, the above constants satisfy the following equations:*

$$\begin{aligned} g_3 &= 4e_1e_2e_3 \\ g_2 &= -4(e_1e_2 + e_1e_3 + e_2e_3) \\ 0 &= e_1 + e_2 + e_3 \\ g_2^3 - 27g_3^2 &= 16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2 \end{aligned}$$

We also have

$$g_2^3 - 27g_3^2 \neq 0.$$

Proof. Follows from the above. □

Lemma 10.14. *Let $z_1, z_2 \in \mathbb{C} \setminus \Omega$, such that $z_1 \not\equiv z_2 \mod \Omega$. Let $\wp(z_1) = \wp(z_2)$. Then $z_1 + z_2 \in \Omega$.*

In other words, the lemma is saying that $\wp(z_1) = \wp(z_2)$ implies that $z_2 \in \{-z_1, z_1\}$ modulo Ω.

Proof. For any $z \in \mathbb{C}$, there exists a unique $\omega_z \in \Omega$, so that $z + \omega_z$ is contained in the semi-open parallelogram of periods P of Ω.

Suppose that $\wp(z_1) = \wp(z_2) =: v$.

Since $\operatorname{ord}(\wp) = 2$, the value v is assumed on the semi-open parallelogram of periods at most twice.

Since $\wp$ is an even function, we know that $\wp(-z_1) = \wp(z_1)$. Therefore

$$\wp^{-1}(\{v\}) \cap P = \{z_1 + \omega_{z_1}, -z_1 + \omega_{-z_1}\}.$$

In particular, since $\wp(z_2) = v$, we must have

$$z_2 + \omega_{z_2} \in \{z_1 + \omega_{z_1}, -z_1 + \omega_{-z_1}\}$$

If $z_2 + \omega_{z_2} = z_1 + \omega_{z_1}$, then $z_1 \equiv z_2 \mod \Omega$, a contradiction to the assumption of the lemma.

Therefore we must have $z_2 + \omega_{z_2} = -z_1 + \omega_{-z_1}$, which implies $z_1 + z_2 \in \Omega$. □

Proposition 10.15. (Theorem of Addition) *Let $z_1, z_2 \in \mathbb{C} \setminus \Omega$, such that $z_1 + z_2 \notin \Omega$.*

Then

$$\wp(z_1 + z_2) = \begin{cases} \frac{1}{4}\left(\frac{\wp'(z_1)-\wp'(z_2)}{\wp(z_1)-\wp(z_2)}\right)^2 - \wp(z_1) - \wp(z_2) & \text{if } z_1 - z_2 \notin \Omega \\ \frac{1}{4}\left(\frac{12\wp(z_1)^2-g_2}{2\wp'(z_1)}\right)^2 - 2\wp(z_1) & \text{if } z_1 - z_2 \in \Omega \end{cases}$$

Proof. For the proof one applies exactly the same strategy that we used to show the differential equations for $\wp$ and $\wp'$ above. We leave it here as an exercise to the reader. □

Remark 10.16. (i) It is obvious that the first formula is symmetric in z_1 and z_2.

For the second formula, let $\omega := z_1 - z_2 \in \Omega$. Then $\wp(z_1) = \wp(\omega + z_2) = \wp(z_2)$ by the periodicity property, and analogously $\wp'(z_1) = \wp'(z_2)$.

(ii) We excluded the case $z_1 + z_2 \in \Omega$, since that would result in a pole of $\wp$. Note that this correspond on the right hand side to a division by zero.

In the first formula we find in the denominator

$$\wp(z_1) - \wp(z_2) = \wp(z_1 - (z_1 + z_2)) - \wp(z_2) = 0.$$

In the second case, where $\tilde{\omega} := z_1 - z_2 \in \Omega$,

$$2\wp'(z_1) = 2\wp'(z_1 - (\tilde{\omega} + z_1 + z_2)) = 2\wp'(-z_2) = 2\wp'(-z_1)$$

Since $\wp'$ is an odd function, we find for the denominator in this case $\wp'(z_1) = 0$, too.

Remark 10.17. Clearly, if $z_1 - z_2 \in \Omega$, then we have $\wp(z_1+z_2) = \wp(2z_1)$. The second part of the above formula is therefore also known as the *doubling formula*

$$\wp(2z) = \frac{1}{4}\left(\frac{12\wp(z)^2 - g_2}{2\wp'(z)}\right)^2 - 2\wp(z).$$

11. Complex Tori

Throughout this section let

$$\Omega = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} \subset \mathbb{C}$$

be a lattice, with fixed $\mathbb{R}$-linearly independent generators $\omega_1, \omega_2 \in \mathbb{C}$. Let

$$\overline{P} := \{t_1\omega_1 + t_2\omega_2 \in \mathbb{C} \text{ where } 0 \leq t_1, t_2 \leq 1\}$$

be the corresponding closed parallelogram of periods.

Definition 11.1. *A* complex torus *is a quotient*

$$\pi : \mathbb{C} \to \mathbb{C}/\Omega.$$

The equivalence class of a point $z \in \mathbb{C}$ *is denoted by*

$$[z] := \pi(z) := \ z \mod \omega.$$

The map π *is called the* quotient map*, and we usually write*

$$T := \mathbb{C}/\Omega.$$

It is clear from the construction of T that the restriction $\pi|\overline{P} \to T$ is surjective, but not injective.

Remark 11.2. Note that group structure "+" on $\mathbb{C}$ induces a well-defined composition on the quotient. For any two points $z_1, z_2 \in \mathbb{C}$, we put

$$[z_1] + [z_2] := [z_1 + z_2].$$

Note that for the identity element holds

$$[0] = [z] \quad \Leftrightarrow \quad z \in \Omega.$$

Thus the pair $(T, +)$ forms an Abelian group.

Definition 11.3. *A subset* $U \subseteq T$ *is called* open *if and only if its set-theoretic preimage* $\pi^{-1}(U) \subset \mathbb{C}$ *is open.*

Proposition 11.4. *With this definition, T becomes a topological space. Moreover, the quotient map $\pi : \mathbb{C} \to T$ is continuous, and T is compact.*

Proof. It is left to the reader to verify the axioms of a topological space for T, as well as the statement about the map π.

To prove compactness, consider some open covering of T

$$T = \bigcup_{i \in I} U_i$$

where $U_i \subset T$ is open for all $i \in I$, where I is some set of indices.

By the definition of the topology on T, all preimage sets $\pi^{-1}(U_i)$ are open in $\mathbb{C}$, and their union covers all of $\mathbb{C}$.

In particular, for the closed parallelogram of periods holds

$$\overline{P} \subset \bigcup_{i \in I} \pi^{-1}(U_i).$$

Since $\overline{P}$ is compact, there exists a finite number of indices $i_1, \ldots, i_n \in I$, such that

$$\overline{P} \subset \bigcup_{j=1,\ldots,n} \pi^{-1}(U_{i_j}).$$

By applying the quotient map, we obtain

$$T = \pi(\overline{P}) = \bigcup_{j=1,\ldots,n} U_{i_j}$$

and thus a finite sub-covering of T. □

What we want to do is to study meromorphic functions which are defined on the torus, instead of the complex plane.

This is the realm of differential geometry, and there in particular the theory of complex manifolds.

Luckily for us, we don't have do do the full abstract machinery. Since we are only interested in a very special example, namely the complex torus, we can define all the tools we need from scratch.

Definition 11.5. *Let $U \subseteq T$ be an open subset. A continuous map*

$$f : U \to \mathbb{C}$$

is called holomorphic *(or* meromorphic*) if the composed map*

$$f \circ \pi : \pi^{-1}(U) \to \mathbb{C}$$

is holomorphic (or meromorphic, respectively).

The set of all molomorphic functions on U is denoted by $\mathcal{O}(U)$, and the set of all meromorphic functions on U by $\mathcal{M}(U)$.

Remark 11.6. Again, it is not hard to verify, that $\mathcal{O}(U)$ has the natural structure of a ring, if summation and multiplication is done pointwise on the values, and $\mathcal{M}(U)$ is even a field.

Proposition 11.7. *Any holomorphic map on T is constant, i.e.*

$$\mathcal{O}(T) \;=\; \mathbb{C}.$$

Proof. Let $f \in \mathcal{O}(T)$.

Then by definition the composition $f \circ \pi : \mathbb{C} \to \mathbb{C}$ is holomorphic.

Since the torus T is compact, so is $f(T) = f \circ \pi(\mathbb{C})$.

In particular, the function $f \circ \pi$ is bounded.

By the theorem of Liouville, such a holomorphic function must be constant.

Since π is surjective, f must be constant, too. $\square$

Remark 11.8. Let $f \in \mathcal{M}(T)$ be a meromorphic function o the torus. By the definition of the quotient map π we have for all $z \in \mathbb{C}$

$$f \circ \pi(z) = f \circ \pi(z + \omega) \text{ for all } \omega \in \Omega.$$

This is equivalent to

$$f \circ \pi \in \mathcal{K}(\Omega),$$

so $f \circ \pi$ is an elliptic function with respect to Ω.

In this way, we obtain a map

$$\begin{aligned} \pi^* : \ \mathcal{M}(T) &\to \mathcal{K}(\Omega) \\ f &\mapsto f \circ \pi \end{aligned}$$

Exercise 11.9. Show that this map is a homomorphism of fields.

Theorem 11.10. *The map π^* is an isomorphism of fields.*

Proof. To prove surjectivity, consider an element $\tilde{f} \in \mathcal{K}(\Omega)$.

For any $t \in T$, choose some $z_t \in \mathbb{C}$, such that $\pi(z_t) = t$. Note that for any other choice $\tilde{z}_t \in \mathbb{C}$ satisfying $\pi(\tilde{z}_t)_t$, we have

$$\tilde{z}_t = z_t + \omega$$

for some $\omega \in \Omega$. Hence

$$\tilde{f}(\tilde{z}_t) = \tilde{f}(z_t)$$

since $\tilde{f}$ is elliptic.

We therefore have a well-defined map

$$\begin{array}{rccc} f: & T & \to & \mathbb{C} \\ & t & \mapsto & \tilde{f}(z_t) \end{array}$$

Let $z \in \mathbb{C}$. We compute

$$\pi^* f(z) = f \circ \pi(z) = f([z]) = \tilde{f}(z),$$

and thus $\tilde{f} = \pi^*(f)$.

Clearly, the map π^* is not constant, so as a homomorphism of fields it is injective. However, the reader is welcome to do the easy proof injectivity directly from the definition. □

The importance of the above theorem is that is allows us to carry over everything we learned about elliptic functions the theory of functions of complex tori.

Definition 11.11. *Let $f \in \mathcal{M}(T)$. The* order of f *is*

$$\mathrm{ord}(f) := \mathrm{ord}(\pi^* f).$$

Proposition 11.12. *Let $f \in \mathcal{M}(T)$ with $d := ord(f) > 0$. In particular, f is not constant. Then*

$$f : T \to \hat{\mathbb{C}}$$

is surjective, and any value $v \in \hat{\mathbb{C}}$ is assumed exactly d times, counted with multiplicities.

Definition 11.13. *Let $T = \mathbb{C}/\Omega$ and $T' = \mathbb{C}/\Omega'$ be two complex tori. A continuous map*

$$\varphi : T \to T'$$

is called holomorphic*, if for any open subset $U' \subseteq T'$ and for any $f \in \mathcal{O}(U')$ holds*

$$\varphi^*(f) := f \circ \varphi \in \mathcal{O}(\varphi^{-1}(U')).$$

Remark 11.14. Note that if φ is continuous, and $U' \subset T'$ is open, then $\varphi^{-1}(U') \subset T$ is open, too.
By definition, $\varphi^*(f)$ is holomorphic, if the composition

$$f \circ \varphi \circ \pi : \quad \pi^{-1}(\varphi^{-1}(U')) \to \mathbb{C}$$

is holomorphic in the classical sense.

It is easy to verify that for a holomorphic map φ, the map $\varphi^* : \mathcal{O}(U') \to \mathcal{O}(\varphi^{-1}(U'))$ is a homomorphism of rings.

Example 11.15. Let $m \in \mathbb{N}$ with $m > 0$. We define for a point $P \in T$

$$m \cdot P := P + \ldots + P$$

where we take the sum over m-times the point p. From this we get a map

$$\begin{array}{rccc} [m] : & T & \to & T \\ & P & \mapsto & m \cdot P \end{array}$$

In fact, $[m]$ is a holomorphic map.

Remark 11.16. The holomorphic map $[m] : T \to T$ is in fact a homomorphism of groups.

It therefore has kernel, and we define

$$T[m] := \ker([m])$$

By this definition, we have

$$\begin{aligned} T[m] &= \{P \in T \text{ such that } m \cdot P = [0]\} \\ &= \pi(\{z \in \mathbb{C} \text{ such that } mz \in \Omega\}) \\ &= \pi(\tfrac{1}{m}\Omega) \end{aligned}$$

As an Abelian group, we have $\Omega \cong \mathbb{Z} \times \mathbb{Z}$, so we obtain

$$\begin{aligned} T[m] &\cong \pi(\tfrac{1}{m}\mathbb{Z} \times \tfrac{1}{m}\mathbb{Z}) \\ &\cong \mathbb{Z}_m \times \mathbb{Z}_m \end{aligned}$$

The elements of $T[m]$ are called the *m-torsion points* of T.

Example 11.17. Let $Q \in T$ be fixed. We define a map

$$\begin{aligned} t_Q : \ T &\to \quad T \\ P &\mapsto \ P + Q \end{aligned}$$

This map is called the *translation on T by the element Q*. It is again a holomorphic map, but clearly not a homomorphism of groups (unless $Q = [0]$).

Exercise: Show that t_Q is biholomorphic, and $(t_Q)^{-1} = t_{-Q}$.

Definition 11.18. Let Ω and Ω' be two lattices with, $T = \mathbb{C}/\Omega$ and $T' = \mathbb{C}/\Omega'$ the two complex tori defined by them.
Let $\alpha \in \mathbb{C} \setminus \{0\}$. The map

$$\begin{array}{rccc} \alpha: & \mathbb{C} & \to & \mathbb{C} \\ & z & \mapsto & \alpha z \end{array}$$

is called a *homothety* between Ω and Ω' if

$$\alpha\Omega \subseteq \Omega'.$$

Remark 11.19. A homothety $\alpha : \mathbb{C} \to \mathbb{C}$ induces a holomorphic map

$$\varphi_\alpha : T \to T'$$

of complex tori, such that the diagram

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\alpha} & \mathbb{C} \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\ T & \xrightarrow[\varphi_\alpha]{} & T' \end{array}$$

commutes.
The condition of the homothety $\alpha\Omega \subseteq \Omega'$ ensures that the map

$$\varphi_\alpha([z]) := [\alpha z]$$

is well-defined:
Indeed, if $[z'] = [z]$ in T, then by definition $z' = z + \omega$ for some $\omega \in \Omega$.

Therefore $\alpha z' = \alpha z + \alpha\omega$. Since by assumption $\alpha\omega \in \Omega'$, we have

$$[\alpha z'] = [\alpha z]$$

in T'.

Note: φ_α is a homomorphism of groups.

Theorem 11.20. *Let $\varphi : T \to T'$ be a non-constant holomorphic map between complex tori. Then φ can be written as*

$$\varphi = t_Q \circ \varphi_\alpha$$

where φ_α is induced by a homothety with $\alpha \in \mathbb{C} \setminus \{0\}$ and t_Q is the translation by $Q := \varphi(0)$.

Proof. At this point, our interdisciplinary course could take a detour into *Topology*.

An elegant method to prove the theorem makes use of *liftings* to covering spaces, and the concept of a *universal cover* of a *non simply-connected* topological *manifold*. □

Corollary 11.21. *Let $\varphi : T \to T'$ be a non-constant holomorphic map. Then the following hold true.*

(i) φ is surjective.

(ii) φ is a homomorphism of groups $\Leftrightarrow \varphi([0]) = [0]$. (!!!)

(iii) φ is biholomorphic $\Leftrightarrow \alpha\Omega = \Omega'$.

Definition 11.22. *Let $\varphi : T \to T'$ be a non-constant holomorphic map. Let $\varphi = t_Q \circ \varphi_\alpha$ be its decomposition as in theorem 11.20. The* degree of φ *is*

$$\deg(\varphi) = |\ker(\varphi_\alpha)|.$$

Remark 11.23. In fact, we have

$$\ker(\varphi_\alpha) \ \cong \ \Omega'/\alpha\Omega$$

and $\deg(\varphi) = |\Omega'/\alpha\Omega| < \infty$.

Definition 11.24. *Let $\varphi : T \to T'$ be a non-constant holomorphic map. It is called an* isogeny*, if $\varphi([0]) = [0]$.*

Remark 11.25. By theorem 11.20, φ is an isogeny if and only if φ is a group homomorphism.

Proposition 11.26. *Let $\varphi : T \to T'$ be an isogeny with $\deg(\varphi) = d$. Then there exists a* dual isogeny $\varphi^\vee : T' \to T$*, such that*

$$\varphi^\vee \circ \varphi = [d].$$

Proof. By corollary 11.21, φ is surjective.

Hence for any point $Q \in T'$, there exists at least one point $P_Q \in T$ such that $\varphi(P_Q) = Q$.

We now define

$$\begin{aligned} \varphi^\vee : \ T' \ &\to \quad T \\ Q \ &\mapsto \ d \cdot P_Q. \end{aligned}$$

This map is well-defined. Indeed, suppose $\varphi(P) = \varphi(P') = Q$ for two points $P, P' \in T$. Then for $\alpha := P - P'$ we compute

$$\varphi(\alpha) = \varphi(P - P') = \varphi(P) - \varphi(P') = 0,$$

so $\alpha \in \ker(\varphi)$. Since $d = |\ker(\varphi)|$, it follows from group theory that

$$d \cdot \alpha \ = \ 0.$$

This implies $dP = dP'$, so $\varphi^\vee(Q)$ is well-defined.

Obviously, $\varphi^\vee \circ \varphi(P) = dP$, and $\varphi(0) = 0$.

To complete the proof, it remains to show that φ is holomorphic. This is left as a exercise to the reader. □

Remark 11.27. Isogenies from a torus T to itself are called *endomorphisms*. They can be thought of as "symmetries" of T.

Together they form the *ring of endomorphisms* of T.

Dual isogenies form an important tool in the study of this endomorphism ring. It provides important insights into the structure of complex tori, and ultimately the structure of elliptic curves (see below).

In particular, the study of endomorphisms gives rise to powerful methods to compute group orders of elliptic curves and their subgroups.

Construction 11.28. Let $T = \mathbb{C}/\Omega$ be a complex torus.

We define a map from T into the projective plane $\mathbb{P}^2$ as follows.

$$\begin{array}{rccc} \Phi: & T & \to & \mathbb{P}^2 \\ & [z] & \mapsto & (\wp(z) : \wp'(z) : 1). \end{array}$$

Note that this map is well-defined. If $[z] = [z']$, then by definition $z' = z + \omega$ for some $\omega \in \Omega$. Since $\wp$ and $\wp'$ are elliptic, we obtain $(\wp(z') : \wp'(z') : 1) = (\wp(z) : \wp'(z) : 1)$.

We can even makes sense of this for the point $[0] \in T$.

Use the properties of homogeneous coordinates to obtain

$$(\wp(z) : \wp'(z) : 1) \; = \; (z^3\wp(z) : z^3\wp'(z) : z^3).$$

Since $\wp$ has a pole of order 2 at 0 and $\wp'$ has a pole of order 3 at 0, the function $g(z) := z^3\wp'(z)$ does not have a zero at $z = 0$.

At the point [0] we now compute

$$\Phi([0]) = (0 : 1 : 0).$$

Let us consider the image of this map $\Phi(T) \subset \; P^2$. The differential equation of the Weierstrass $\wp$-function

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

implies for a point $[z] \in T$

$$\Phi([z]) \; \in \; V(Y^2Z - 4X^3 - g_2XZ^2 - g_3Z^3).$$

So the image of T is contained in a cubic curve!

The discriminant of this cubic curve can be computed as

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

By corollary 10.13, we have $\Delta \neq 0$, so the cubic is smooth.

In fact, by putting

$$\mathcal{O} := (0:1:0) = \Phi([0]),$$

we obtain an elliptic curve in (almost) Weierstrass normal form

$$(C_{g_2,g_3}, \mathcal{O})$$

with $C_{g_2,g_3} := V(Y^2Z - 4X^3 - g_2XZ^2 - g_3Z^3)$.
The coefficient "4" can easily be removed by a change of coordinates from X to $\sqrt[3]{4}X$.

Proposition 11.29. *The map constructed above*

$$\Phi : T \to C_{g_2,g_3}$$

is a bijective map of sets.

Remark 11.30. In fact, up to projective transformation in $\mathbb{P}^2$, any elliptic curve in Weierstrass normal form is the image of a complex torus.

Theorem 11.31. *The map constructed above*

$$\Phi : T \to C_{g_2,g_3}$$

is an isomorphism of groups

$$(T, +) \cong (C_{g_2,g_3}, \mathcal{O}).$$

Proof. We need to show for any $z_1, z_2 \in \mathbb{C}$ the identity

$$\Phi([z_1]) + \Phi([z_1]) \;=\; \Phi([z_1] + [z_2]).$$

In coordinates, this is equivalent to

$$(\wp(z_1) : \wp'(z_1) : 1) + (\wp(z_2) : \wp'(z_2) : 1) = (\wp(z_1+z_2) : \wp'(z_1+z_2) : 1).$$

Now compare proposition 3.13, for the rules of adding two points on a Weierstrass elliptic curve, and proposition 10.15 for the rules for addition in the Weierstrass $\wp$-function. □

Corollary 11.32. *Let T be a complex torus, and $C := C_{g_2,g_3}$ the corresponding elliptic curve.*
Then for all $0 \neq m \in \mathbb{N}$ holds

$$T[m] \;\cong\; C[m].$$

In particular, this gives a proof of proposition 6.13.

– THANK YOU ! –