# Complex elliptic curves

N. Goldhirsch, P. Golliard

21.11.2023

## Contents

# 1 Prelimiaries

We let $\Omega = \mathbb{Z}w_1 + \mathbb{Z}w_2$ be a lattice in $\mathbb{C}$.

**Theorem 1.1.** *The Weierstrass $\wp$-function*

$$\wp(z) = \wp_\Omega(z) = z^{-2} + \sum_{0 \neq w \in \Omega} ((z-w)^{-2} - w^{-2}) \qquad z \in \mathbb{C} \setminus \Omega,$$

*converges absolutely and uniformly in every compact subset of $\mathbb{C} \setminus \Omega$. It is an even elliptic function with respect to $\Omega$ and has poles of second order with residue $0$ in every lattice points of $\Omega$. The Laurent expansion at $0$ has the form*

$$\wp = z^{-2} + a_2 z^2 + ...$$

Moreover we have already seen that the Eisenstein series

$$G_k = G_k(\Omega) = \sum_{0 \neq w \in \Omega} w^{-k}, \qquad k \in \mathbb{Z},$$

converges absolutely for $k \geq 3$ and that $G_k(\Omega) = 0$ for odd $k \geq 3$ and any lattice $\Omega$ since the terms $w^{-k}$ and $(-w)^{-k}$ cancel out in the sum.

Finally, the last thing to remember from last week and which we will need later is a first differential equation:

**Proposition 1.2.** *The $\wp$−function satisfies the differential equation*

$$\wp'(z) = 4\wp(z)^3 - g_2\wp(z) - g_3 \tag{1}$$

*with the Weierstrass invariants*

$$g_2 := g_2(\Omega) := 60G_4(\Omega),$$

$$g_3 := g_3(\Omega) := 140G_6(\Omega).$$

**Remark.** *The lattice $\Omega$ is uniquely determined by $g_2(\Omega)$ and $g_3(\Omega)$.*

# 2 The discriminant and the j-invariant

We are finally ready to define three three constants $e_1, e_2, e_3$ and explore their properties. They will help us find some rather special invariants of lattice.

**Definition.** *Let $\Omega$ be a lattice spanned by two numbers $w_1$ and $w_2$. Then we set*

$$e_1 := \wp(\frac{w_1}{2}),$$

$$e_2 := \wp(\frac{w_2}{2}),$$

$$e_3 := \wp(\frac{w_3}{2}),$$

$$w_3 := w_1 + w_2.$$

With these new notion we obtain a second differential equation for the Weierstrass $\wp$-function.

**Proposition 2.1.** *For $z \in \mathbb{C} \setminus \Omega$ we have*

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

Proving this Comparing the differential equation (1) and the differential equation (2), we obtain the identity

$$4\wp^3 - g_2\wp - g_3 = 4(\wp - e_1)(\wp - e_2)(\wp - e_3).$$

Since the $\wp$-function takes more than three different values, we obtain the following identity of polynomials:

**Corollary.** *The following equality holds true for all $X \in \mathbb{C}$*

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

*In particular, we have*

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

Using these identites for $e_1, e_2, e_3$, we obtain the following relation.

**Corollary.** *We have*

$$g_2^3 - 27g_3^2 = 16(e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2 \neq 0.$$

*We define the discriminant of $\Omega$ by*

$$\Delta := \Delta(\Omega) := g_2^3 - 27g_3^2 = 16(e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2 \neq 0,$$

*and the $j$-invariant of $\Omega$ by*

$$j := j(\Omega) := \frac{(12g_2)^3}{\Delta} = -4 \cdot 12^3 \frac{(e_1e_2 + e_2e_3 + e_3e_1)^3}{(e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2}.$$

# 3 The dependence on the lattice

In this chapter we investigate the behaviour of $G_k(\Omega)$ and $\wp_\Omega$ when the lattice $\Omega$ varies.

## 3.1 Homogeneity and base change

If $\Omega$ is a lattice in $\mathbb{C}$, then $\lambda\Omega$ is a lattice for every $0 \neq \lambda \in \mathbb{C}$. From the series definitions of $G_k$ and $\wp$ it is clear that we have

$$\begin{aligned} \wp_{\lambda\Omega}(\lambda z) &= \lambda^{-2}\wp_\Omega(z), \\ G_k(\lambda\Omega) &= \lambda^{-k}G_k(\Omega). \end{aligned}$$

This also gives the identities

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

**Proposition 3.1.** *For two lattices $\Omega$ and $\Omega'$ in $\mathbb{C}$, the following are equivalent.*

- *We have $\Omega' = \lambda\Omega$ for some $0 \neq \lambda \in \mathbb{C}$.*
- $j(\Omega') = j(\Omega)$.

*Proof.* We have already observed above that $j(\lambda\Omega) = j(\Omega)$ for $\lambda \neq 0$. Conversely, suppose that $j(\Omega') = j(\Omega) \neq 0$. Then we have $g_2(\Omega) \neq 0$ and $g_2(\Omega') \neq 0$. Hence there is some $0 \neq \lambda \in \mathbb{C}$ such that

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

Using the fact that $\Delta = g_2^3 - 27g_3^2$ and $\Delta(\lambda\Omega) = \lambda^{-12}\Delta(\Omega)$, we obtain

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

Replacing $\lambda$ with $i\lambda$ if necessary, we get $g_2(\Omega') = g_2(\lambda\Omega)$ and $g_3(\Omega') = g_3(\lambda\Omega)$. We have seen that $g_2$ and $g_3$ uniquely determine the lattice, so we obtain that $\Omega' = \lambda\Omega$.
If $j(\Omega) = j(\Omega') = 0$, then $g_2(\Omega) = g_2(\Omega') = 0$, and it follows from cor (2) that $g_3(\Omega) \neq 0$ and $g_3(\Omega') \neq 0$. Now we can proceed in a similar way as before. $\square$

Let $(w_1, w_2)$ be basis of $\Omega$. Since $w_1, w_2$ are linearly independent over $\mathbb{R}$, we have $\tau := \frac{w_1}{w_2} \notin \mathbb{R}$. Replacing $w_1$ with $-w_1$ if necessary, we may assume that $\mathrm{Im}(\tau) > 0$. Hence, every lattice in $\mathbb{C}$ is of the form

$$\Omega = \lambda(\mathbb{Z}\tau + \mathbb{Z})$$

for some $\lambda \in \mathbb{C}$, and $\tau$ in the upper half plane

$$\mathbb{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}.$$

Since $\wp$ and $G_k$ are homogeneus in $\lambda$, it remains to study their behaviour on lattices $\Omega = \mathbb{Z}\tau + \mathbb{Z}$ as $\tau \in \mathbb{H}$ varies. Hence, we will now view $\wp$ and $G_k$ as functions of $\tau \in \mathbb{H}$, that is, we define

$$\wp(z;\tau) := \wp_{\mathbb{Z}\tau+\mathbb{Z}}(z),$$

$$G_k(\tau) := G_k(\mathbb{Z}\tau + \mathbb{Z}).$$

**Proposition 3.2.** *For* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ *we have*

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

*and*

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

*Proof.* Let $\tau' = \frac{a\tau+b}{c\tau+d}$. Then we have

$$\mathbb{Z}\tau' + \mathbb{Z} = \mathbb{Z}\frac{a\tau+b}{c\tau+d} + \mathbb{Z} = (c\tau+d)^{-1}(\mathbb{Z}(a\tau+b) + \mathbb{Z}(c\tau+d)) = (c\tau+d)^{-1}(\mathbb{Z}\tau+\mathbb{Z}).$$

Where we used that the map $x \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} x$ is a bijection on $\mathbb{Z}^2$. By the homogeneity of $G_k$ we obtain

$$G_k(\tau') = G_k(\mathbb{Z}\tau' + \mathbb{Z}) = G_k((c\tau + d)^{-1}(\mathbb{Z}\tau + \mathbb{Z})) = (c\tau + d)^k G_k(\tau),$$

and similarly for $\wp$. □

**Remark.** *The group* $\mathrm{SL}_2(\mathbb{R})$ *acts on* $\mathbb{H}$ *by fractional linear transformations*

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

*A holomorphic function* $f : \mathbb{H} \to \mathbb{C}$ *is called a modular form of weight* $k \in \mathbb{Z}$ *for* $\mathrm{SL}_2(\mathbb{Z})$ *if it satisfies the transformation law*

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

*for all* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ *and* $\tau \in \mathbb{H}$, *and if* $f(\tau)$ *remains bounded as* $\mathrm{Im}(\tau) \to \infty$.

## 3.2 Eisenstein series

For even $k \geq 4$ we may write the Eisenstein series $G_k(\tau)$ for $\tau \in \mathbb{H}$ as the series

$$G_k(\tau) = G_k(\mathbb{Z}\tau + \mathbb{Z}) = \sum_{0 \neq w \in \mathbb{Z}\tau + \mathbb{Z}} w^{-k} = \sum_{m,n \in \mathbb{Z}}{}' (m\tau + n)^{-k}, \tag{3}$$

where the symbol $\Sigma'$ means that the summand for $(m, n) = (0, 0)$ has to be omitted.
Since the sum converges absolutely and locally uniformly, the Eisenstein series $G_k(\tau)$ defines a holomorphic function on $\mathbb{H}$.

**Proposition 3.3.** *For* $\tau \in \mathbb{H}$ *and even* $k \geq 4$ *we have the Fourier expansion*

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

*where*

$$\zeta(s) = \sum_{m=1}^{\infty} m^{-s}, \quad s \in \mathbb{C}, \mathrm{Re}(s) > 1$$

*is the Riemann zeta function and*

$$\sigma_s(m) = \sum_{d|m} d^s, \quad (s \in \mathbb{R})$$

*is a generalized divisor sum. In particular,* $G_k(\tau)$ *is a modular form of weight* $k$ *for* $\mathrm{SL}_2(\mathbb{Z})$.

*Proof.* Since the Eisenstein series converges absolutely, we may write the series in (3) as

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

We will use the so-called Lipschitz formula

$$\sum_{n\in\mathbb{Z}}(\tau+n)^{-k} = \frac{(-2\pi i)^k}{(k-1)!}\sum_{s=1}^{\infty}\sum_{r=1}^{\infty} r^{k-1}e^{2\pi i r\tau}, \qquad (\tau\in\mathbb{H}, k\in\mathbb{N}, k\geq 3),$$

whose proof will omit for brevity. Then we obtain

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

By collecting the terms with $m = rs$ we obtain the stated Fourier expansion. Since the Fourier expansion of $G_k(\tau)$ does not have terms of negative index, we have $\lim_{\mathrm{Im}(\tau)\to\infty} G_k(\tau) = 2\zeta(k)$, that is, $G_k(\tau)$ remains bounded as $\mathrm{Im}(\tau)\to\infty$. We have al.ready seen above that $G_k(\tau)$ is holomorphic on $\mathbb{H}$ and satisfies the state transformation law under $\mathrm{SL}_2(\mathbb{Z})$. Hence $G_k(\tau)$ is a modular form of weight $k$. □

# 4 Lattices and elliptic curves

In this section we will investigate the connection between lattices and elliptic curves over $\mathbb{C}$.

## 4.1 The addition Theorem

Let $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ denote a lattice in $\mathbb{C}$ and $\wp(z) = \wp_\Omega(z) = \wp(z,\omega_1,\omega_2)$ be its Weierstrass $\wp$-function.

Recall a useful theorem from the past lesson:

**Theorem 4.1.** *Let $f\in\mathcal{K}(\Omega)$ and $P$ be a periodic parallelogram, then it holds that*

$$\sum_{c\in P} res_c f = 0$$

**Theorem 4.2** (Addition Theorem)**.** *Given $z, w\in\mathbb{C}$ with $z, w, z\pm w\notin\Omega$ it holds*

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

To prove the Addition Theorem we need the following Proposition.

**Proposition 4.3.** *For $w\in\mathbb{C}\setminus\frac{1}{2}\Omega$ the function*

$$f(z) := f(z,w) := \frac{1}{2}\frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)}$$

*is an elliptic function w.r.t the lattice $\Omega$ with first order poles at $z \in \Omega$ and $z \in -w + \Omega = \{-w + \omega : \omega \in \Omega\}$ with Laurent expansions:*

$$\begin{aligned} f(z) &= -\frac{1}{z} - \wp(w)z + O(z^2) \qquad \text{at} \quad z = 0 \\ f(z) &= \frac{1}{z+w} + c(w) + O(z) \qquad \text{at} \quad z = -w \end{aligned}$$

*for some constant $c(w) \in \mathbb{C}$, which we have to find out.*

*Proof.* Apart from the points $z \in \Omega$ and $z \in -w + \Omega$, we see that $f$ is also not defined at $z \in w + \Omega$. But since

$$\lim_{z \to w} f(z) = \frac{1}{2} \lim_{z \to w} \frac{\wp'(z) - \wp'(w)}{z - w} \frac{z - w}{\wp(z) - \wp(w)} = \frac{1}{2} \frac{\wp''(w)}{\wp'(w)}$$

they are removable singularities, i.e. $f$ is holomorphic in their neighbourhood. Note that the condition $w \in \mathbb{C} \setminus \frac{1}{2}\Omega$ ensures that $\wp'(w) \neq 0$.

The Laurent expansion of $f$ at $z = 0$ becomes manifest by using the Laurent expansion of $\wp$, namely $\wp(z) = z^{-2} + O(z^2)$.
Moreover, $\wp(z) - \wp(w)$ has a simple root at every $z \in -w + \Omega$, and $\wp'(z) - \wp'(w) = -2\wp(w) \neq 0$ (recall that $\wp$ is even and $\wp'$ is odd). Consequently $f$ has a simple poles at $z \in -w + \Omega$. Since the sum of the residues of $f$ in a fundamental parallelogram is 0 (compare Theorem 4.1), and since we have seen the residue at $z = 0$ equals $-1$, the residues at points $z \in -w + \Omega$ must be 1. This gives the stated Laurent expansions. □

*Proof of Theorem 4.2.* Consider the elliptic function

$$g(z) := f(z, w)^2 - \wp(z + w) - \wp(z) - \wp(w)$$

with $w \in \mathbb{C} \setminus \frac{1}{2}\Omega$.

From the above proposition we see that $g$ may have poles at points $z \in \Omega$ and $z \in -w + \Omega$.
At $z = 0$ we have:

$$g(z) = (z^{-2} + 2\wp(w)) - \wp(w) - z^{-2} - \wp(w) + O(z) = O(z)$$

and at $z = -w$:

$$g(z) = \frac{1}{(z+w)^2} + \frac{2c(w)}{z+w} - \frac{1}{(z+w)^2} + O(1) = \frac{2c(w)}{z+w} + O(1)$$

If now $c(w) \neq 0$ then $g$ would have simple poles only at the points $z \in -w + \Omega$, which is not possible since the sum of the residues must be 0 by Theorem 4.1. Hence $c(w) = 0$.
This means that $g$ is holomorphic, and thus constant ($f$ elliptic and holomorphic implies $f$ constant). Moreover from the Laurent expansion $g(z) = O(z)$ at $z = 0$ we find $g(z) = 0$.

This concludes the proof of the addition theorem in the case that $w \in \mathbb{C} \setminus \frac{1}{2}\Omega$. For the remaining points the addition theorem follows by continuity. □

The following corollaries are special cases of the Addition Theorem 4.2.

**Corollary.** *Given $z \in \mathbb{C} \setminus \frac{1}{2}\Omega$, then*

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

*Proof.* Obtained by letting $w \to z$. □

**Corollary.** *Given $z, w \in \mathbb{C}$ with $z, w, z \pm w \notin \Omega$ it holds*

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

*Proof.* We get the above statement by substituting $w$ by $-w$. □

## 4.2 The factor group $\mathbb{C}/\Omega$

For $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ a lattice in $\mathbb{C}$, we define the equivalence relation

$$z \sim w \iff z - w \in \Omega$$

The equivalence classes can be then written in the form $z + \Omega$ and the factor group $\mathbb{C}/\Omega := \{z + \Omega \, : \, z \in \mathbb{C}\}$. The canonical projection is denoted by $\pi$:

$$\pi \, : \, \mathbb{C} \to \mathbb{C}/\Omega \quad , \quad \pi(z) := z + \Omega$$

From last talk we know that for a parallelogram $P = \diamond(u, \omega_1, \omega_2)$ there exists for any $z \in \mathbb{C}$ exactly an $\omega \in \Omega$ with $z + \omega \in P$. This means that there is a one to one correspondence between $P$ and $\mathbb{C}/\Omega$ via $\pi$, i.e. the restriction $\pi|_P$ is bijective.

We can therefore imagine $\mathbb{C}/\Omega$ as a torus as the following picture describe:

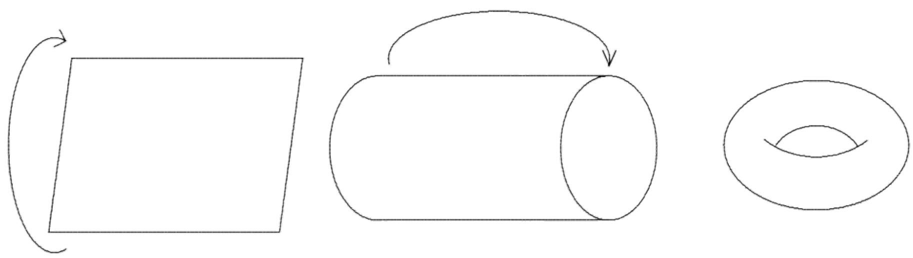

Figure 1: The torus $\mathbb{C}/\Omega$

## 4.3 Elliptic curves

**Definition.** *Let $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice in $\mathbb{C}$ with Weierstrass invariants $g_2$ and $g_3$. The subset*

$$\mathbb{E} := \mathbb{E}(\Omega) := \{(X, Y) \in \mathbb{C} \times \mathbb{C} \, : \, Y^2 = 4X^3 - g_2 X - g_3\}$$

*is called the (affine) elliptic curve associated to $\Omega$.*

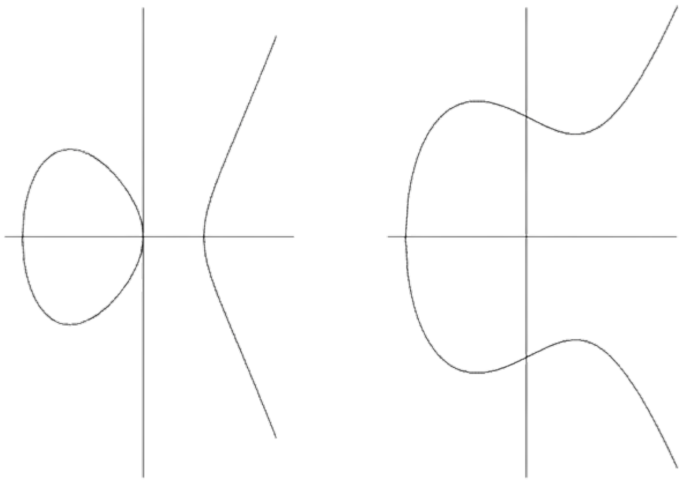

Figure 2: Elliptic curves $f$ and $g$

**Example.** *Suppose that $g_2, g_3$ are real numbers. Then we may look at the real points on $\mathbb{E}$, that is, the real solutions $(X, Y) \in \mathbb{R}^2$ of the equation $Y^2 = 4X^3 - g_2X - g_3$. The right-hand side has either three or one real root. Typical examples of such curves are $f : Y^2 = 4X^3 - 4X$ (with real roots $X = 0, \pm 1$) and $g : Y^2 = 4X^3 + 4$ (with real root $X = -1$).*

The Weierstrass $\wp$-function allows a parametrisation of the elliptic curve $\mathbb{E}$ trough $\mathbb{C}/\Omega$.

**Lemma 4.4.** *The map*

$$\Phi : (\mathbb{C}/\Omega) \setminus \Omega \to \mathbb{E}(\Omega) \quad , \quad \Phi(z + \Omega) := (\wp(z), \wp'(z))$$

*is a bijection.*

*Proof.* The differential equation $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$ shows that the image of $\Phi$ is indeed contained in $\mathbb{E}$.

For $(X, Y) \in \mathbb{E}$ we choose some $z \in \mathbb{C}$ with $\wp(z) = X$. Then we have

$$Y^2 = 4X^3 - g_2X - g_3 = 4\wp(z)^3 - g_2\wp(z) - g_3 = \wp'(z)^2$$

Hence we either have $Y = \wp'(z)$ or $Y = -\wp'(z)$. Since $\wp(z)$ is even and $\wp'(z)$ is odd, we may assume that $Y = \wp'(z)$ by replacing $z$ with $-z$ if necessary. This shows that $(X, Y)$ lies in the image of $\Phi$, therefore $\Phi$ is surjective.

Now suppose that there are $z_1, z_2 \in \mathbb{C}\backslash\Omega$ with $(\wp(z_1), \wp'(z_1)) = (\wp(z_2), \wp'(z_2))$. By a property of $\wp$ the identity $\wp(z_1) = \wp(z_2)$ implies $z_1 \sim \pm z_2$. If $\wp'(z_1) \neq 0$, then $z_1 \nsim -z_2$ since $\wp'$ is odd, so we must have $z_1 \sim z_2$. If $\wp'(z_1) = 0 = \wp'(z_2))$, then each of $z_1$ and $z_2$ is equivalent to one of $\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_3}{2}$. But since $\wp(\omega_k) = e_k$ for $k = 1, 2, 3$ are pairwise different, we must have $z_1 \sim z_2$. This shows that $\Phi$ is injective. $\square$

By a small adjustment we can extend the bijection to the whole factor group $\mathbb{C}/\Omega$. In fact we can consider the closure of $\mathbb{E}$ by adding a "point at infinity" $\mathcal{O} := (\infty, \infty)$:

$$\overline{\mathbb{E}} := \overline{\mathbb{E}}(\Omega) := \mathbb{E} \cup \{\mathcal{O}\}$$

In this way we get the bijection:

$$\overline{\Phi} \,:\, \mathbb{C}/\Omega \to \overline{E}(\Omega) \quad , \quad \overline{\Phi}(z+\Omega) := \begin{cases} (\wp(z), \wp'(z)) & \text{if} \quad z \notin \Omega \\ \mathcal{O} & \text{if} \quad z \in \Omega \end{cases}$$

Using the bijection $\overline{\Phi}$ one can now carry over the natural group structure of $\mathbb{C}/\Omega$ to the elliptic curve $\overline{\mathbb{E}}$: for $P, Q \in \overline{\mathbb{E}}$ we define their sum as:

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

We therefore directly obtain the following proposition.

**Proposition 4.5.** *Under the above defined sum, $\overline{\mathbb{E}}$ becomes a commutative group with unit element $\mathcal{O}$ and $\overline{\Phi}$ a group isomorphism. Moreover, for $z \in \mathbb{C}/\Omega$ the inverse element can be computed as*

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

*and for $u, v \in \mathbb{C}$ with $u, v, u+v \notin \Omega$ the addition can be computed as*

$$(\wp(u), \wp'(u)) + (\wp(v), \wp'(v)) = (\wp(u+v), \wp'(u+v))$$

# References


[1] M. Koecher and A. Krieg, *Elliptische Funktionen und Modulformen*, Springer, 2007

[2] M. Schwagenscheidt, *Elliptic Functions and Elliptic Curves*, Spring Term 2022 (update: May 28, 2022)