7. Elliptic Curves

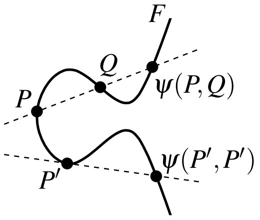
In this chapter, we will interrupt our general discussion of plane curves for a moment to study (projective) curves of degree 3 in detail. We have seen already that this is the first interesting case of curves in many respects: It is, for example, the lowest degree for which real or complex curves are topologically interesting (see Propositions 5.10 and 5.16), and for which the Picard group is non-trivial (see Example 6.33 and Proposition 6.34). We will show now that curves of degree 3 have in fact a very rich structure, both from an algebraic and — over $\mathbb{C}$ — from an analytic point of view. In the literature, they are usually called *elliptic curves*.

Definition 7.1 (Elliptic curves)**.** An **elliptic curve** is simply a projective cubic curve (which is smooth and defined over an algebraically closed field, in accordance with our convention at the beginning of Chapter 6).

The term "elliptic curve" might sound confusing at first, because the shape of a plane cubic curve has no similarities with an ellipse, not even over the real numbers (see e. g. Remark 5.8). The historical reason for this name is that the formula for the circumference of an ellipse can be expressed in terms of an integral over a plane cubic curve.

Probably the single most important (and surprising) result about elliptic curves is that they carry a natural group structure. The easiest, or at least the most conceptual way to prove this is by showing that an elliptic curve admits a natural bijection to its degree-0 Picard group. To establish this, we need the following construction.

Construction 7.2. Let P and Q be two (not necessarily distinct) points on an elliptic curve F. Then there is a unique line l with $P+Q \le \operatorname{div} l$ on F, namely the line through P and Q if these points are distinct, and the tangent line to F at $P=Q$ otherwise. But $\operatorname{div} l$ is an effective divisor of degree 3 by Remark 6.27 (a), and hence there is a unique point $R \in F$ (which need not be distinct from P and Q) with $\operatorname{div} l = P+Q+R$. In the following, we will denote this point R by $\psi(P,Q)$. In short, it is just "the third point of intersection of the line through P and Q with F".



Lemma 7.3. *For any three points P,Q,R on an elliptic curve F there is a point S on F such that $P+Q \sim R+S$, namely*

$$S = \psi(\psi(P,Q),R).$$

Proof. Applying Construction 7.2 to the points P and Q we find a line l with $\operatorname{div} l = P+Q+\psi(P,Q)$ on F. Similarly, for $\psi(P,Q)$ and R we find a line l' with $\operatorname{div} l' = \psi(P,Q)+R+\psi(\psi(P,Q),R)$. The quotient of these lines is then a rational function on F, whose divisor is therefore linearly equivalent to zero: We have

$$0 \sim \operatorname{div} \frac{l}{l'} = P+Q+\psi(P,Q) - (\psi(P,Q)+R+\psi(\psi(P,Q),R)),$$

and hence, as claimed, $P+Q \sim R+S$ with $S=\psi(\psi(P,Q),R)$. □

Proposition 7.4. *Let P_0 be a fixed point on an elliptic curve F. Then the map*

$$\Phi \colon V(F) \to \operatorname{Pic}^0 F,\ P \mapsto P - P_0$$

of Corollary 6.35 is a bijection.

Proof. As we already know by Corollary 6.35 that Φ is injective, it remains to prove surjectivity. So let D be an arbitrary element of $\operatorname{Pic}^0 F$, which we can write as

$$D = P_1 + \cdots + P_m - Q_1 - \cdots - Q_m$$

for some $m \in \mathbb{N}_{>0}$ and not necessarily distinct points $P_1,\dots,P_m,Q_1,\dots,Q_m \in F$. Assume first that $m \geq 2$. By Lemma 7.3 there is then a point $S \in F$ with $P_1+P_2 \sim Q_1+S$, and hence

$$D \sim S+P_3+\cdots+P_m-Q_2-\cdots-Q_m.$$

Up to linear equivalence, we have thus reduced the number m of (positive and negative) points in D by 1. Continuing this process as long as $m \geq 2$, we see that $D \sim P-Q$ for some $P,Q \in F$. In the same way, Lemma 7.3 now gives us a point T with $P+P_0 \sim Q+T$, i. e. with $D \sim P-Q \sim T-P_0$. But this means that $\Phi(T)=D$, i. e. that Φ is surjective. □

Remark 7.5. Let F be an elliptic curve. After choosing a base point $P_0 \in F$, Proposition 7.4 gives us a canonical bijection between the variety $V(F)$ and the Abelian group $\operatorname{Pic}^0 F$, i. e. between two very different types of mathematical objects. We can use it to give $V(F)$ the structure of an Abelian group, and $\operatorname{Pic}^0 F$ the structure of a smooth projective variety.

In fact, it can be shown that $\operatorname{Pic}^0 F$ can be made into a variety (the so-called *Picard variety*) for every smooth projective curve F. In contrast, the statement that $V(F)$ has a natural structure of an Abelian group is very special to elliptic curves. Let us explore this group structure in more detail.

Construction 7.6 (The group structure on an elliptic curve)**.** Let P_0 be a fixed base point on an elliptic curve F. As in Remark 7.5, we can use Proposition 7.4 to define a group structure on $V(F)$ in such a way that the map Φ becomes an isomorphism of groups. More precisely, if we denote this group operation on $V(F)$ by the symbol $\oplus$ (to distinguish it from the addition of points in $\operatorname{Div} F$ or $\operatorname{Pic} F$), then $P \oplus Q$ for $P,Q \in F$ is the unique point of F satisfying

$$\Phi(P \oplus Q) = \Phi(P) + \Phi(Q),$$

where "$+$" denotes the addition of divisors in $\operatorname{Pic}^0 F$. We can use Lemma 7.3 to solve this for $P \oplus Q$:

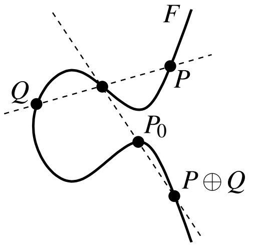
$$\begin{aligned}
P \oplus Q &= \Phi^{-1}(\Phi(P)+\Phi(Q)) \\
&= \Phi^{-1}(P-P_0+Q-P_0) \\
&= \Phi^{-1}(P+Q-2P_0) \\
&\overset{7.3}{=} \Phi^{-1}(P_0+\psi(\psi(P,Q),P_0)-2P_0) \\
&= \Phi^{-1}(\psi(\psi(P,Q),P_0)-P_0) \\
&= \psi(\psi(P,Q),P_0).
\end{aligned}$$

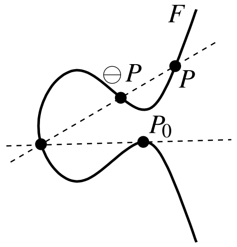
In other words, to construct the point $P \oplus Q$ we draw a line through P and Q. Then we draw another line through the third intersection point $\psi(P,Q)$ of this line with F and the point P_0. The third intersection point of this second line with F is then $P \oplus Q$, as in the picture below on the left.

Similarly, for the inverse $\ominus P$ of P in the above group structure we obtain

$$\begin{aligned}
\ominus P &= \Phi^{-1}(-\Phi(P)) \\
&= \Phi^{-1}(P_0-P) \\
&= \Phi^{-1}(P_0+P_0-P-P_0) \\
&\overset{7.3}{=} \Phi^{-1}(P+\psi(\psi(P_0,P_0),P)-P-P_0) \\
&= \psi(\psi(P_0,P_0),P).
\end{aligned}$$

So to construct the inverse $\ominus P$ we draw the tangent to F through P_0. Then we draw another line through the other intersection point $\psi(P_0,P_0)$ of this tangent with F and the point P. The third intersection point of this second line with F is $\ominus P$, as in the following picture.





Note that, using this geometric description, the operation $\oplus$ could also be defined in a completely elementary way, without referring to the theory of divisors. However, it would then be very difficult to show that we obtain a group structure in this way, in particular to prove associativity.

Remark 7.7 (Non-algebraically closed fields)**.** Let K' be a subfield of K which is not necessarily algebraically closed, such as $\mathbb{R}$ in $\mathbb{C}$ or a finite field in its algebraic closure. Assume that $F \in K'[x,y,z]$ is defined over K'. Note that for two points $P,Q \in V(F) \cap \mathbb{P}^2_{K'}$ on F with coordinates in K' the point $\psi(P,Q)$ then lies in $V(F) \cap \mathbb{P}^2_{K'}$ as well: The polynomial F restricted to the line through P and Q is a cubic homogeneous polynomial over K' that splits off two linear factors over K' corresponding to its zeros P and Q. Hence the remaining linear factor corresponding to $\psi(P,Q)$ is also defined over K', which means that $\psi(P,Q) \in V(F) \cap \mathbb{P}^2_{K'}$.

Choosing the base point P_0 in $V(F) \cap \mathbb{P}^2_{K'}$, we can therefore restrict the group structure on $V(F)$ to $V(F) \cap \mathbb{P}^2_{K'}$, obtaining a subgroup of $V(F)$.

Exercise 7.8. Let F be an elliptic curve of the form

$$F = y^2z - x^3 - \lambda xz^2 - \mu z^3$$

for some given $\lambda, \mu \in K$ (it can be shown that every elliptic curve can be brought into this form by a change of coordinates if the characteristic of K is not 2 or 3). Pick the point $P_0 = (0:1:0) \in F$ as the base point for the group structure on $V(F)$.

For given points P and Q on F compute explicitly the coordinates of the sum $P \oplus Q$ and the inverse $\ominus P$ in terms of the coordinates of P and Q.

Example 7.9 (Elliptic Curve Cryptography)**.** There is an interesting application of the group structure on an elliptic curve to cryptography. The key observation is that "multiplication is easy, but division is hard". More precisely, assume that we are given a specific elliptic curve F, and that we choose a base point $P_0 \in F$ for the group structure as well as an additional point $P \in F$. In view of Remark 7.7, the ground field for the curve does not have to be algebraically closed; in fact, for practical computations one will usually choose a finite field so that its elements can be stored in a chunk of computer memory of fixed size without rounding errors. Then we observe the following:

(a) Given $n \in \mathbb{N}$, the n-fold addition $n \odot P := P \oplus \cdots \oplus P$ can be computed very quickly using Exercise 7.8, even for very large n (think of numbers with hundreds of digits):

- By repeatedly applying the operation $P \mapsto P \oplus P$, we can compute all points $2^k \odot P$ for all k such that $2^k \leq n$.
- Now we just have to add these points $2^k \odot P$ for all k such that the k-th digit in the binary representation of n is 1.

This computes the point $n \odot P$ in a time proportional to $\log n$ (i. e. in a very short time).

(b) On the other hand, given a sufficiently general point $Q \in V(F)$ it is essentially impossible to compute an integer $n \in \mathbb{N}$ such that $n \odot P = Q$ (in case such a number exists). Note that this is not a mathematically precise statement — there is just no known algorithm that can perform the "inverse" of the multiplication of (a) in shorter time than a simple trial-and-error approach (which would be impractical for large n).

Let us now assume that Alice and Bob want to establish an encrypted communication over an insecure channel, but that they have not met in person before, so that they could not secretly agree on a key for the encryption. Using the above idea, they can then agree (publicly) on a ground field K, a specific elliptic curve F over K, a base point $P_0 \in V(F)$, and another point $P \in V(F)$. Now Alice picks a secret (very large) integer n, computes $n \odot P$ as in (a), and sends (the coordinates of) this point to Bob. In the same way, Bob chooses a secret number m, computes $m \odot P$, and sends this point to Alice.

As Alice knows her secret number n and the point $m \odot P$ from Bob, she can then compute the point $mn \odot P = n \odot (m \odot P)$. In the same way, Bob can compute this point as $mn \odot P = m \odot (n \odot P)$ as well. But except for the data of the chosen curve the only information they have exchanged publicly was P, $n \odot P$, and $m \odot P$, and by (b) it is not possible in practice to recover n or m, and hence $mn \odot P$, from these data. Hence Alice and Bob can use (the coordinates of) $mn \odot P$ as a secret key for their encrypted communication.

This method is actually used by many modern computer applications that need encryption, such as popular instant messengers for secure communication and file encryption software. The most common choice for the parameters is called Curve25519 in the literature, and uses the ground field $\mathbb{Z}/p\mathbb{Z}$ with the prime number $p = 2^{255} - 19$, the curve $F = y^2z - x^3 - 486662x^2z - xz^2$, the base point $P_0 = (0:1:0)$, and a point $P \in F$ with $x = 9$ and $z = 1$ [W].

Exercise 7.10. Let $F = y^2z - x^3 - \lambda xz^2$ be an elliptic curve as in Exercise 7.8 with $\mu = 0$, defined over a finite field of characteristic p (so that $\mathbb{Z}/p\mathbb{Z}$ is a subfield of K). Show:

(a) If $p = 3 \bmod 4$ then $V(F) \cap \mathbb{P}^2_{\mathbb{Z}/p\mathbb{Z}}$ contains exactly $p+1$ points.

(b) If $p = 1 \bmod 4$ then the number of points of $V(F) \cap \mathbb{P}^2_{\mathbb{Z}/p\mathbb{Z}}$ may also be smaller or bigger than $p+1$, but is always even.

Exercise 7.11. Let $F = y^2z - x^3 - \lambda xz^2 - \mu z^3$ be an elliptic curve as in Exercise 7.8.

Show that the subgroup $\{D \in \operatorname{Pic} F : 2D \sim 0\}$ of $\operatorname{Pic} F$ has exactly 4 elements and is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(Hint: Translate the problem to the group structure on $V(F)$.) 11

Let us now restrict our attention to the ground field $\mathbb{C}$, so that an elliptic curve is topologically a torus by Example 5.17 (a). In the remaining part of this chapter we want to see how these tori and elliptic curves arise in complex analysis in a totally different way. As we have not developed any analytic techniques in these notes we will only sketch most arguments; more details can be found e. g. in [Ki, Section 5.1]. Let us start by giving a quick review of what we will need from standard complex analysis. As usual, we will denote a complex variable in $\mathbb{C}$ by z. In contrast, for the rest of this chapter the homogeneous coordinates of $\mathbb{P}^2_{\mathbb{C}}$ will be called x_0, x_1, x_2 instead of x, y, z to avoid confusion.

Remark 7.12 (Holomorphic and meromorphic functions)**.** Let $U \subset \mathbb{C}$ be an open subset. Recall that a function $f\colon U \to \mathbb{C}$ is called *holomorphic* if it is complex differentiable at all points $z_0 \in U$, i. e. if the limit

$$f'(z_0) := \lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0}$$

exists. A function $f\colon U \to \mathbb{C} \cup \{\infty\}$ is called *meromorphic* if it is holomorphic except for some isolated singularities which are all poles, i. e. if for all $z_0 \in U$ there is a number $n \in \mathbb{Z}$ and a holomorphic function $\tilde{f}$ in a neighborhood of z_0 in U in which

$$f(z) = (z - z_0)^n \cdot \tilde{f}(z).$$

If f does not vanish identically in a neighborhood of z_0 we can moreover assume that $\tilde{f}(z_0) \neq 0$ in this representation; the number n is then uniquely determined. We will call it the *multiplicity* of f at z_0 and denote it by $\mu_{z_0}(f)$. It is obviously the analogue of the multiplicity of a rational function as in Construction 6.6 and Proposition 6.10 (b). The notions of (orders of) *zeros* and *poles* are used for meromorphic functions in the same way as for rational functions. Note that every rational function (i. e. every quotient of polynomials) in z is clearly meromorphic; there are however many more meromorphic than rational functions as e. g. the exponential function $z \mapsto \mathrm{e}^z$.

Remark 7.13 (Properties of holomorphic and meromorphic functions)**.** Although the definition of holomorphic, i. e. *complex* differentiable functions is formally exactly the same as that of *real* differentiable functions, the behavior of the complex and real cases is totally different. The most notable differences that we will need are:

(a) Every holomorphic function f is analytic, i. e. it can be represented locally around every point z_0 by its Taylor series. Consequently, a meromorphic function f of order n at z_0 can locally be expanded in a *Laurent series* as $f(z) = \sum_{k=n}^{\infty} c_k (z-z_0)^k$, with $n = \mu_{z_0}(f)$ [G4, Proposition 9.8]. The coefficient c_{-1} of this series is called the *residue* of f at z_0 and denoted by $\operatorname{res}_{z_0} f$.

(b) (*Residue Theorem*) If γ is a closed (positively oriented) path in $\mathbb{C}$ and f is a meromorphic function in a neighborhood of γ and its interior, without poles on γ itself, then

$$\int_\gamma f(z)\,dz = 2\pi\mathrm{i} \sum_{z_0} \operatorname{res}_{z_0} f,$$

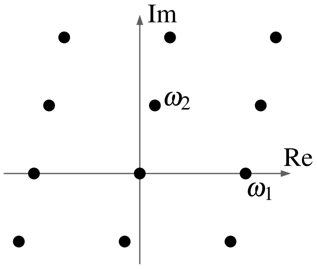
with the sum taken over all z_0 in the interior of γ (at which f has poles) [G4, Proposition 11.14]. In particular, if f is holomorphic in the interior of γ then this integral vanishes.

(c) (*Liouville's Theorem*) Every function that is holomorphic and bounded on the whole complex plane $\mathbb{C}$ is constant [G4, Proposition 8.2].

Construction 7.14 (Tori from lattices)**.** As mentioned above, for our applications to elliptic curves we have to construct a torus. To do this, fix two complex numbers $\omega_1, \omega_2 \in \mathbb{C}$ that are linearly independent over $\mathbb{R}$, i. e. that do not lie on the same real line in $\mathbb{C}$ through the origin. Then

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{m\omega_1 + n\omega_2 : m,n \in \mathbb{Z}\} \quad \subset \mathbb{C}$$

is called a *lattice* in $\mathbb{C}$, as indicated by the points in the picture on the right. It is an additive subgroup of $\mathbb{C}$, and the quotient $\mathbb{C}/\Lambda$ is topologically a torus.



For the rest of this chapter, Λ will always be a fixed lattice in $\mathbb{C}$. Note that functions on the torus $\mathbb{C}/\Lambda$ correspond exactly to Λ-*periodic* functions on $\mathbb{C}$, i. e. to functions f on $\mathbb{C}$ with $f(z+\omega) = f(z)$ for all $z \in \mathbb{C}$ and $\omega \in \Lambda$. In the following, we will use the concepts of functions on $\mathbb{C}/\Lambda$ and Λ-periodic functions on $\mathbb{C}$ interchangeably.

It is our goal to show that the torus $\mathbb{C}/\Lambda$ can be identified with an elliptic curve in a natural way. Let us start with a first auxiliary result that already indicates the similarities between the algebraic and analytic setting: We will show the analytic analogue of Remark 6.27 (b), namely that a meromorphic function on the torus $\mathbb{C}/\Lambda$ has equally many zeros as poles.

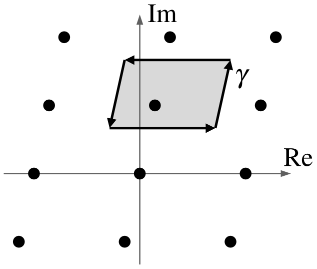
Lemma 7.15. *Let* $f \colon \mathbb{C}/\Lambda \to \mathbb{C} \cup \{\infty\}$ *be a non-zero meromorphic function. Then*

$$\sum_{z_0 \in \mathbb{C}/\Lambda} \mu_{z_0}(f) = 0.$$

Proof sketch. Let γ be the path around a "parallelogram of periodicity" as in the picture on the right, i. e. a parallelogram with side vectors spanning Λ. We choose it so that the zeros and poles of f do not lie on γ, and hence have a unique representative inside this parallelogram. It follows that

$$\int_\gamma \frac{f'(z)}{f(z)}\,dz = 0 \qquad (*)$$

since the integrals along opposite sides of the parallelogram cancel each other due to the periodicity of f.



On the other hand, we can compute this integral using the Residue Theorem of Remark 7.13 (b): At a point z_0 with $\mu_{z_0}(f) = n$ so that we can write $f(z) = (z-z_0)^n \tilde{f}(z)$ with $\tilde{f}$ holomorphic and non-zero around z_0 as in Remark 7.12 we have

$$\operatorname{res}_{z_0} \frac{f'}{f} = \operatorname{res}_{z_0} \frac{n\,(z-z_0)^{n-1}\tilde{f} + (z-z_0)^n \tilde{f}'}{(z-z_0)^n \tilde{f}} = \operatorname{res}_{z_0} \left(\frac{n}{z-z_0} + \frac{\tilde{f}'}{\tilde{f}} \right) = n = \mu_{z_0}(f),$$

and hence we obtain by the Residue Theorem

$$\int_\gamma \frac{f'(z)}{f(z)}\,dz = 2\pi\mathrm{i} \sum_{z_0 \in \mathbb{C}/\Lambda} \operatorname{res}_{z_0} \frac{f'}{f} = 2\pi\mathrm{i} \sum_{z_0 \in \mathbb{C}/\Lambda} \mu_{z_0}(f).$$

Comparing this with (∗) then gives the desired result. □

Remark 7.16 (Residue Theorem on manifolds)**.** In the same way as Remark 6.27 (b), Lemma 7.15 does not only hold for a torus $\mathbb{C}/\Lambda$, but also for an arbitrary compact 1-dimensional complex manifold X, and thus for any (smooth) complex projective curve. Let us briefly explain how to adapt the proof of Lemma 7.15 to this more general case.

The main step in this generalization is to extend the concepts of path integrals and the Residue Theorem from the complex plane to manifolds. This is not entirely straightforward, since the differential dz in the integral depends on the choice of a local coordinate z on X. As a consequence, there is no well-defined integral over a *function* on X since we would have to combine it with the coordinate-dependent dz to integrate it. Instead, we have to combine a function with a differential to obtain expressions of the form $\alpha = f\,dg$ for (meromorphic) functions f and g that satisfy the usual rules of differentiation. Such objects are called *differential forms* on X.

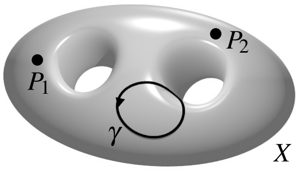
In these notes we will use differential forms only in a few side remarks that will not be needed later on, and hence we will not introduce them rigorously. Let us just mention that integrals and the Residue Theorem then behave as expected: For a closed path γ and a differential form α on X not having any poles on γ itself, we can define an integral $\int_\gamma \alpha$ whose value can be computed by the Residue Theorem

$$\int_\gamma \alpha = 2\pi\mathrm{i} \sum_P \operatorname{res}_P \alpha$$

as in Remark 7.13 (b), where the sum is taken over all points P in the interior of γ, and the residue of α at a point P is defined similarly to Remark 7.13 (a).

An additional benefit of this version of the Residue Theorem on manifolds is that we can exchange the roles of the interior and exterior of γ: Consider a differential form α on X with poles at some points (marked P_1 and P_2 in the picture below on the right). If we form the integral $\int_\gamma \alpha$ over a small loop γ that contains none of these points, the result will be 0 by the Residue Theorem. But we can also swap the roles of the interior and exterior of γ (without changing the value of the integral), so that now *all* poles lie in the interior of γ, and the Residue Theorem gives us the sum over all residues of α. Comparing these two results we see that

$$\sum_{P \in X} \operatorname{res}_P \alpha = 0,$$



which is also sometimes called the Residue Theorem (for manifolds) in the literature.

Applying this now to the differential form

$$\alpha = d(\log f) = \frac{f'(z)}{f(z)}\,dz \quad \text{gives us} \quad \sum_{P \in X} \operatorname{res}_P \frac{f'(z)}{f(z)}\,dz = 0,$$

and thus with the same (local) computation $\operatorname{res}_P \frac{f'(z)}{f(z)}\,dz = \mu_P(f)$ as in the proof of Lemma 7.15

$$\sum_{P \in X} \mu_P(f) = 0,$$

i. e. that f has equally many zeros as poles.

But let us now return to our study of the torus $\mathbb{C}/\Lambda$. The key ingredient to identify it with the points of an elliptic curve is the following meromorphic function.

Proposition and Definition 7.17 (The Weierstraß $\wp$-function)**.** *There is a meromorphic function $\wp$ on $\mathbb{C}$, called the **Weierstraß $\wp$-function** (pronounced like the letter "p"), defined by*

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

It has poles of order 2 exactly at the lattice points.

Proof sketch. It is a standard fact that an (infinite) sum of holomorphic functions is holomorphic at z_0 provided that the sum converges uniformly in a neighborhood of z_0. We will only sketch the proof of this convergence: Let $z_0 \in \mathbb{C}\setminus\Lambda$ be a fixed point that is not in the lattice. Then every summand is a holomorphic function in a neighborhood of z_0. The expansions of these summands for large ω are

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left(\frac{1}{(1-\frac{z}{\omega})^2} - 1 \right) = \frac{2z}{\omega^3} + \left(\text{terms of order at least } \frac{1}{\omega^4} \right),$$

so the summands grow like ω^3. Let us add up these values according to the absolute value of ω. Note that the number of lattice points with a given absolute value approximately equal to $n \in \mathbb{N}$ is roughly proportional to the area of the annulus with inner radius $n - \frac{1}{2}$ and outer radius $n + \frac{1}{2}$, which grows linearly with n. Hence the final sum is of the order $\sum_{n=1}^{\infty} n \cdot \frac{1}{n^3} = \sum_{n=1}^{\infty} \frac{1}{n^2}$, which is convergent.

Note that the sum would not have been convergent without the subtraction of the constant $\frac{1}{\omega^2}$ in each summand, as then the individual terms would grow like $\frac{1}{\omega^2}$, and therefore the final sum would be of the type $\sum_{n=1}^{\infty} \frac{1}{n}$, which is divergent.

Finally, the poles of order 2 at the points of Λ are clearly visible. □

Remark 7.18 (Properties of the $\wp$-function)**.** One can show that in an absolutely convergent series as above all manipulations (reordering of the summands, term-wise differentiation) can be performed as expected. In particular, the following properties of the $\wp$-function are obvious:

(a) The $\wp$-function is an even function, i. e. $\wp(z) = \wp(-z)$ for all $z \in \mathbb{C}$. Hence its Laurent series at 0 as in Remark 7.13 (a) contains only even exponents.

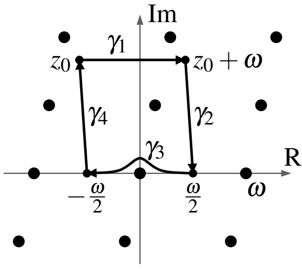
(b) Its derivative is $\wp'(z) = \sum_{\omega\in\Lambda} \frac{-2}{(z-\omega)^3}$. It is an odd function, i. e. $\wp'(z) = -\wp'(-z)$ for all z. In other words, its Laurent series at 0 contains only odd exponents. It has poles of order 3 exactly at the lattice points.

(c) The $\wp$-function is Λ-periodic, and hence gives a meromorphic function $\wp\colon \mathbb{C}/\Lambda \to \mathbb{C}\cup\{\infty\}$. To show this note first that $\wp'$ is Λ-periodic by (b). Now, for given $z_0 \in \mathbb{C}$ and $\omega \in \Lambda$ we integrate $\wp'$ along the path $\gamma = \gamma_1 + \gamma_2 + \gamma_3 + \gamma_4$ shown in the picture below on the right.

Of course, the result is 0, since $\wp$ is an integral of $\wp'$. But also the integral along γ_2 cancels the integral along γ_4 as $\wp'(z)$ is periodic. The integral along γ_3 is equal to $\wp(-\frac{\omega}{2}) - \wp(\frac{\omega}{2})$, so it vanishes as well since $\wp$ is an even function. So we conclude that

$$0 = \int_{\gamma_1} \wp'(z)\,dz = \wp(z_0+\omega) - \wp(z_0),$$

i. e. that $\wp$ is Λ-periodic.



Lemma 7.19 (Differential equation of the $\wp$-function)**.** *The $\wp$-function satisfies a differential equation*

$$\wp'(z)^2 = c_3\wp(z)^3 + c_2\wp(z)^2 + c_1\wp(z) + c_0 \quad \textit{for all } z \in \mathbb{C}$$

for some constants $c_0, c_1, c_2, c_3 \in \mathbb{C}$ (depending on Λ).

Proof sketch. By Remark 7.18 (b) we know that $(\wp')^2$ is an even function with a pole of order 6 at the origin. Hence its Laurent series around 0 is of the form

$$\wp'(z)^2 = \frac{a_{-6}}{z^6} + \frac{a_{-4}}{z^4} + \frac{a_{-2}}{z^2} + a_0 + (\text{terms of positive multiplicity at } 0)$$

for some constants $a_{-6}, a_{-4}, a_{-2}, a_0 \in \mathbb{C}$. The functions $\wp^3$, $\wp^2$, $\wp$, and 1 are also even and have poles at the origin of order 6, 4, 2, and 0, respectively. Hence there are constants $c_3, c_2, c_1, c_0 \in \mathbb{C}$ such that the Laurent series of the linear combination

$$f(z) := \wp'(z)^2 - c_3\wp(z)^3 - c_2\wp(z)^2 - c_1\wp(z) - c_0$$

has only positive powers of z. This means that f is holomorphic around the origin and vanishes at 0. But $\wp$ and $\wp'$, and hence also f, are Λ-periodic by Remark 7.18 (c). Hence f is holomorphic around all lattice points. Moreover, f is holomorphic around all other points as well, as $\wp$ and $\wp'$ are. Hence f is holomorphic on all of $\mathbb{C}$.

The Λ-periodicity means that every value taken on by f is already assumed on the parallelogram $\{x\omega_1 + y\omega_2 : x, y \in [0,1]\}$. As f is continuous, its image on this compact parallelogram, and hence on all of $\mathbb{C}$, is bounded. So we see by Liouville's Theorem of Remark 7.13 (c) that f must be constant. But as we have already shown that $f(0) = 0$, it follows that f is the zero function, which is exactly the statement of the lemma. □

Remark 7.20. By an explicit computation one can show that the coefficients c_3, c_2, c_1, c_0 in Lemma 7.19 are given by

$$c_3 = 4, \quad c_2 = 0, \quad c_1 = -60 \sum_{\omega \in \Lambda\backslash\{0\}} \frac{1}{\omega^4}, \quad \text{and} \quad c_0 = -140 \sum_{\omega \in \Lambda\backslash\{0\}} \frac{1}{\omega^6}.$$

The proof of Lemma 7.19 shows impressively the powerful methods of complex analysis: To prove our differential equation, i. e. the equality of the two functions $(\wp')^2$ and $c_3\wp^3 + c_2\wp^2 + c_1\wp + c_0$, it was sufficient to just compare four coefficients of their Laurent expansions at the origin — the rest then follows entirely from general theory.

Note also that the differential equation of Lemma 7.19 is a (non-homogeneous) cubic equation in the two functions $\wp$ and $\wp'$, which are Λ-periodic and thus well-defined on the quotient $\mathbb{C}/\Lambda$. We can therefore use it to obtain a map from $\mathbb{C}/\Lambda$ to an elliptic curve as follows.

Proposition 7.21 (Complex tori as elliptic curves)**.** *Consider the elliptic curve*

$$F = x_2^2x_0 - c_3x_1^3 - c_2x_1^2x_0 - c_1x_1x_0^2 - c_0x_0^3$$

for the constants $c_3, c_2, c_1, c_0 \in \mathbb{C}$ of Lemma 7.19. There is a bijection

$$\Psi\colon \mathbb{C}/\Lambda \to V(F),\ z \mapsto (1:\wp(z):\wp'(z)).$$

Proof sketch. As $\wp$ and $\wp'$ are Λ-periodic and satisfy the differential equation of Lemma 7.19, it is clear that Ψ is well-defined as a map to $V(F)$. Strictly speaking, for $z = 0$ we have to note that $\wp$ and $\wp'$ have poles of order 2 and 3, respectively, so that the given expression for $\Psi(0)$ is of the form $(1:\infty:\infty)$. But by Remark 7.12 we can write $\wp(z) = \frac{f(z)}{z^2}$ and $\wp'(z) = \frac{g(z)}{z^3}$ locally around the origin for some holomorphic functions f, g that do not vanish at 0, and so we have to interpret the expression for Ψ as

$$\Psi(0) = \lim_{z\to 0}(1:\wp(z):\wp'(z)) = \lim_{z\to 0}(z^3:zf(z):g(z)) = (0:0:1),$$

i. e. $\Psi(z)$ is well-defined at $z = 0$ as well.

Now let $(x_0:x_1:x_2) \in V(F)$ be a given point; we have to show that it has exactly one inverse image under Ψ. By what we have just said this is obvious for the "point at infinity" $(0:0:1)$, so let us assume that we are not at this point and hence pass to inhomogeneous coordinates where $x_0 = 1$. We thus have to show that there is exactly one (non-zero) $z \in \mathbb{C}/\Lambda$ with $\wp(z) = x_1$ and $\wp'(z) = x_2$.

Recall that $\wp$, and thus also $\wp - x_1$, has exactly one pole in $\mathbb{C}/\Lambda$, namely the origin, and that this pole is of order 2. Hence $\wp - x_1$ also has exactly two zeros (counted with multiplicities) in $\mathbb{C}/\Lambda$ by

Lemma 7.15, i. e. there are two $z \in \mathbb{C}/\Lambda$ with $\wp(z) = x_1$. For such a point z we then have by Lemma 7.19

$$\wp'(z)^2 = c_3\wp(z)^3 + c_2\wp(z)^2 + c_1\wp(z) + c_0 = c_3x_1^3 + c_2x_1^2 + c_1x_1 + c_0 = x_2^2$$

since $(1:x_1:x_2) \in V(F)$. So there are two possibilities:

- $\wp'(z) = 0$: Then $x_2 = 0$ as well, and z is a double zero (i. e. the only zero) of the function $\wp - x_1$. So there is exactly one $z \in \mathbb{C}/\Lambda$ with $\Psi(z) = (1:\wp(z):\wp'(z)) = (1:x_1:x_2)$.
- $\wp'(z) \neq 0$: Then z is only a simple zero of $\wp - x_1$. As $\wp$ is even and $\wp'$ odd by Remark 7.18, we see that $-z$ must be the other zero, and it satisfies $\wp'(-z) = -\wp'(z)$. Hence exactly one of the equations $\wp'(z) = x_2$ and $\wp'(-z) = x_2$ holds, and the corresponding point is the unique inverse image of $(1:x_1:x_2)$ under Ψ.

Altogether we conclude that Ψ is bijective, as we have claimed. □

Remark 7.22. In fact, the map Ψ of Proposition 7.21 is not just a bijection: Both $\mathbb{C}/\Lambda$ and $V(F)$ are 1-dimensional complex manifolds in a natural way, and Ψ is even an isomorphism between these two manifolds.

Remark 7.23 (Group structures on elliptic curves)**.** With Proposition 7.21 we are again in a similar situation as in Proposition 7.4: We have a bijection between a group $\mathbb{C}/\Lambda$ and a variety $V(F)$, so that the map Ψ of the above proposition can be used to construct a group structure on $V(F)$. In fact, we will see in Exercise 7.25 that this group structure is precisely the same as that obtained by the map Φ of Proposition 7.4 using divisors. But the algebraic properties of this group structure is a lot more obvious in this new picture: For example, the points of order n are easily read off to be the n^2 points

$$\frac{1}{n}(i\omega_1 + j\omega_2) \quad \text{for } 0 \le i,j < n.$$

Exercise 7.24. Let Λ be a lattice in $\mathbb{C}$, and let $P \neq Q$ be points in $\mathbb{C}/\Lambda$. Show that there is no meromorphic function on $\mathbb{C}/\Lambda$ with a simple zero at P, a simple pole at Q, and which is holomorphic with non-zero value at all other points.

Note that we can view this as an analytic analogue of Proposition 6.34 for elliptic curves.

Exercise 7.25. Let F be an elliptic curve corresponding to a torus $\mathbb{C}/\Lambda$ as in Proposition 7.21. Show that the group structure on $V(F)$ induced by $\operatorname{Pic}^0 F$ as in Proposition 7.4 (using $(0:0:1)$ as the base point) is the same as the one induced by the natural group structure of $\mathbb{C}/\Lambda$.

Exercise 7.26. Let $\Lambda \subset \mathbb{C}$ be a lattice. Given two points $z,w \in \mathbb{C}/\Lambda$, it is very easy to find a natural number n such that $n \cdot w = z$ (in the group structure of $\mathbb{C}/\Lambda$), in case such a number exists. Why is this no contradiction to the idea of the cryptographic application in Example 7.9? 12