15. Elliptic Curves

At the end of the last chapter we have used Picard groups to show in Proposition 14.19 and Remark 14.20 that smooth cubic curves in $\mathbb{P}^2$ are not isomorphic to $\mathbb{P}^1$. In fact, if our ground field is not necessarily $\mathbb{C}$ (so that we cannot apply topological methods as in Remark 13.19), this is the first class of smooth projective curves for which we could prove rigorously that they are not isomorphic to $\mathbb{P}^1$. So let us now study these curves in more detail. We will see that they have a very rich structure, both from an algebraic and — over $\mathbb{C}$ — from an analytic point of view.

Definition 15.1 (Elliptic curves)**.** In this chapter, by an **elliptic curve** we will simply mean a smooth cubic curve in $\mathbb{P}^2$.

Usually in the literature, an elliptic curve is defined to be a smooth complete curve of genus 1 (see Remark 13.13 and Exercise 13.20 for the definition of genus). Note that a smooth cubic curve in $\mathbb{P}^2$ is in fact complete by Example 7.22 (b) and of genus 1 by Example 13.18 (b) and Exercise 13.20. Conversely, one can show that every smooth complete curve of genus 1 can be embedded as a cubic curve in $\mathbb{P}^2$. Hence our somewhat non-standard definition of an elliptic curve is consistent with the literature.

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 13.9). 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 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 computing the degree-0 Picard group of an elliptic curve X, which (after the choice of a base point) turns out to be in natural bijection with X itself.

Proposition 15.2. *Let $X \subset \mathbb{P}^2$ be an elliptic curve, and let $a_0 \in X$ be a point. Then the map*

$$\Phi : X \to \operatorname{Pic}^0 X, \quad a \mapsto a - a_0$$

is a bijection.

Proof. As $\deg(a - a_0) = 0$, the map Φ is clearly well-defined. It is also injective: if $\Phi(a) = \Phi(b)$ for $a, b \in X$ this means that $a - a_0 = b - a_0$, and hence $a - b = 0$, in $\operatorname{Pic}^0 X$. By Proposition 14.19 this is only possible if $a = b$.

To show that Φ is surjective, let D be an arbitrary element of $\operatorname{Pic}^0 X$, which we can write as

$$D = a_1 + \cdots + a_m - b_1 - \cdots - b_m$$

for some $m \in \mathbb{N}_{>0}$ and not necessarily distinct $a_1, \ldots, a_m, b_1, \ldots, b_m \in X$. Assume first that $m \geq 2$. Then there are homogeneous linear polynomials l, l' on X such that $\operatorname{div} l = a_1 + a_2 + \psi(a_1, a_2)$ and $\operatorname{div} l' = b_1 + b_2 + \psi(b_1, b_2)$, where ψ is as in Notation 14.18. The quotient of these polynomials is then a rational function on X, whose divisor $a_1 + a_2 + \psi(a_1, a_2) - b_1 - b_2 - \psi(b_1, b_2)$ is therefore zero in $\operatorname{Pic}^0 X$. It follows that we can also write

$$D = \psi(b_1, b_2) + a_3 + \cdots + a_m - \psi(a_1, a_2) - b_3 - \cdots - b_m \quad \in \operatorname{Pic}^0 X.$$

We have thus reduced the number m of (positive and negative) points in D by 1. Continuing this process, we can assume that $m = 1$, i. e. that $D = a_1 - b_1$ for some $a_1, b_1 \in X$.

In the same way, we then also have

$$a_0 + a_1 + \psi(a_0, a_1) - b_1 - \psi(a_0, a_1) - \psi(b_1, \psi(a_0, a_1)) = 0 \quad \in \operatorname{Pic}^0 X,$$

so that $D = a_1 - b_1 = \psi(b_1, \psi(a_0, a_1)) - a_0 \in \mathrm{Pic}^0 X$. Hence $D = \Phi(\psi(b_1, \psi(a_0, a_1)))$, i. e. Φ is surjective. □

Remark 15.3. Let $X \subset \mathbb{P}^2$ be an elliptic curve. After choosing a base point $a_0 \in X$, Proposition 15.2 gives a canonical bijection between the variety X and the Abelian group $\mathrm{Pic}^0 X$, i. e. between two totally different mathematical objects. So we can use this bijection to give X the structure of an Abelian group, and $\mathrm{Pic}^0 X$ the structure of a smooth projective variety.

In fact, $\mathrm{Pic}^0 X$ can be made into a variety (the so-called *Picard variety*) for every smooth projective curve X. It is in general not isomorphic to X, however. One can only show that the map $\Phi : X \to \mathrm{Pic}^0 X$, $a \mapsto a - a_0$ of Proposition 15.2 is injective if X is not $\mathbb{P}^1$, so that we can then think of X as a subvariety of the Picard variety.

In contrast, the statement that X can be made into an Abelian group is very special to elliptic curves. In the following, we want to explore this group structure in more detail.

Construction 15.4 (The group structure on an elliptic curve)**.** Let a_0 be a fixed base point on an elliptic curve $X \subset \mathbb{P}^2$. As in Remark 15.3, we can use Proposition 15.2 to define a group structure on X. More precisely, if we denote this group operation by the symbol $\oplus$ (to distinguish it from the addition of points in $\mathrm{Div} X$ or $\mathrm{Pic} X$), then $a \oplus b$ for $a, b \in X$ is the unique point of X satisfying

$$\Phi(a \oplus b) = \Phi(a) + \Phi(b).$$

To find an explicit description for $a \oplus b$, note that — as in the proof of Proposition 15.2 — both $a + b + \psi(a,b)$ and $a_0 + \psi(a,b) + \psi(a_0, \psi(a,b))$ are divisors of homogeneous linear polynomials, and thus

$$a + b + \psi(a,b) - a_0 - \psi(a,b) - \psi(a_0, \psi(a,b)) = 0 \quad \in \mathrm{Pic}^0 X.$$

Hence

$$\begin{aligned} a \oplus b &= \Phi^{-1}(\Phi(a) + \Phi(b)) \\ &= \Phi^{-1}(a - a_0 + b - a_0) \\ &= \Phi^{-1}(\psi(a_0, \psi(a,b)) - a_0) \\ &= \psi(a_0, \psi(a,b)). \end{aligned}$$

In other words, to construct the point $a \oplus b$ we draw a line through a and b. Then we draw another line through the third intersection point $\psi(a,b)$ of this line with X and the point a_0. The third intersection point of this second line with X is then $a \oplus b$, as in the picture below on the left.

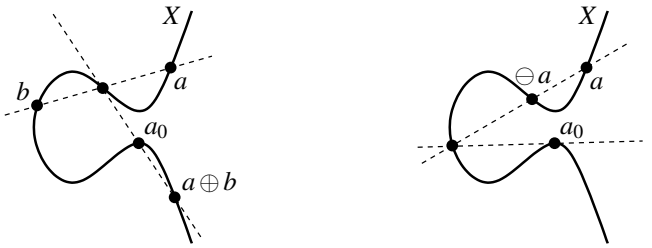
Similarly, to construct the inverse $\ominus a$ of a in the above group structure we use the relation

$$a_0 + a_0 + \psi(a_0, a_0) - a - \psi(a_0, a_0) - \psi(a, \psi(a_0, a_0)) = 0 \quad \in \mathrm{Pic}^0 X$$

to obtain

$$\begin{aligned} \ominus a &= \Phi^{-1}(-\Phi(a)) \\ &= \Phi^{-1}(a_0 - a) \\ &= \Phi^{-1}(\psi(a, \psi(a_0, a_0)) - a_0) \\ &= \psi(a, \psi(a_0, a_0)). \end{aligned}$$

So to construct the inverse $\ominus a$ we draw the tangent to X through a_0. Then we draw another line through the other intersection point $\psi(a_0, a_0)$ of this tangent with X and the point a. The third intersection point of this second line with X is $\ominus a$, 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.

Exercise 15.5. Let X and Y be two distinct elliptic curves in $\mathbb{P}^2$, and assume that they intersect in 9 distinct points $a_1,\dots,a_9$. Prove that every elliptic curve passing through $a_1,\dots,a_8$ also has to pass through a_9.

Can you find a stronger version of this statement that applies in the case when the intersection multiplicities in $X \cap Y$ are not all equal to 1?

Example 15.6 (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 X and a base point $a_0 \in X$ for the group structure.

(a) Given $a \in X$ and $n \in \mathbb{N}$, the n-fold addition $n \odot a := a \oplus \dots \oplus a$ can be computed very quickly, even for very large n (think of numbers with hundreds of digits):
   - By repeatedly applying the operation $a \mapsto a \oplus a$, we can compute all points $2^k \odot a$ for all k such that $2^k \leq n$.
   - Now we just have to add these points $2^k \odot a$ for all k such that the k-th digit in the binary representation of n is 1.

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

(b) On the other hand, given two sufficiently general points $a, b \in X$ it is essentially impossible to compute an integer $n \in \mathbb{N}$ such that $n \odot a = b$ (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 X over K, a base point $a_0 \in X$, and another point $a \in X$. Now Alice picks a secret (very large) integer n, computes $n \odot a$ as in (a), and sends (the coordinates of) this point to Bob. In the same way, Bob chooses a secret number m, computes $m \odot a$, and sends this point to Alice.

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

Exercise 15.7. Let X be an elliptic curve of the form

$$X = \{(x_0 : x_1 : x_2) : x_2^2 x_0 = x_1^3 + \lambda x_1 x_0^2 + \mu x_0^3\} \quad \subset \mathbb{P}^2$$

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 $a_0 = (0:0:1)$ as

the base point for the group structure on X. For given points $b = (b_0 : b_1 : b_2)$ and $c = (c_0 : c_1 : c_2)$ compute explicitly the coordinates of the inverse $\ominus b$ and of the sum $b \oplus c$. Conclude that the group structure on X is well-defined even if the ground field K is not necessarily algebraically closed. (This is important for practical computations, where one usually wants to work over finite fields in order to avoid rounding errors.)

25

Let us now restrict our attention to the ground field $\mathbb{C}$, so that an elliptic curve is topologically a torus by Example 13.18 (b). In the remaining part of this chapter we want to see how these tori arise in complex analysis in a totally different way. As we have not developed any analytic techniques in this class we will only sketch most arguments; more details can be found e. g. in [K, Section 5.1] (and many other books on complex analysis). Let us start by giving a quick review of what we will need from standard complex analysis.

Remark 15.8 (Holomorphic and meromorphic functions)**.** Let $U \subset \mathbb{C}$ be an open set in the classical topology. Recall that a function $f : U \to \mathbb{C}$ 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 $f : U \to \mathbb{C} \cup \{\infty\}$ 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 V of z_0 in U such that

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

on V. If f does not vanish identically in a neighborhood of z_0 we can moreover assume $\tilde{f}(z_0) \neq 0$ in this representation; the number n is then uniquely determined. We will call it the *order* of f at z_0 and denote it by $\operatorname{ord}_{z_0} f$. It is the analogue of the multiplicity of a rational function in Construction 14.5. If $n > 0$ we say that f has a *zero* of order n at z_0; if $n < 0$ then f has a *pole* of order $-n$ there. A meromorphic function is holomorphic around a point z_0 if and only if its order at this point is non-negative.

Of course, every regular (resp. rational) function on a Zariski-open subset of $\mathbb{A}^1_{\mathbb{C}} = \mathbb{C}$ is holomorphic (resp. meromorphic). However, there are many holomorphic (resp. meromorphic) functions that are not regular (resp. rational), e. g. $f : \mathbb{C} \to \mathbb{C}$, $z \mapsto e^z$.

Remark 15.9 (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 is automatically infinitely differentiable: all higher derivatives $f^{(k)}$ for $k \in \mathbb{N}$ exist and are again holomorphic [G4, Corollary 8.1].

(b) Every holomorphic function f is analytic, i. e. it can be represented locally around every point z_0 by its Taylor series. The radius of convergence is "as large as it can be", i. e. if f is holomorphic in an open ball U around z_0, then the Taylor series of f at z_0 converges and represents f at least on U. Consequently, a meromorphic function f of order n at z_0 can be expanded in a *Laurent series* as $f(z) = \sum_{k=n}^{\infty} c_k (z - z_0)^k$ [G4, Proposition 9.8]. The coefficient c_{-1} of this series is called the *residue* of f at z_0 and denoted by $\operatorname{res}_{z_0} f$.

Residues are related to orders of meromorphic functions as follows: if $f(z) = (z - z_0)^n \tilde{f}(z)$ as in Remark 15.8 above, we obtain

$$\operatorname{res}_{z_0} \frac{f'(z)}{f(z)} = \operatorname{res}_{z_0} \left(\frac{n}{z - z_0} + \frac{\tilde{f}'(z)}{\tilde{f}(z)} \right) = n = \operatorname{ord}_{z_0} f.$$

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

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

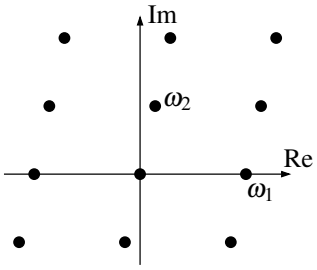
with the sum taken over all z_0 in the interior of γ (at which f has poles) [G4, Proposition 11.13]. In particular, if f is holomorphic in the interior of γ then this integral vanishes.

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

For our applications to elliptic curves we will need a particular meromorphic function. To describe its construction, 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. Note that Λ is an additive subgroup of $\mathbb{C}$, and that the quotient $\mathbb{C}/\Lambda$ is topologically a torus. We want to see that it can be identified with an elliptic curve in a natural way, using a map that we are going to introduce now.



Proposition and Definition 15.10 (The Weierstraß $\wp$-function)**.** *Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice in $\mathbb{C}$. 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 behaves like $\sum_{n=1}^\infty n \cdot \frac{1}{n^3} = \sum_{n=1}^\infty \frac{1}{n^2}$, 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 15.11 (Properties of the $\wp$-function)**.** It is a standard fact 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 contains only even exponents.

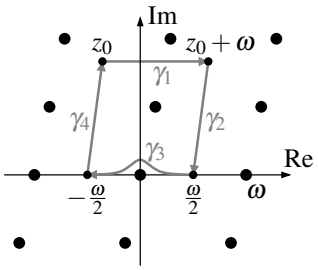
(b) Its derivative is $\wp'(z) = \sum_{\omega\in\Lambda} \frac{-2}{(z-\omega)^3}$. It is an odd function, i. e. $\wp'(z) = -\wp'(-z)$ for all z. In other words, its Laurent series at 0 contains only odd exponents. It has poles of order 3 exactly at the lattice points.

(c) The $\wp$-function is doubly periodic with respect to Λ, i. e. $\wp(z_0) = \wp(z_0+\omega)$ for all $z_0 \in \mathbb{C}$ and $\omega \in \Lambda$. To show this note first that it is obvious from (b) that $\wp'(z_0) = \wp'(z_0+\omega)$. Now integrate $\wp'(z)$ along the closed contour $\gamma = \gamma_1+\gamma_2+\gamma_3+\gamma_4$ 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. $\wp$ is periodic with respect to Λ.



Lemma 15.12. *The $\wp$-function associated to a lattice Λ satisfies a differential equation*

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

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

Proof. By Remark 15.11 (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

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

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 15.11 (c). Hence f is holomorphic around all lattice points. But f is also holomorphic around all other points, as $\wp$ and $\wp'$ are. In other words, f is holomorphic on all of $\mathbb{C}$.

Moreover, the 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 15.9 (d) 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 15.13. By an explicit computation one can show that the coefficients c_3, c_2, c_1, c_0 in Lemma 15.12 are given by

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

The proof of Lemma 15.12 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 15.12 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 15.14. *Let $\Lambda \subset \mathbb{C}$ be a fixed lattice, and let $X \subset \mathbb{P}^2_{\mathbb{C}}$ be the cubic curve*

$$X = \{(x_0 : x_1 : x_2) : x_2^2 x_0 = c_3 x_1^3 + c_2 x_1^2 x_0 + c_1 x_1 x_0^2 + c_0 x_0^3\}$$

for the constants $c_3, c_2, c_1, c_0 \in \mathbb{C}$ of Lemma 15.12. Then there is a bijection

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

Proof. As $\wp$ and $\wp'$ are periodic with respect to Λ and satisfy the differential equation of Lemma 15.12, it is clear that Ψ is well-defined as a map to X. (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 $\Psi(0)$ formally looks like $(1 : \infty : \infty)$. But by Remark 15.8 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

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

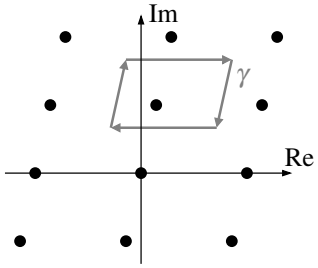
i. e. $\Psi(z)$ is well-defined at $z = 0$ as well.)

Now let $(x_0 : x_1 : x_2) \in X$ be a given point; we will show that it has exactly one inverse image point 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 will first look for a number $z \in \mathbb{C}$ such that $\wp(z) = x_1$. To do so, consider the integral

$$\int_\gamma \frac{\wp'(z)}{\wp(z) - x_1}\, dz$$

over the boundary of any "parallelogram of periodicity" (that does not meet the zeroes and poles of the function $z \mapsto \wp(z) - x_1$), as in the picture on the right. The integrals along opposite sides of the parallelogram vanish because of the periodicity of $\wp$ and $\wp'$, so that the total integral must be 0. Hence by Remark 15.9 (b) and (c) we get



$$0 = \sum_{z_0 \in \mathbb{C}/\Lambda} \operatorname{res}_{z_0} \frac{\wp'(z)}{\wp(z) - x_1} = \sum_{z_0 \in \mathbb{C}/\Lambda} \operatorname{ord}_{z_0}(\wp(z) - x_1).$$

In other words, the function $z \mapsto \wp(z) - x_1$ has as many zeroes as it has poles in $\mathbb{C}/\Lambda$, counted with multiplicities. (This is a statement in complex analysis analogous to the algebraic result of Remark 14.8 (b).) As $\wp$ has a pole of order 2 in the lattice points, it thus follows that there are exactly two points in $\wp^{-1}(x_1)$, counted with multiplicities.

For such a point z with $\wp(z) = x_1$ we then have by Lemma 15.12

$$\wp'(z)^2 = c_3 \wp(z)^3 + c_2 \wp(z)^2 + c_1 \wp(z) + c_0 = c_3 x_1^2 + x_2 x_1^2 + c_1 x_1 + c_0 = x_2^2$$

since $(1 : x_1 : x_2) \in X$. 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 $z \mapsto \wp(z) - x_1$. 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 $z \mapsto \wp(z) - x_1$. As $\wp$ is even and $\wp'$ odd by Remark 15.11, 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 15.15. With Proposition 15.14 we are again in a similar situation as in Proposition 15.2: we have a bijection between a group $\mathbb{C}/\Lambda$ and a variety X, so that the map Ψ of the above proposition can be used to construct a group structure on X. In fact, we will see in Exercise 15.17 that this group structure is precisely the same as that obtained by the map Φ of Proposition 15.2 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

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

It should be said however that the analytic bijection of Proposition 15.14 differs from that of Proposition 15.2 in that both $\mathbb{C}/\Lambda$ and X can independently be made into a 1-dimensional complex manifold, and the map Ψ of the above proposition is then an isomorphism between these two manifolds.

Exercise 15.16. Using the identification of an elliptic curve X with a torus $\mathbb{C}/\Lambda$ as in Proposition 15.14, reprove the statement of Proposition 14.19 that there is no rational function φ on an elliptic curve X with divisor $\operatorname{div}\varphi = a - b$ for distinct points $a, b \in X$.

Exercise 15.17. Let X be an elliptic curve corresponding to a torus $\mathbb{C}/\Lambda$. Show that the group structure of Pic^0_X is isomorphic to the natural group structure of $\mathbb{C}/\Lambda$.

Exercise 15.18. Let $\Lambda \subset \mathbb{C}$ be a lattice. Given two points $z, w \in \mathbb{C}/\Lambda$, it is obviously 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 15.6?

26