3. Del

Elliptic curves over the complex numbers

Version 0.2— *Monday, September 22, 2014 11:00:37 AM*

This is a raw and preliminary version, and will be expanded, but it covers basically what I'll do to day (monday). It is to found in Milne chapter III and Silverman chapter VI.

Historically the theory of elliptic curves grew out of the theory of elliptic integral, and the first such to be considered was the integral one has to solve when trying to compute the length of elliptic arc (*i.e.,* a portion of an ellipse). In the computation the following integral comes up

$$\int_0^a \sqrt{\frac{1-k^2x^2}{1-x^2}}\,dx, \tag{$\bigstar$}$$

where k is the eccentricity of the ellipse. This integral is not expressible in terms of the classical elementary functions, so one undertook a separate study of it, and of course of the greater class of so called elliptic integrals shearing the basic properties with the integral. These integrals have thousands of applications and there is an enormous literature about them, but we leave them here in the historical introduction. ellint

It turns out that the inverse functions to these integrals are simpler to work with, as discovered by Abel and Gauss. And they are what concerns us in this chapter. They are the *doubly periodic meromorphic* function in $\mathbb{C}$. Such functions have two periods ω_1 and ω_2 that are independent over the reals, *i.e.,* there is no real number t with $t\omega_1 = \omega_2$. The double periodic functions satisfy $f(z+\omega_i) = f(z)$ for all z, and one sees immediately that $f(z+n_1\omega_1+n_2\omega_2) = f(z)$ for all integers n_1 and n_2. The subset of $\mathbb{C}$ of these integral linear combinations form what one calls a *lattice*, the *period lattice* of f. Among the doubly periodic functions having a given lattice Λ as period lattice, there is one that stands out, namely the *Weierstrass $\wp$-function* (which even has the specially design glyph $\wp$ for it self). Together with its derivative, it satisfies the differential relation

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

so using $x(x) = \wp(z)$ and $y(z) = \wp'(z)$ one arrives at a parametrization of an elliptic curve on Weierstarss form (and of course, this is the origin of the term *Weierstrass form*). And one proves that any elliptic curve over $\mathbb{C}$ arise equivalent to one of this type.

3.1 Lattices

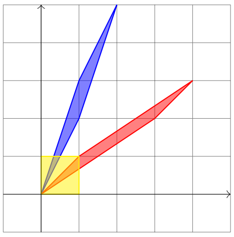
There is a general definition of a lattice—it is a discrete subgroup of an euclidean space—but in our context we simply say that a *lattice* Λ is an additive subgroup of the complex numbers $\mathbb{C}$ free of rank two that generate $\mathbb{C}$ as a real vector space.

If ω_1 and ω_2 are group-generators for Λ one has

$$\Lambda = \{\, n_1\omega_1 + n_2\omega_2 \mid n_1, n_2 \in \mathbb{Z}\,\},$$

and we say ω_1, ω_2 form a $\mathbb{Z}$-basis for Λ. Of course $\mathbb{Z}$-basis are no more unique than other bases.

A subset of the form $\{\, z+\lambda_1\omega_1+\lambda_2\omega_2 \mid 0 < \lambda_1, \lambda_2 < 1\,\}$ where $z \in \mathbb{C}$ is any element is called an *open fundamental parallelogram* for the lattice. Of course there are may such, they depend on the chosen basis and the point z.



Three different fundamental domains for the Gaussian lattice.

Including the four line segments bounding the parallelogram, we a *closed fundamental parallelogram*, and the set $F = \{\, z_0 + \lambda_1\omega_1 + \lambda_2\omega_2 \mid 0 \leq \lambda_1, \lambda_2 < 1\,\}$, where the two bounding line segments emanating from z are included, is what one calls a *fundamental domain*[1]. It has the property that in any translation class $\{\, z + \omega \mid \omega \in \Lambda\,\}$, there is *exactly* one element belonging to F:

[1] In general, if the group G acts on X a subset $A \subseteq X$ is a fundamental domain if every orbit Gx has exactly one point in common with A. That is a is a set of representatives of the quotient X/G. We reserve the term fundamental domain for a parallelogram that is a fundamental domain

Lemma 3.1 *Let A be a fundamental domain for the lattice Λ. Every point $a \in \mathbb{C}$ has exactly one translate $a + \omega$ lying in A.*

PROOF: Indeed, $z - z_0 = a_1\omega_1 + a_2\omega_2$ with the a_i's real numbers. One may write $a_i = n_i + \lambda_i$ where $n_i \in \mathbb{Z}$ and $0 \leq \lambda_i < 1$, and the n_i's and λ_i's are uniquely defined by these properties. Then one has $z - n_i\omega_1 + n_2\omega_2 = z_0 + \lambda_1\omega_1 + \lambda_2\omega_2 \in F$. ❏

THE QUOTIENT $\mathbb{C}/\Lambda$ Any lattice acts on the complex numbers by translation, *i.e.,* a lattice element ω acts as $z \mapsto z + \omega$, and the quotients $\mathbb{C}/\Lambda$ of $\mathbb{C}$ by this action, are the real heros of this story. The reason is that the functions on $\mathbb{C}/\Lambda$ correspond exactly to the doubly periodic functions on $\mathbb{C}$ having Λ as period lattice, that is functions $f(z)$ satisfying $f(z + \omega) = f(z)$ for all z and all $\omega \in \Lambda$.

Indeed, if one denotes by π the quotient map $\pi \colon \mathbb{C} \to \mathbb{C}/\Lambda$ and if g is a function on $\mathbb{C}/\Lambda$, the composition $f = \pi \circ g$ has Λ as period lattice:

$$f(z + \omega) = g(\pi(z + \omega)) = g(\pi(z)) = f(z)$$

since $\pi(z + \omega) = \pi(z)$.

On the other hand, if $f(z)$ is doubly periodic, f takes by definition the same value on all elements in the equivalence class $\{\, z + \omega \mid \omega \in \Lambda \,\}$, and therefore it descends to a function on $\mathbb{C}/\Lambda$.

We shall put a lot of more structure on the quotient. The first thing is a topology. We equip the quotient $\mathbb{C}/\Lambda$ by the quotient topology, a subset $U \subseteq \mathbb{C}/\Lambda$ being open if and only if the inverse image $\pi^{-1}U \subseteq \mathbb{C}$ is open, where π denotes the quotient map $\mathbb{C} \to \mathbb{C}/\Lambda$.

One may think of this construction as taking any closed fundamental parallelogram and identifying opposite sides. If you are in a playful mood imagine cutting the parallelogram out with scissors, fold it and glue opposite sides together—of course you need a copy of $\mathbb{C}$ made of a sufficently flexile material. In this manner you obtain a space looking like a doughnut—the precise statement being that $\mathbb{C}/\Lambda$ is homeomorphic to the product $\mathbb{S}^1 \times \mathbb{S}^1$ of two circles.

Secondly, we equip the quotient $\mathbb{C}/\Lambda$ with an analytic structure and thus making it into a Riemann surface. The genus of this Riemann surface is one, and we shall later on, in a canonical manner, identify such quotients with elliptic curves in $\mathbb{P}^2(\mathbb{C})$ in Weierstrass form. On of the fundamental theorems about elliptic curves over the complex numbers states that every elliptic curve $\mathbb{C}$ is isomorphic to such a quotient and describes precisely the relation between lattices giving rise to isomorphic elliptic curves. This is the main content of this chapter.

To put an analytic structure on any topological space, is to specify for any open set U which function in U are holomorphic. For $\mathbb{C}/\Lambda$ one simply declares a function f on $\mathbb{C}/\Lambda$ to be holomorphic in the open set U if the composition $f \circ \pi$ is holomorphic in the inverse image $\pi^{-1}U$.

Now $\mathbb{C}/\Lambda$ is the quotient of the additive group of complex numbers by an additive subgroup, and thus it is an abelian group. One easily verifies that this group is isomorphic to the direct product $\mathbb{S}^1 \times \mathbb{S}^1$ of two copies of the group $\mathbb{S}^1$ (addition in $\mathbb{C}$ is componentwise addition of the coordinates with respect to any real basis of $\mathbb{C}$, in particular ω_1, ω_2). And we shall prove that the isomorphism above indeed is a group homomorphism.

Of special interest is the field of meromorphic functions on $\mathbb{C}/\Lambda$. We shall denote this field by $K(\mathbb{C}/\Lambda)$. As we saw, if $f \in K(\mathbb{C}/\Lambda)$ the composition $g = f \circ \pi$ is a meromorphic function in $\mathbb{C}$, and it is doubly periodic with
Lambda as period lattice. In this way the field $K(\mathbb{C}/\Lambda)$ is identified with the field of meromorphic function with period lattice Λ.

PROBLEM 3.1. Show that the torsion subgroup of $\mathbb{C}/\Lambda$ is isomorphic to $\mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z}$. ✷

PROBLEM 3.2. Show that the subgroup of n-torsion points in $\mathbb{C}/\Lambda$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. ✷

3.2 Basics of double periodic functions

Liouville prove several results about double periodic functions, and the following three results are among them.

The first one is just an asaption of his famous theorem from complex anaøysis stating that bounded holomorphic functions in $\mathbb{C}$ are constatnt, an the ohters all rely on versions of Cauchy's integral theorem. We fix a lattice Λ and basis ω_1, ω_2. Recall that a closed fundamental parallelogram for Λ is a set of the form

$$A_z = \{\, z + \lambda_1\omega_1 + \lambda_2\omega_2 \mid 0 \leq \lambda_1, \lambda_2 \leq 1 \,\}.$$

Geometrically it is the parallelogram whose corners are z, $z+\omega_1$, $z+\omega_2$ and $z+\omega_1+\omega_2$.

The first of Liouville's theorems is a special case of a very general theorem about holomorphic functions on a compact Riemann surface (or even variety of higher dimension as long as it is compact), if they are globally holomorphic, they are constant.

Liouville1

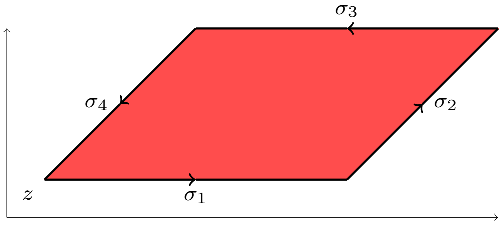
Proposition 3.1 (Liouville's first) *Is $f(z)$ is a Λ-periodic function holomorphic everywhere in $\mathbb{C}$, the $f(z)$ is constant.*

PROOF: Let A be a closed fundamental domain, *e.g.,* the parallelogram with corners 0, ω_1, ω_2 and $\omega_1 + \omega_2$. Then A is compact, and f being continuous on A, the absolute value $|f|$ is bounded on A, say by M. For any point $z \in \mathbb{C}$, some translate $z + \omega$ lies in A, but then $|f(z)| = |f(z+\omega)| \leq M$, and by Liouville's theorem about bounded holomorphic functions, f is constant. ❏

The boundary ∂A of a fundamental domain A consists four line segments σ_i oriented as in the figurer below. If $f(z)$ is double periodic and continuous on ∂A_z, one has

$$\int_{\sigma_1} f = -\int_{\sigma_3} f \qquad \int_{\sigma_2} f = -\int_{\sigma_4} f.$$

Indeed, the substitutions $z \mapsto z+\omega_2$ and $z \mapsto z+\omega_1$ take respectively σ_1 to σ_3 reversed and σ_2 to σ_4 reversed, and one has $d(z+\omega_1) = dz$ and $d(z+\omega_2) = dz$.



A fundamental domain with oriented boundary

This means that $\int_{\partial A} f = 0$. Combined with Cauchy's residue theorem this gives:

Liouville2

Proposition 3.2 (Liouville's second) *Let A be fundamental parallelogram for the lattice Λ, and assume that the Λ-periodic meromorphic function f has no poles on the boundary of A. Then $\sum_{a \in A} \operatorname{res}_a(f) = 0$*

Proof: Indeed, by Cauchy's theorem

$$\sum_{a \in A} \operatorname{res}_a(f) = \frac{1}{2\pi i} \int_{\partial A} f = 0.$$

❏

It might of course happen that f has a pole on the boundary of A. One may then slightly translate the fundamental parallelogram and apply the proposition with the new parallelogram and in that manner obtain information about the residues. For example, using an A based at a non-lattice-point z, one proves that there is no doubly periodic function with simple poles at the lattice points as the only singularities. A little more generally one has:

Corollary 3.1 *There is no Λ-periodic meromorphic function having as only singularities simple poles at the translates of a point a.*

Proof: Indeed, choose a fundamental domain A so that a lies in the interior of A. Then there is no poles on the boundary ∂A, and a is the only pole in the interior of A. By the proposition one has $\operatorname{res}_a(f) = 0$. But since the pole was supposed to be simple, this means that f does not have a pole at a. ❏

The derivative $f'(z)$ is Λ-periodic whenever $f(z)$ is, indeed the identity $f(z+\omega) = f(z)$ for all z gives $f'(z+\omega) = f'(z)$. Hence the meromorphic function $f'(z)/f(z)$ is Λ-periodic as well. Recall that the order $\nu = \operatorname{ord}_z(f)$ of a meromorphic[2] function at a is the integer ν such that $f(z) = (z-a)^\nu g(z)$ where $g(z)$ is holomorphic and non-vanishing at a. Hence

$$\frac{f'(z)}{f(z)} = \frac{\nu}{z-a} + \frac{g'(z)}{g(z)}.$$

Since $g(z)$ does not vanish at a, the quotient $g'(z)/g(z)$ is holomorphic at a, and it follows that the residue of $f(z)/f(z)$ at a equals the order $\operatorname{ord}_a(f)$. Applying Cauchy's residue theorem one arrives at

$$\frac{1}{2\pi i}\int_{\partial A} f'/f = \sum_{a\in A} \operatorname{res}_a(f'/f) = \sum_{a\in A} \operatorname{ord}_a(f).$$

Liouville3

Proposition 3.3 (Liouville's third) *Let f be a Λ-periodic meromorphic function. Assume that A is a fundamental domain without any of the poles of f lying on the boundary. Then $\sum_{a\in A} \operatorname{ord}_a(f) = 0$.*

PROOF: After what we just did, it suffices to say that

$$0 = \int_{\partial A} f'/f = \sum_{a\in A} \operatorname{ord}_a(f).$$

❏

A Λ-periodic function therefore has as many zeros as poles in any fundamental domain A (they must of course be counted with multiplicities). One can even say a lot more. Given any complex number w and let $g(z)$ be defined such $g(z) = f(z) - w$. The of course the zeroz of g are the soliutions of the equation

$$f(z) = w. \tag{✣}$$

BanalEqu

Clearly a is a pole of $g(z)$ if and only if it is a pole of $f(z)$ and the pole orders at a are the same (adding a constant does not change the principal part of a function). So it follows that the equation (✣) has the same number of solutions in A as $f(z)$ has zeros, or phrased slightly differently, the number of solution is independent of w! And this nuber equal the number of poles. In particular if $f(z)$ is not constant, it has at least one pole by proposition 3.3, and therefore the equation (✣) has a solution.

Any meromorphic function defines a map $\mathbb{C}/\Lambda \to \mathbb{P}^1(\mathbb{C})$ which we continue to denote by $f(z)$. Intuitively one extends the definition of f in the obvious way by sending

[2] Not all functions have an order at a even if they are holomorphic on a (deleted) neigbourhood. Being meromorphic is almost by definition equivalent to having an order at every point.

the poles of f to the point $(1;0)$ at infinity. Formally on extends f by sending z to $(f(z);1)$ when z is not a pole and to $(1;1/f(z))$ when z is not a zero. The coordinates being homogenous, the two assignments coincide in points which are neither poles nor zeros.

MeroSurjective

Proposition 3.4 *Assume that $f(z)$ is a meromorphic Λ-periodic function. Then f is surjective.*

The last result we give in this section is of a slightly more subtle nature than the precedeeing ones. It says that the difference between the sum of the zeros and sum of the poles of a Λ-periodic function is a period when counted with multiplicity. The converse problem is substantially more complicated to resolve. The question is: Given a finite collection of points a_i with corresponding integers ν_i, when can one find a Λ-periodic function having the prescribed order ν_i at a_i (and order zero elsewhere)? The answer, found by Abel, is that $\sum_i \nu_i a_i$ has to be a period. It is the genus one case of a similar result he proved for any compact Riemann surface.

Abel

Proposition 3.5 (Liouville, Abel) *Let f be a Λ-periodic meromorphic function. Assume that A is a fundamental domain without any of the poles of f lying on the boundary. Then one has $\sum_{a\in A} \operatorname{ord}_a(f)\cdot a \in \Lambda$.*

PROOF: The idea is to apply Cauchy's residue theorem to the function $zf'(z)/f(z)$, the residue of this function at a being $a \cdot \operatorname{ord}_a(f)$. This function is no longer periodic, so the simple cancellation argument for integrals along opposing line segments of the boundary is not valid. However the substitution $z \mapsto z+\omega_2$ gives

$$\int_{\sigma_3} zf'/f = -\int_{\sigma_1} zf'/f - \omega_2\int_{\sigma_1} f'/f = -\int_{\sigma_1} zf'/f - (\log f(z) - \log f(z+\omega_1))$$

since $f'/f = d\log f$. Now $f(z) = f(z+\omega_1)$, but complex logarithms can be tricky stuff[3]. They are not uniquely defined, so it does not follow that $\log f(z) = \log f(z+\omega_1)$. However, the ambiguity in the logarithm is always an integral multiple of $2\pi i$, and we can conclude that

$$\int_{\sigma_3} zf'/f + \int_{\sigma_1} zf'/f = 2\pi i n\omega_2$$

for an *integer* n. In a similar fashion one finds

$$\int_{\sigma_2} zf'/f + \int_{\sigma_4} zf'/f = 2\pi i n'\omega_1$$

for an $n' \in \mathbb{Z}$. Together with the observation about the residues in the beginning of the proof, these two equalities and Cauchy's residue theorem give

$$\sum_{a\in A} \operatorname{ord}_a(f)a = \frac{1}{2\pi i}\int_{\partial A} zf'/f = n\omega_2 + n'\omega_1 \in \Lambda,$$

since $n, n' \in \mathbb{Z}$. ❑

[3] The integer n is the winding number of the closed curve $f(\sigma_1)$ around the origin

3.3 Weierstrass $\wp$ - function

As we mentioned, there is a special function attached to every lattice. In some sense it is the simplest non-constant meromorphic doubly periodic function with period lattice the given lattice Λ. We saw that a non-constant function with period lattice Λ has at least two poles, and the Weierstrass $\wp$-function will be a function with double poles at the lattice points having residue zero at the poles. It goes without mentioning that it be double periodic with the given lattice Λ as period lattice.

We start out with a criterion for convergence of sums over lattices that will be useful

Lemma 3.2 *If Λ is a lattice and $s > 2$, then the series $\sum_{\omega\in\Lambda\setminus\{0\}} \omega^{-s}$ is absolute convergent.*

Proof: The starting point is a reduction to the case when the lattice is the Gaussian lattice $G = \{\, (n,m) \mid n, m \in \mathbb{Z}\,\}$. Let A be the 2×2-matrix with columns $(\operatorname{Re}\omega_i, \operatorname{Im}\omega_i)^t$ for $i = 1, 2$. It is invertible, and since the unit circle $\mathbb{S}^1 \subseteq \mathbb{R}^2 = \mathbb{C}$ is compact and $Av \neq 0$ for all non-zero v's, we know that $|Av|$ attains a non-zero minimum, say M, for $v \in \mathbb{S}^1$. Then $M\,|v| \leq |Av|$ for all v, and we arrive at the inequality

$$\sum_{\omega\in\Lambda} |\omega|^{-s} = \sum_{v\in G} |Av|^{-s} \leq M^{-s} \sum_{v\in G} |v|^{-s},$$

so once we have proven the last sum being finite, we are through.

For the Gaussian lattice, let Q_ν be the set of lattice points (n,m) with $\max\{|n|, |m|\} = \nu$. There are 8ν points in Q_ν, and their distances to the origin are all greater than ν. Hence

$$\sum_{\omega\in G} |\omega|^{-s} \leq 8 \sum_{\nu} \nu \cdot \nu^{-s} = 8 \sum_{\nu} \nu^{-(s-1)}$$

where the last series converges since $s - 1 > 1$.

❏

One should be careful working with functions like z^s when z complex since the logarithm is not well defined. We shall stick wiyh s being an integer. For any integer n with $n > 2$ the series $\sum_{\omega\in\Lambda'} \omega^{-n}$, where $\Lambda' = \Lambda \setminus \{0\}$, is called an *Eisenstein series*. It is absolute convergent, and the standard notation is

$$G_n(\Lambda) = \sum_{\omega\in\Lambda'} \omega^{-n}. \tag{3.1}$$

Eisenstein

If n is odd one has $G_n(\Lambda) = 0$, since

$$\sum_{\omega\in\Lambda'}\omega^{-2k-1}=\sum_{\omega\in\Lambda'}\omega^{-2k-1}=1/2\sum_{\omega\in\Lambda'}\left(\omega^{-2k-1}+(-\omega)^{-2k-1}\right)=0.$$

Problem 3.3. If c is non-zero complex number, $c\Lambda$ denotes the lattice $c\Lambda=\{\, c\omega \mid \omega\in\Lambda\,\}$. Show that $G_{2k}(c\Lambda)=c^{-2k}G_{2k}(\Lambda)$. ✱

One standard way to obtain functions invariant under a group is to take averages over the group elements. If the group G acts on X, and $f(x)$ is a function on X, then $g(x)=\sum_{g\in G}f(gx)$ is invariant. This works perfectly well when G is finite, but in the infinite case, one must give a meaning to the infinite sum. For us, a tempting way to construct Λ-periodic functions, or functions invaraint under the action of Λ by translation, is to use sums of the form

$$g(z)=\sum_{\omega\in\Lambda}(z-\omega)^{-s},$$

where $z\notin\Lambda$, and where s is a natural number. Of course, we must be sure that the series converges, that is $s\geq 3$. If ω_0 is any lattice point $\omega+\omega_0$ runs through Λ when ω does, so as long as the series converges absolutely and one freely can rearrange the terms, the series defines indeed a Λ-periodic function:

$$g(z)=\sum_{\omega\in\Lambda}(z-\omega)^{-s}=\sum_{\omega\in\Lambda}(z-\omega-\omega_0)^{-s}=\sum_{\omega\in\Lambda}((z+\omega_0)-\omega)^{-s}=g(z+\omega_0).$$

In view of this anf the next proposition, the function

$$g(z)=\sum_{\omega\in\Lambda}(z-\omega)^{-3} \qquad (✯)$$

is a Λ-periodic meromorphic function whose only singularities are triple poles at the period points. The function g is—as we subsequently shall see—up to the factor -2 the *derivative* of the $\wp$-function, and it easier to construct than the $\wp$-function it self. Subsequently we find the $\wp$-function by term-wise integration. PDerivert1

Proposition 3.6 *Let $\Lambda'\subseteq\Lambda$ be a subset. If $s>2$, then the sum $\sum_{\omega\in\Lambda'}(z-\omega)^{-s}$ converges absolutely if $z\notin\Lambda'$ and uniformly on any compact subset U disjoint from Λ'.* NormKonv

Before giving the proof let us see that the statement about the function $g(z)$ in (✯) above follows. The series for the function $g(z)$ converges uniformly on small compact neigbourhoods of points not in Λ, so $g(z)$ is holomorphic off Λ. For $\omega_0\in\Lambda$ let $\Lambda'=\Lambda\setminus\{\omega_0\}$. Then $g(z)=(z-\omega_0)^{-3}+\sum_{\omega\in\Lambda'}(z-\omega)^{-3}$ where the series converges absolutely and uniformly on compact neighbourhoods of ω_0 not meeting Λ', and therefore it is holomorphic around ω_0. This shows that $g(z)$ has a pole at ω_0 with principal part $(z-\omega_0)^{-3}$.

Proof of Proposition 3.6: Only finitely many ω in Λ' satisfy $|z/\omega - 1| \leq 3/2$ for $z \in U$. For those finitely many ω's, the functions $|z/\omega - 1|$ have a common non-zero lower bound when z belongs to the compact set U, say ϵ. Then $\epsilon\,|\omega| \leq |z-\omega|$ for all $z \in U$ and $\omega \in \Lambda'$ (we clearly can require that $\epsilon < 3/2$), and it holds true that

$$\sum_{\omega\in\Lambda'} |z-\omega|^{-s} \leq \epsilon^{-1} \sum_{\omega} |\omega|^{-s},$$

showing that the series converges absolutely. Uniform convergence follow from Weierstrass' M-test. ❑

Now we move on to the construction of the $\wp$-function. Recall that we are looking for the simples possible non-constant Λ-periodic function. All holomorphic functions are constant and there no meromorphic doubly periodic one with just one pole in a fundamental domain. Our function thus must have two poles, and place both at the lattice points, that is we are looking for a function having double poles at the lattice points and, to keep it simple, with residue zero.

The series $\sum_\omega (z-\omega)^{-2}$ would be a good try, but it does not converge. However the series

$$\wp(z) = z^{-2} + \sum_{\omega\in\Lambda'} \left((z-\omega)^{-2} - \omega^{-2}\right) \qquad (✦)$$

WeierP

where we have written Λ' for $\Lambda \setminus \{0\}$, will work. Except for the z^{-2} term this series is obtained by termwise integration of the function $g(z)$ from (✯) (or more precisely $-2g(z)$) between 0 and z. It remains to be seen that series converges absolutely and uniformly on compact subsets disjoint from Λ, and to that end we establish the following estimate:

$$\left|(z-\omega)^{-2} - \omega^{-2}\right| = |z|\,|2\omega - z|\,|\omega|^{-2}\,|z-\omega|^{-2} \leq A\,|z|\,|\omega|^{-3}$$

where A is a constant only depending on the compact set U (and of course on the lattice Λ). Indeed, just as in the proof of proposition 3.6 there is an $\epsilon > 0$ such that $|z-\omega| \geq \epsilon\,|\omega|$ for $z \in U$. Now $w = \min\{\,|\omega| \mid \omega \in \Lambda'\,\} > 0$, and letting $Z = \sup\{\,|z| \mid z \in U\,\}$, one finds $|2\omega - z| < (2 + Z/w)\,|\omega|$. Then put $A = \epsilon^{-1}(2 + Z/w)$.

Proposition 3.7 *The Weierstarss $\wp$-function associated to the lattice Λ has the following three properties*

- □ *It is even, i.e., $\wp(-z) = \wp(z)$*
- □ *It is Λ-periodic,i.e., $\wp(z+\omega) = \wp(z)$ for $\omega \in \Lambda$ and $z \in \mathbb{C}$.*
- □ *It has as its only singularities double poles with residue zero at the lattice points.*

Proof: We already saw the last property. Since $-\omega$ runs through Λ' when ω does, and since the series (✦) defining $\wp(z)$ converges absolutely, we can rearrange the terms, and hence arrive at

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

We checked that the derivative $\wp'(z)$ is periodic, from which follows that $\wp(z)$ is periodic. Indeed, take thing derivative of $\wp(z+\omega) - \wp(z)$ we find

$$\wp'(z+\omega) - \wp'(z) = 0$$

since $\wp'(z)$ is periodic, Therefore $\wp(z+\omega) - \wp(z)$ is constant. Putting $z = -\omega/2$ and using that $\wp(z)$ is an even function, one concludes that $\wp(z)$ is periodic. ❏

Problem 3.4. Show that the series

$$\zeta(z) = z^{-1} + \sum_{\omega\in\Lambda'} \left((z-\omega)^{-1} + \omega^{-1} + z\omega^{-2}\right)$$

converges absolute and uniformly on compact sets disjoint from Λ. Show that $\zeta(z)$ has simple poles at the lattice points as its only singularities and that $\zeta'(z) = -\wp(z)$. Show that $\zeta(z+\omega) - \zeta(z) = \eta(\omega)$ where $\eta(\omega)$ is a nontrivial additive function on Λ. ✱

3.3.1 The Weierstrass equation

Recall that on an elliptic curve E with equation $y^2 = x^3 + ax + b$ the y coordinate has a pole at ∞ of other three and the x-coordinate one of order 2. This behavior resemles the behavior of the functions $\wp(z)$ and $\wp'(z)$, and indeed, they satisfy a differential equation analogous to Weierstarss equation:

WeierDiffProp

Proposition 3.8 *The Weierstrass function $\wp(z)$ satisfies an equation*

$$\wp'(z)^2 = \wp(z)^3 - g_4\wp(z) - g_6. \tag{3.2}$$

WeierDiff

The coefficients g_2 and g_4 are given as $g_4 = 60G_4(\Lambda)$ and $g_6 = 140G_6(\Lambda)$ where $G_k(\Lambda)$ are the Eisenstein series as defined in (3.1) on page 8.

This shows that the assignments $x(z) = \wp(z)$ and $y(z) = \wp'(z)$ give a parametrization of the elliptic curve in $\mathbb{C}^2$ given by the equation 3.2; well, for the moment we can only say that the map $\mathbb{C} \to \mathbb{C}^2$ given by $z \mapsto (\wp(z), \wp'(z))$ takes values in the elliptic curve E whose equation is 3.2. In the end, the map induces an analytic isomorphism between $\mathbb{C}/\Lambda$ and the projective curve E, lattice points being mapped to $(0;1;0)$, but we are not there yet. One should also add that the group structures —the geometric one on the elliptic curve and the additive quotient structure on $\mathbb{C}/\Lambda$—coincide (of course!).

Proof: The starting-point of the proof is the Laurent developments of $\wp(z)$ and $\wp'(z)$ around 0. To obtain the one of $\wp(z)$ one uses the good old classic

$$\frac{1}{(1-t)^2} = \sum_{n\geq 0}(n+1)t^n$$

from which we deduce

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

Summing up over the lattice one arrives at

$$\wp(z) = \frac{1}{z^2}+\sum_{\omega\in\Lambda'}\sum_{n\geq 0}\frac{(n+1)z^n}{\omega^{n+2}} = \frac{1}{z^2}+\sum_{n\geq 0}(n+1)z^n\sum_{\omega\in\Lambda'}\frac{1}{\omega^{n+2}} = \frac{1}{z^2}+\sum_{n\geq 0}G_{n+2}(\Lambda)(n+1)z^n.$$

Writing out the few first remembering that the odd Eistenstein series vanish, one finds

$$\wp(z) = z^{-2} + 3G_4(\Lambda)z^2 + 5G_6(\Lambda)z^4 + \dots. \tag{3.3}$$

LaurentP Taking the derivative we get

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

LaurentPder With these formulas it is a matter of simple book-keeping to see that the function

$$\wp'(z)^2 - 4\wp(z)^3 + 60G_4(\Lambda)\wp(z) + 140G_6(\Lambda)$$

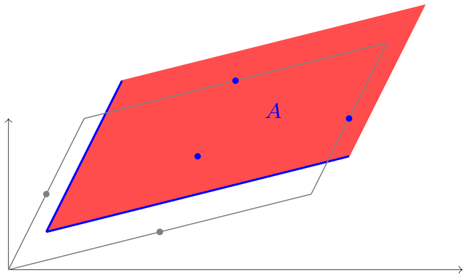
has no principal part at 0. Being Λ-periodic it has no poles at any lattice point, and hence it is holomorphic in the whole plane. By Liouville's theorem, it must be constant. The same book-keeping procedure shows that the value at the origin is 0, so the function vanishes identically, and we are done. ❏

Problem 3.5. Do the computation and verify the statement about the principal part above. ✸

The half periods The points $\omega/2$ where $\omega \in \Lambda$ are called *the half periods* and they play a special role. In every fundamental domain, not having lattice points on the boundary, there are exactly three half periods. Their images in the quotient $\mathbb{C}/\Lambda$ are the two-torsion points. We therefore suspect their y-coordinates, that is $\wp'(z)$, to vanish; and of course, this holds true. The point is that $\wp'(z)$ is an odd function (as the derivative of an even one). Hence we have, since $\wp'(z)$ is doubly periodic as well:

$$-\wp'(\omega/2) = \wp'(-\omega/2) = \wp'(\omega-\omega/2) = \wp'(\omega/2).$$

The half periods are the only zeros of $\wp'(z)$. In an appropriate fundamental domain A the derivative $\wp'(z)$ has as only singularity a pole of order three, and because the number zeros in A is the same as the number of poles by proposition 3.2 on page 5, $\wp'(z)$ can only have three zeros. These zeros must for the same reason be simple, so the double derivative $\wp''(z)$ never vanishes in a half period.



The half periods in a fundamental domain A.

The value of $\wp(z)$ at a half period is a root of the polynomial $4x^3 - g_4x - g_6$; indeed

$$0 = \wp'(\omega/2)^2 = \wp(\omega/2)^3 - g_4\wp(\omega/2) - g_6.$$

Assume that ω_1, ω_2 is a basis for the lattice Λ. Then the values of $\wp(z)$ at the three half period $\omega_1/2$, $\omega_2/2$ and $(\omega_1+\omega_2)/2$ are different. Indeed, the function $\wp(z)-\wp(\omega_1/2)$ vanishes doubly at $\omega_1/2$ since the derivative vanises there, but like any doubly periodic function, it has as many zeos as poles in a fundamental domain A, so it can not vanish elsewhere in A. We have established:

HalfPeriods

Proposition 3.9 *Let ω_1 and ω_2 form a basis for the lattice Λ.*

- □ *The half periods $\omega/2$ are the only zeros of $\wp'(z)$, and $\wp'(z)$ vanishes simply there, that is $\wp''(\omega/2) \neq 0$.*
- □ *The values $\wp(\omega_1/2)$, $\wp(\omega_2/2)$ and $\wp((\omega_1+\omega_2)/2)$ of $\wp(z)$ at the half periods are different, and they are the three roots of the polynomial $4x^3 - g_4x - g_6$.*

As remark, we observe that this implies that the discriminant $27g_6^2 - 4g_4^3$ is non-zero and that the curve given by (✦) below is nonsingular.

3.3.2 The isomorphism

In this section we prove that for any lattice Λ the quotient $\mathbb{C}/\Lambda$ is analytically isomorphic to an elliptic curve over $\mathbb{C}$ as we defined it early, that is a nonsingular, cubic curve with point singled out. The elliptic curve $E(\Lambda)$, or just E for short, will be given by the Weierstrass equation

$$y^2 = 4x^3 - g_4x - g_6 \qquad (✦)$$

where the g_i's are the modified Eisenstein series as defined just after proposition 3.8 on page 11, and of course the specified point is as usual the point $(0;1;0)$ at infinity. It will correspond to the origin in $\mathbb{C}/\Lambda$ (that is, the equivalence class consisting of lattice points). WeierHer

The isomorphism rely heavily on the Weierstrass $\wp$-function, which together with its derivative defines a map $\phi\colon \mathbb{C}/\Lambda \to E$ by the assignment $z \mapsto (\wp(z); \wp'(z); 1)$. This expression is valid in $\mathbb{C} \setminus \Lambda$ where both functions $\wp(z)$ and $\wp'(z)$ are holomorphic, and around the lattice points the map ϕ is given as $(\wp(z)/\wp'(z); 1; 1/\wp'(z))$. Clearly ϕ is an analytic map (meaning just that the coordinate functions in affine coordinates are analytic) off the lattice, and as $\wp'(z)$ has a pole at the lattice points, its inverse $1/\wp'(z)$ is holomorphic in a vicinity of any such. Similarly as $\mathrm{ord}_\omega(\wp(z)) - \mathrm{ord}_\omega(\wp'(z)) = -2-(-3) = 1$ for any $\omega \in \Lambda$, the quotient $\wp(z)/\wp'(z)$ is holomorphic at ω—in fact it has a simple zero there.

In proposition 3.8 we established the differential equation

$$\wp'(z)^2 = 4\wp(z)^3 - g_4\wp(z) - g_6, \qquad (✡)$$

www so our map ϕ takes values in $E(\Lambda)$. We shall show

TheIsomorphism **Proposition 3.10** *The map $\phi\colon z \to (\wp(z); \wp'(z); 1)$ induces an analytic group homomorphism $\phi\colon \mathbb{C}/\Lambda \to E$.*

Before making our way into the proof we restate some of the properties of the $\wp$-function as a lemma:

Lemma 3.3 *The map $\wp\colon \mathbb{C}/\Lambda \to \mathbb{P}^1(\mathbb{C})$ given by $z \mapsto (\wp(z); 1)$ is a surjective two-to-one map whose only ramification points are the half periods.*

Proof: The map is surjective by proposition 3.4 on page 7. And having a double poles at the lattice points as sole singularities, it is two-to-one by the discussion preceeding that proposition. The ramification points are the points where the derivative $\wp'(z)$ vanishes, and by proposition 3.9 on page 13 this happens only in the half periods. ❏

Proof: First of all, on $\mathbb{C}/\Lambda$ and E we have the natural involutions ι and ι', that respectively are given by $\iota(z) = -z$ and $\iota'(x; y; 1) = (x; -y; 1)$. Since $\wp(z)$ is an even function and $\wp'(z)$ an odd one, the map ϕ is compatible with the involutions, that is, $\iota' \circ \phi = \phi \circ \iota$.

Secondly, let X denotes the function that gives the x-coordinate of a point in E. Then $X \circ \phi = \wp$, as illustrated in the the commutative diagram below:

$$\begin{tikzcd}
\mathbb{C}/\Lambda \arrow[rr, "\phi"] \arrow[dr, "\wp"'] & & E(\Lambda) \arrow[dl, "X"] \\
& \mathbb{P}^1(\mathbb{C}) &
\end{tikzcd}$$

Both maps are surjective and two-to-one, and both commute with the corresponding involution (if $(y; x; 1)$ lies on E, then $(-y; x; 1)$ does as well, and $\wp(-z) = \wp(z)$)

Outside the ramification loci, the fibers of the two maps consist of two distinct points exchanged by the corresponding involutions. And the maps ramify at corresponding points, indeed, the Weierstrass map $\wp$ ramifies at the points where $-z = z$ (mod the lattice), that is at the half periods, and the x-coordinate map ramifies at the points where $y = 0$, that is over the roots of $4x^3 - g_4x - g_6$. In proposition 3.9 on page 13 we showed that these roots were exactly the values of $\wp$ at the half periods. This shows that ϕ is bijective.

To finish off the proof that ϕ is an isomorphism, it suffices (By the analytic implicit function theorem) to show that ϕ is immersion into $\mathbb{P}^2(\mathbb{C})$, *i.e.,* that its derivative is injective everywhere. But the derivative of ϕ at the point z is the linear map $\mathbb{C} \to \mathbb{C}^2$ sending ξ to $(\wp'(z)\xi, \wp''(z)\xi)$. Off the two-torsion points $\wp'(z)$ does not vanish, and at a two torsion point $\wp''(z)$ does not vanish; hence the derivative is injective. That ϕ is a group homomorphism will br done in the next paragraph. ❑

3.3.3 The addition formula

When working with the group structure of an elliptic curve $E \subseteq \mathbb{P}^2(k)$ on Weierstrass form, we proved (proposition 1.6 on page 13 in part 1 with $a_1 = 0$) the following formula for the x-coordinate of the sum of two points (x_1, y_1) and (x_2, y_2), valid whenever $x_1 \neq x_2$:

$$x = \Big(\frac{y_2 - y_1}{x_2 - x_1}\Big)^2 - x_1 - x_2.$$

Translated into the language of Weierstrass functions this formula appears as in equation (3.4) below (the factor $1/4$ in that equation comes from the factor 4 in the leading term of the equation satisfied by $\wp(z)$), and once this is established, we have proved that ϕ is a group homomorphism. That said, there are several other ways to see this. May be the most natural one follows from the fact that all regular maps between complete curves with a regular group structure (or more generally, between any abelian varities) are homomorphism once they respect the origins.

Proposition 3.11 *Whenever $z \neq z'$ one has:*

$$\wp(z + z') = \frac{1}{4}\Big(\frac{\wp'(z) - \wp'(z')}{\wp(z) - \wp(z')}\Big)^2 - \wp(z) - \wp(z') \tag{3.4}$$

Additionformula

PROOF: We fix z' and regard z as the variable. The strategy of the proof is to verify that the two sides have the same principal part everywhere except for a possible discrepance in the residue at one point at most (in a fundamental domain A). The difference of the two sides is then a function having at worst one simple pole in the fundament domain A, and therefore it must be constant (Liouville's third, proposition 3.3 on page 6). It remains to verify that the two sides coincide at one point.

The left side of (3.4) has a pole for $z = -z'$, and the possible pole of the right side are $z = 0$ and $z = \pm z'$. We analyze each case separately. We Assume that z' is not a half period, leaving that case as an exercise.

The case $z = 0$. In the fraction

$$\frac{\wp'(z) - \wp'(z')}{\wp(z) - \wp(z')} \tag{✣}$$

The Fraction

the enumerator has a pole of order three and the denominator one of order two, so the fraction has simple pole. One computes the residue:

$$\lim_{z\to 0} z\frac{\wp'(z) - \wp'(z')}{\wp(z) - \wp(z')} = \lim_{z\to 0} \frac{z^3(\wp'(z) - \wp'(z'))}{z^2(\wp(z) - \wp(z'))} = -2.$$

The dominant term of the Laurent series of one fouth of the square is then $1/z^2$, which is the same as the one of $\wp(z)$. Hence the right side has at most a simple pole at 0.

The case $z = z'$: By l'Hopital's rule, the fraction (✣) has the value $\wp''(z')/\wp'(z')$ and there is no poles as long as z' is not half period since then $\wp'(z') \neq 0$.

The case $z = -z'$: Then the fraction(✣) ha a simple pole with residue -2, and the principal part of its square equals $1/z + z'$. The left side has a double pole with the same principal part (substitute $z + z'$ in the Laurent series for $\wp(z)$ round the origin). ❏

PROBLEM 3.6. Complete the proof by checking the formula for z' one of the half periods. ✷

3.4 Mappings between elliptic curves

In any mathematical theory the relations between the objects one studies are as important than the objects themselves. Usually the relations appears as maps respecting the structure of the objects. This has been formalized in theory of *categories*, where "maps" usually are called morphisms.

Elliptic curves posses two structures. They are varieties as well as groups. So our morphisms should respect both these structures, they should group homomorphisms as well as regular. It is common to call such maps *isogenies*. Now, it happens that a regular map between two elliptic curves respecting the neutral elements automatically is a group homomorphism! Even if this might appear as a miracle, it is not very deep (certainly not for curves over ℂ), and we shall soon prove it.

However we start with some examples, which in the end are not merely examples but the generic situation.

3.4.1 Examples

Let Λ' and Λ be two lattices, and let $a \in \mathbb{C}$ be a complex number such that $a\Lambda \subseteq \Lambda'$. Then the map $z \mapsto az$ is an additive map that takes Λ' into Λ, and by elementary group theory it induces a group homomorphism $\phi_a \colon \mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda$. This map will also be regular, indeed, it follows since $z \mapsto az$ is analytic, and the quotient maps are locally analytic isomorphisms. The situation is summed up by the usual commutative diagram

$$\begin{tikzcd} \mathbb{C} \arrow[r, "\iota_a"] \arrow[d] & \mathbb{C} \arrow[d] \\ \mathbb{C}/\Lambda' \arrow[r, "\phi_a"] & \mathbb{C}/\Lambda \end{tikzcd}$$

where we temporarily have denoted $z \mapsto az$ by ι_a. The kernel of ϕ_a is isomorphic to $\Lambda/a\Lambda$, so there is the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \Lambda/a\Lambda \arrow[r] & \mathbb{C}/\Lambda' \arrow[r] & \mathbb{C}/\Lambda \arrow[r] & 0 \end{tikzcd}$$

Indeed, the kernel clearly is equal to $a^{-1}\Lambda/\Lambda'$, but this quotient is isomorphic to $\Lambda/a\Lambda$ via the multiplication-by-a map.

The quotient between to finitely generated free abelian groups of the same rank is always finite; slightly more general, the cokernel of an injective map between two such groups is finite. In order to see this, we choose basises for the two groups and represents the map by a matrix M with integral coefficients. Since the two groups are of the same rank, the matrix is a square matrix and since the map is injective, M has a non-zero determinant. Now the if M^c is the cofactor matrix of M, one has the identity

$$det M \cdot I = MM^c$$

hence $\det M \cdot x = MM^c x \in \operatorname{Im} M$ for any element x, so the integer $\det M$ kills the cokernel, and consequently the cokernel is finite. We have proved

Proposition 3.12 *Let Λ' and Λ be two lattices and let $a \in \mathbb{C}$ be a complex number such that $a\Lambda \subseteq \Lambda$. Then multiplication-by-a map $z \mapsto az$ induces a regular group homomorphism $\phi_a \colon \mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda$ whose kernel is finite and isomorphic to $\Lambda/a\Lambda$.*

This proposition merits a few comments. Firstly, as we soon shall see, it covers every regular group homomorphisms. They are all induced by multiplication by some complex number, see proposition 3.13 on page 19 below. Secondly, ϕ_a is an isomorphism if and only if $a\Lambda = \Lambda$. Thirdly, the case $a = 1$ is a highly nontrivial and interesting case. The condition on the lattices is then that $\Lambda' \subseteq \Lambda$, and up to isomorphisms, the isogneis with a given curve $\mathbb{C}/\Lambda$ as target are classified by the sublattices of Λ:

EXAMPLE 3.1. Assume that Λ' is a sublattice of Λ. Then the identity map on $\mathbb{C}$ induces an isogeny

$$\phi_{\Lambda/\Lambda'} \colon \mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda.$$

This is nothing but the good old group homomorphism sendig a translation class mod Λ' to the one mod Λ. The kernel of $\phi_{\Lambda/\Lambda'}$ is the quotient Λ/Λ' between the two lattices, and there is an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \Lambda/\Lambda' \arrow[r] & \mathbb{C}/\Lambda' \arrow[r, "\phi_{\Lambda/\Lambda'}"] & \mathbb{C}/\Lambda \arrow[r] & 0. \end{tikzcd}$$

The quotient Λ'/Λ is finite, and the degree of $\phi_{\Lambda/\Lambda'}$ is the index of Λ' in Λ, *i.e.*, $\deg \phi_{\Lambda/\Lambda'} = [\Lambda : \Lambda']$, since the degree is the number of elements in the fibres. ❄

Example 3.2. Let $n \in \mathbb{N}$ be a natural number. A lattice Λ gives rise to the two lattices by $n\Lambda = \{\, n\omega \mid \omega \in \Lambda \,\}$ and $1/n\Lambda = \{\, \omega/n \mid \omega \in \Lambda \,\}$. The curve $\mathbb{C}/\Lambda$ is isomorphic to both $\mathbb{C}/n\Lambda_n$ and $\mathbb{C}/1/n\Lambda$. An isomorphism with $\mathbb{C}/\Lambda$ as source being induced by multiplication by n respectively $1/n$. ❄

Example 3.3. Let $n \in \mathbb{N}$ be a natural number. The multiplication-by-n-map $z \mapsto nz$ takes any lattice Λ into itself and hence induces a map $[n]\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$, which is nothing but multiplication by n on the elliptic curve $\mathbb{C}/\Lambda$, a map we already have encountered. The quotient $\Lambda/n\Lambda$, being isomorphic to the cokernel of the map $\mathbb{Z}^2 \to \mathbb{Z}^2$ sending x to nx, is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$. So we have the exact sequence

$$\begin{tikzcd}
0 \arrow[r] & (\mathbb{Z}/n\mathbb{Z})^2 \arrow[r] & \mathbb{C}/\Lambda \arrow[r, "{[n]}"] & \mathbb{C}/\Lambda \arrow[r] & 0
\end{tikzcd}$$

and $[n]$ is of degree n^2.

The two pairs of sublattices $n\Lambda \subseteq \Lambda$ and $\Lambda \subseteq n^{-1}\Lambda$ both realises $[n]$ up to isomorphism. The meaning of this sentce is that there are the two commutative diagrams with exact rows, the first one being

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ker}[n] \arrow[r] \arrow[d, "\simeq"'] & \mathbb{C}/\Lambda \arrow[r, "{[n]}"] \arrow[d, "n"] & C/\Lambda \arrow[r] \arrow[d, "="'] & 0 \\
0 \arrow[r] & \Lambda/n\Lambda \arrow[r] & \mathbb{C}/n\Lambda \arrow[r, "\phi"] & C/\Lambda \arrow[r] & 0
\end{tikzcd}$$

where n and ϕ are shorthand notation for the maps ϕ_n and $\phi_{n\Lambda/\Lambda}$ as defined above. The second diagram is the following with a similar shorthand notation:

$$\begin{tikzcd}
0 \arrow[r] & n^{-1}\Lambda/\Lambda \arrow[r] \arrow[d, "\simeq"'] & \mathbb{C}/n^{-1}\Lambda \arrow[r, "\phi"] \arrow[d, "n"] & C/\Lambda \arrow[r] \arrow[d, "="'] & 0 \\
0 \arrow[r] & \mathrm{Ker}[n] \arrow[r] & \mathbb{C}/\Lambda \arrow[r, "{[n]}"] & C/\Lambda \arrow[r] & 0
\end{tikzcd}$$

❄

Example 3.4. Let $G = \mathbb{Z}[i]$ be the Gaussian lattice generated by 1 and i. Then multiplication by i takes G into G, and hence induces an automorphism of $\mathbb{C}/G$ denoted by $[i]$ satisfying $[i]^2 = [-1]$. Such an isomorphism is called a *complex multiplication*, and are pretty rear. Another example is the *Eisenstein lattice* $H = \mathbb{Z}[\rho]$ where $\rho = \exp 2\pi i/3$. Multiplication by ρ induces an automorphism $\mathbb{C}/H$ (one has $\rho^2 = -\rho - 1$). ❄

Problem 3.7. Show that the lattice $1, \alpha$ has complex multiplication if and only if α is quadratic over $\mathbb{Q}$. ✱

Example 3.5. Assume that $G \subseteq \mathbb{C}/\Lambda$ is a finite subgroup. Thw $\Lambda_G = \{\, z \in \mathbb{C} \mid \pi z \in G \,\}$ is discrete subgroup of $\mathbb{C}$, hence a lattice. ❄

Given any pair of lattices one contained in the other, say $\Lambda' \subseteq \Lambda$. As the quotient Λ/Λ' is a finite group, it is killed by som integer n. This means that $n\Lambda \subseteq \Lambda'$. The two isogenies

$$\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$$
$$\mathbb{C}/\Lambda' \to \mathbb{C}/n\Lambda$$

have as composition $[n]$.

3.4.2 Every map is linear

Recall that any $\mathbb{C}$-linear map $\mathbb{C} \to \mathbb{C}$ is of the form $az + b$. In the previous section we saw that the homotethy $z \mapsto az$ induces isogenies of elliptic curves. In a similar way the translations $z \mapsto z+b$ induces a regular map , denoted by T_b, of every elliptic curve $\mathbb{C}/\Lambda$, sending the translation class of z to the one of $z + b$. This map is however no more an isogeny since it does preserve the origin, but $T_b(0) = b$. The aim of this section is to show that any regular map between to complex elliptic curves is the composition of a translation map and multiplication map:

Proposition 3.13 *Let $\phi\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ be a non-constant regular map.* EveryMapIsLinea

- □ *If ϕ is an isogeny, that is $\phi(0) = 0$, then ϕ is a group homomorphdism.*

- □ *For a general ϕ, there is a translation map $T\colon \mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda'$ and an isogeny $\phi_0\colon \mathbb{C}/\Lambda \to \mathbb{C}/L'$ such that $\phi = T\phi_0$*

PROOF: The proof consists in finding a linear map $\phi_0\colon \mathbb{C} \to \mathbb{C}$, that is a map with $\phi_0(z) = az + b$ for constants $a, b \in \mathbb{C}$, that fits into the commutative diagram

$$\begin{tikzcd}
\mathbb{C} \arrow[r, "\phi_0"] \arrow[d, "\pi"'] & \mathbb{C} \arrow[d, "\pi'"] \\
\mathbb{C}/\Lambda \arrow[r, "\phi"'] & \mathbb{C}/\Lambda'
\end{tikzcd}$$

where the two vertical arrows represent the quotient maps sending a complex number to its translation class.

If $\phi(0) = 0$, clearly $b = 0$, and ϕ_0 is additive. This immediate implies that ϕ is additive and hence a group homomorphism. The second item follows once we have proven the first; just use the translation $T_{-\phi(0)}$.

In the attack on the first item we need a fact from topology. The quotient map $\pi\colon \mathbb{C} \to \mathbb{C}/\Lambda$ is the universal covering map of the elliptic curve $\mathbb{C}/\Lambda$. It has the property that any continuous map $\psi\colon X \to \mathbb{C}/\Lambda$ where X is a simply connected topological space, lifts to $\mathbb{C}$; that is, there is a continuous map $\psi_0\colon X \to \mathbb{C}$ such that $\psi = \pi\psi_0$, or as one says, the following diagram commutes

$$\begin{tikzcd} X \arrow[r, "\psi_0"] \arrow[dr, "\psi"'] & \mathbb{C} \arrow[d] \\ & \mathbb{C}/\Lambda \end{tikzcd}$$

If now $X = \mathbb{C}$ and ψ is holomorphic, as will be the case in our application, the lifting ψ_0 will be holomorphic as well. This is more or less the definition of the complex structure on $\mathbb{C}/\Lambda$, and we leave it as an exercise.

So given a regular map $\phi\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$. In particular it is continuous, and one may fill in the diagram below by a continuous map ϕ_0 making it commutative (take $\psi = \phi\pi$), and after the comment above ϕ_0 is holomorphic.

$$\begin{tikzcd} \mathbb{C} \arrow[r, "\phi_0"] \arrow[d, "\pi"'] & \mathbb{C} \arrow[d, "\pi'"] \\ \mathbb{C}/\Lambda \arrow[r, "\phi"'] & \mathbb{C}/\Lambda'. \end{tikzcd}$$

Now pick any lattice element ω from Λ. Clearly the difference $\psi_0(z+\omega)-\psi_0(z)$ belongs to the lattice Λ' since both terms map to $\psi(\pi'(z))$ in $\mathbb{C}/\Lambda'$, and of course, the difference depends on z in a continuous way. So the difference is a continuous map from the connected space $\mathbb{C}$ to the discrete space Λ' and must be constant. By taking derivatives, we conclude that $\psi_0'(z)$ is Λ-periodic. Being holomorphic everywhere it is therefore constant after Liouville I. Thus $\psi_0'(z) = a$ for some a, and integrating we conclude that $\psi_0(z) = az + b$, which is exactly what we were aiming at. ❏

3.4.3 First attempt of moduli-space

One wants to classify the isomorphism classes of the elliptic curves over $\mathbb{C}$. They are all of the form $\mathbb{C}/\Lambda$ for a lattice Λ, but of course several different lattices give birth to isomorphic curves. If $\mathscr{E}$ denotes the set of isomorphism classes of elliptic curves over $\mathbb{C}$ and $\mathscr{L}$ the set of lattices, we have the map

$$\mathscr{L} \to \mathscr{E} \tag{✢}$$

ModuliMap sending a lattice Λ to the curve $\mathbb{C}/\Lambda$. It is surjective but far from injective.

To cope with this problem, one tries to normalize the lattices, that is, imposing conditions on them and thus cutting down the set $\mathscr{L}$. For example, one can demand that $1 \in \Lambda$ and even that 1 is a *primitive* element; meaning that it is not divisible (*i.e.,* that $n^{-1} \notin \Lambda$ for any natural number $n > 2$). This equivalent to Λ having a basis of the form $1, \tau$, and one can further normalize and impose the condition $\operatorname{Im}\tau > 0$. The last condition says that τ belongs to the *upper half plane* $\mathbb{H}$.

We introduce the notation Λ_t for the lattice generated by $1, \tau$ where $\tau \in \mathbb{H}$. The map in ✢ may now be replaced by

$$\mathbb{H} \to \mathscr{E}$$

that sends τ to $\mathbb{C}/\Lambda_\tau$. Still the map is not injective since but there is a good condition for Λ_τ and $\Lambda_{\tau'}$ to define isomorphic elliptic curves:

Lemma 3.4 *For τ and τ' numbers in the upper half plane $\mathbb{H}$, the two elliptic curves $\mathbb{C}/\Lambda_\tau$ and $\mathbb{C}/\Lambda_{\tau'}$ are isomorphic if and only if there are integers a, b, c and d with $ad - bc = 1$ such that*

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

Looking at the matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

the condition on the coefficients is that $\det A = 1$, equivalently it belongs to the group $\mathrm{Sl}(2\,)\mathbb{Z}$.

PROOF: By proposition 3.13 there is a complex number α with the property that $\alpha\Lambda_{\tau'} = \Lambda_\tau$. Hence we may write

$$\begin{aligned} \alpha\tau' =& a\tau + b \\ \alpha =& c\tau + d \end{aligned}$$

where $a, b, c, d \in \mathbb{Z}$. So matrix A is just matrix of the $\mathbb{Z}$-linear map α between the two free abelian groups Λ_τ and $\Lambda_{\tau'}$ with respect to the two basises $1, \tau$ and $1, \tau'$.

This gives

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

Since the map α is invertible (an inverse being multiplication by α^{-1}), its matrix is invertible and so $\det A = 1$.

❏

The group $\mathrm{Sl}(2, \mathbb{Z}\,)$ acts on $\mathbb{H}$ by the rule

$$A\tau = \frac{a\tau + b}{c\tau + d}$$

Some work is required in order to see that this is an action; *i.e.,* that $A(Bz) = (AB)z$ but it just a matter of trivial computations. And what we just proved amounts to the statement that the set $\mathscr{E}$ of complex elliptic curves is bijective to the quotient of the upper half plane $\mathbb{H}$ by the group $\mathrm{Sl}(2, \mathbb{Z}\,)$:

Theorem 3.1 *The map $\tau \to \mathbb{C}/\Lambda_t$ induces a bijection*

$$\mathbb{H}/\,\mathrm{Sl}(2, \mathbb{Z}\,) \simeq \mathscr{E}$$