Lecture 12: Elliptic curves from lattices

October 9, 2014

Today we pick up where we left off last time. Thus, let Γ be a *full lattice* in $\mathbb{C}$: that is, a subgroup of $\mathbb{C}$ which can be generated by two $\mathbb{R}$-linearly independent vectors $v_1, v_2 \in \mathbb{C}$. We proved the following:

Proposition 0.1. *There exists a unique meromorphic function $\wp \in \mathcal{M}(\mathbb{C}/\Gamma)$ such that:*

1. *The only pole of $\wp$ is at $0 \in \mathbb{C}/\Gamma$;*
2. *The Laurent series expansion of $\wp$ at $0 \in \mathbb{C}$ looks like*

$$\wp(z) = \frac{1}{z^2} + (\textit{terms of degree} \geq 1).$$

Note that this $\wp$ is necessarily *even*, namely $\wp(-z) = \wp(z)$. This follows from uniqueness.

Today we want to use this one function $\wp$ to understand the whole field $\mathcal{M}(\mathbb{C}/\Gamma)$. Namely, we will prove:

Theorem 0.2. 1. *For every $f \in \mathcal{M}(\mathbb{C}/\Gamma)$ there are unique rational functions $A, B \in \mathbb{C}(z)$ such that*

$$f = A(\wp) + B(\wp) \cdot \wp',$$

where $\wp'$ is the derivative of $\wp$.

2. *We have an equation of the form*

$$(\wp')^2 = 4 \cdot \prod_{e \in S} (\wp - e),$$

where S is a three-element subset of $\mathbb{C}$ satisfying $\sum_{e \in S} e = 0$. (This set S is determined by the lattice Γ.)

Combined, the two results of this theorem exactly determine $\mathcal{M}(\mathbb{C}/\Gamma)$. In field theory notation, they show

$$\mathcal{M}(\mathbb{C}/\Gamma) = \mathbb{C}(z)\left(\sqrt{4 \cdot \prod_{e \in S}(z - e)}\right).$$

In words, the field $\mathcal{M}(\mathbb{C}/\Gamma)$ is obtained from the field $\mathbb{C}(z)$ by adjoining a square root of $4 \cdot \prod_{e \in S}(z - e)$.

Let us start with something purely formal, which really has nothing to do with Riemann surfaces:

Lemma 0.3. *Every function $f \in \mathcal{M}(\mathbb{C}/\Gamma)$ can be uniquely written in the form*

$$f = f_1 + f_2,$$

where f_1 is even and f_2 is odd. (That is, $f_1(-z) = f_1(z)$ and $f_2(-z) = -f_2(z)$.)

Proof. Define maps $f \mapsto f_+$ and $f \mapsto f_-$ from $\mathcal{M}(\mathbb{C}/\Gamma)$ to itself as follows:

$$f_+(z) = \frac{f(z) + f(-z)}{2},\ f_-(z) = \frac{f(z) - f(-z)}{2}.$$

Then the following claims are obvious:

1. $f = f_+ + f_-$.
2. f_+ is even and f_- is odd.
3. f is even if and only if $f_+ = f$ if and only if $f_- = 0$, and f is odd if and only if $f_+ = 0$ if and only if $f_- = f$.
4. The maps $f \mapsto f_+, f_-$ are $\mathbb{C}$-linear.

The first two points already establish existence. As for uniqueness, suppose $f = f_1 + f_2$ with f_1 even and f_2 odd. Then applying $(-)_+$ to both sides shows $f_+ = f_1$, and applying $(-)_-$ shows $f_- = f_2$. Thus we have uniqueness. □

The relevant general context for this result is that of *isotypic decomposition* in representation theory. Above was just the special case of the cyclic group of order two $\pm$ acting on the vector space $\mathcal{M}(\mathbb{C}/\Gamma)$.

Given the lemma, to prove the first part of the theorem it suffices to show that every even $f \in \mathcal{M}(\mathbb{C}/\Gamma)$ can be written as $A(\wp)$ for some unique $A \in \mathbb{C}(z)$, and every odd $f \in \mathcal{M}(\mathbb{C}/\Gamma)$ can be written as $B(\wp) \cdot \wp'$ for some unique $B \in \mathbb{C}(z)$. But actually it suffices to just show the first claim, for the following reason: $\wp'$ is a nonzero odd function, so multiplication and division by $\wp'$ gives a bijection between even functions and odd functions.

So we should prove that every even meromophic function is uniquely a rational function of $\wp$. For this we study the geometry of $\wp$, viewed as a holomorphic map $\mathbb{C}/\Gamma \to \mathbb{P}^1$.

Lemma 0.4. *The map $\wp$ is surjective. Moreover, for $z, w \in \mathbb{C}/\Gamma$, we have $\wp(z) = \wp(w)$ if and only if $z = \pm w$.*

Thus, at least set-theoretically, what $\wp$ does is it realizes $\mathbb{P}^1$ as being obtained from $\mathbb{C}/\Gamma$ by gluing two points together if they differ by $\pm$. You should try to picture this topologically.

Proof. Since $\wp$ has exactly one pole of multiplicity two, the degree of $\wp$ is two. So each fiber of $\wp$ has either one or two points, and in the first case the point has multiplicity two, and in the second case both points have multiplicity one. In particular each fiber is nonempty, so $\wp$ is surjective.

Now, certainly if $z = \pm w$ then $\wp(z) = \wp(w)$, since $\wp$ is even. For the converse, suppose $\wp(z) = \wp(w)$. Consider the set $\{z, -z, w\}$. This has three elements, and they all map to the same point under the degree two map $\wp$. Thus we either have $z = w$, $-z = w$, or $z = -z$. In the first two cases we're done. So suppose $z = -z$.

Then, consider a small $\epsilon \in \mathbb{C}$, and let $z_0 = z + \epsilon$. Then $-z_0 = z - \epsilon$, so z_0 and $-z_0$ are distinct points arbitrarily close to z which both map to the same point under $\wp$. It follows that $\wp$ is not a local isomorphism near z, so that the multiplicity of $\wp$ at z is bigger than one. Hence it must be two, and the fiber above $\wp(z)$ only has one element, so $w = z$, as desired. □

As a byproduct of the proof, we've understood the multiplicity of $\wp$ at every point $z \in \mathbb{C}/\Gamma$: if $z \neq -z$, the multiplicity is one, and if $z = -z$, the multiplicity is two. Moreover, the points of multiplicity two must map to distinct points in $\mathbb{P}^1$, since otherwise the degree of $\wp$ above the coincidence point would be too large.

Note that there are exactly four points on $\mathbb{C}/\Gamma$ satisfying $z = -z$: indeed, $z = -z$ means that z is represented by a complex number with $2z \in \Gamma$. Thus we need only look for the points of $\Gamma/2$ in the fundamental domain. In terms of the basis vectors, these are 0, $\frac{v_1}{2}$, $\frac{v_2}{2}$, and $\frac{v_1+v_2}{2}$. This is the so-called *2-torsion* of $\mathbb{C}/\Gamma$.

We know 0 maps to $\infty \in \mathbb{P}^1$. Thus the other three points must map to three distinct complex numbers. We take this three-element set to be our $S \subset \mathbb{C}$. Explicitly,

$$S = \{\wp(\frac{v_1}{2}), \wp(\frac{v_2}{2}), \wp(\frac{v_1+v_2}{2})\},$$

though the set itself is independent of the chosen basis v_1, v_2 for Γ.

One says that $\wp$ realizes $\mathbb{C}/\Gamma$ as a degree-two *branched cover* of $\mathbb{P}^1$, branched at the four points in $S \cup \{\infty\}$. Actually, there's only one such branched cover, up to isomorphism (we may see this argument later), so we could say that it realizes $\mathbb{C}/\Gamma$ as *the* degree-two *branched cover* of $\mathbb{P}^1$, branched at the four points in $S \cup \{\infty\}$.

Now, let's prove that every even function $f \in \mathcal{M}(\mathbb{C}/\Gamma)$ can be written as $A(\wp)$ for some unique $A \in \mathbb{C}(z)$. In other words, thinking about meromorphic functions as maps to $\mathbb{P}^1$, we need to show that every even map $f : \mathbb{C}/\Gamma \to \mathbb{P}^1$ is of the form $f = A \circ \wp$ for some unique $A : \mathbb{P}^1 \to \mathbb{P}^1$.

However, by the previous lemma, f being even is exactly the same as f being constant on the fibers of $\wp$. Thus the claim will follow from the following general lemma:

Lemma 0.5. *Let $p : X \to Y$ be a surjective map of connected Riemann surfaces. Then for every Riemann surface Z, composition with p gives a bijection between holomorphic maps $Y \to Z$ and holomorphic maps $X \to Z$ which are constant on each fiber of p.*

We already saw this in the special case when Y is the quotient of X by some free action; the general case is slightly more complicated because p could have points of multiplicity > 1. But it's still not so bad:

Proof. Certainly if $g : Y \to Z$ is holomorphic, then $g \circ p$ is holomorphic and constant on each fiber of p. Let us go the other way. Suppose $f : X \to Z$ is holomorphic and constant on each fiber of p. Define a function $g : Y \to Z$ by $g(y) = f(x)$, where x is any point in the fiber $p^{-1}(y)$. This is well-defined, since f is constant on fibers and p is surjective. Furthermore it's clear that g is the unique set-theoretic function which satisfies $g \circ p = f$. Thus we need only show that g is holomorphic.

Thus, let $y \in Y$, and choose an $x \in X$ with $p(x) = y$. By the local structure theorem, we can represent p in local charts around x and y by some n^{th} power map. Thus the claim is that if φ is a function from a neighborhood of 0 to $\mathbb{C}$ such that $\psi(z) = \varphi(z^n)$ is holomorphic in a neighborhood of 0, then so is φ. Certainly φ is holomorphic at every point except possibly 0, since $z \mapsto z^n$ is a local isomorphism away from 0. But also $\varphi(z)$ is bounded at 0, since ψ is. So we can conclude holomorphicity at 0 as well, by the removable singularities theorem. □

Thus we've proven that every even function is uniquely a rational function of $\wp$, and hence we've proved the first part of the theorem, describing the additive structure of $\mathcal{M}(\mathbb{C}/\Gamma)$. For the second part of the theorem, giving the multiplicative structure, we will need to make the above proof more effective in the case of $f = (\wp')^2$.

Indeed, $(\wp')^2$ is certainly an even function, being the square of an odd function. So we just have to see that the explicit rational function of $\wp$ which $(\wp')^2$ is equal to, is given by that funky product.

This can be accomplished by figuring out the zeros and poles of $\wp'$. These follow from our knowledge of the multiplicities of $\wp$, by considering power series expansions in $(z - z_0)$ for a given $z_0 \in \mathbb{C}$. The result is that the zeros and poles of $\wp'$ are confined to the four points where $\wp$ has multiplicity > 1, i.e. the points $z_0 \in \mathbb{C}/\Gamma$ where $z_0 = -z_0$. More specifically, $\wp'$ has a unique pole at $0 \in \mathbb{C}/\Gamma$ of multiplicity 3, has a zero of order one at the three other points $z_0 \in \mathbb{C}/\Gamma$ satisfying $z_0 \neq -z_0$, and has no zeros or poles elsewhere. Thus $(\wp')^2$ has a pole of order 6 at 0 and a zero of order 2 at those three points z_0, and no other zeros or poles. Now, we can easily find a rational function A such that $A \circ \wp$ has these same zeros and poles, namely by taking

$$A(z) = \prod_{e \in S} (z - e).$$

This $A \in \mathcal{M}(\mathbb{P}^1)$ has a pole of order 3 at ∞, and a zero of order 1 at each $e \in S$. Since multiplicities multiply under holomorphic maps (because $(z^n)^m = z^{nm}$), it follows that $A \circ \wp$ has the same zeroes and poles as $(\wp')^2$. Thus there is a nonzero constant λ such that

$$(\wp')^2 = \lambda \cdot \prod_{e \in S} (\wp - e).$$

To calculate λ, we can just consider Laurent expansions at 0. The lowest-order term on the left-hand side is $(\frac{-2}{z^3})^2 = \frac{4}{z^6}$, whereas the lowest order term on the right is $\lambda \cdot (\frac{1}{z^2})^3 = \frac{\lambda}{z^6}$. Thus $\lambda = 4$, which gives the desired equation.

The last claim was that $\sum_{e \in S} e = 0$. This can be seen by expanding out the product, so writing

$$(\wp')^2 = 4 \cdot \wp^3 + a\wp^2 + b\wp + c.$$

One finds, using the Laurent series expansions of $\wp$ and $\wp'$, that $a = 0$, which translates exactly to the desired $\sum_{e \in S} e = 0$. Going a bit further, one also sees that

$$b = -60 \cdot \sum_{\gamma \in \Gamma \setminus \{0\}} \frac{1}{\gamma^4}$$

and

$$c = -140 \cdot \sum_{\gamma \in \Gamma \setminus \{0\}} \frac{1}{\gamma^6}.$$

Thus our equation can be rewritten

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

where, as is traditional, g_2 and g_3 denote $-b$ and $-c$ respectively. Thus g_2 and g_3 are explicit constants determined by the lattice Γ via the above formula.

Now, there was one last theorem we said we would prove today:

Theorem 0.6. *The map $z \mapsto (\wp(z), \wp'(z))$ gives an isomorphism*

$$(\mathbb{C}/\Gamma) \setminus \{0\} \leftrightarrow \{y^2 = f(x)\} \subset \mathbb{C}^2,$$

where $f(x) = 4 \cdot \prod_{e \in S}(x - e) = 4x^3 - g_2x - g_3$.

Here on the right we mean the Riemann surface associated to the polynomial $P(x,y) = y^2 - f(x)$. Note that this equation is smooth, because the y-derivative of P is $2y$, so is zero only when $y = 0$; but on the other hand the x-derivative is $p'(x)$, so is zero only when $p'(x) = 0$. But p has distinct roots, so p and p' are never simultaneously zero. Thus at every point (x,y) with $P(x,y) = 0$, one or the other of the partial derivatives of P is nonzero. That's why we can call the set $\{y^2 = f(x)\}$ a Riemann surface: we proved in such a situation that there is a unique Riemann surface structure on this set for which both the x-projection and the y-projection give holomorphic maps to $\mathbb{C}$.

Now we prove the theorem.

Proof. Since we've removed the unique pole of both $\wp$ and $\wp'$, the map f defined by $z \mapsto (\wp(z), \wp'(z))$ lands inside $\mathbb{C}^2$. Because of the identity

$$(\wp')^2 = 4 \cdot \prod_{e \in S} (\wp - e),$$

it actually lands inside $\{y^2 = f(x)\}$. Furthermore, this resulting map $f : (\mathbb{C}/\Gamma) \backslash \{0\} \to \{y^2 = f(x)\}$ is holomorphic, since its projection to the x-axis is the holomorphic map $\wp$, and its projection to the y-axis is the holomorphic map $\wp'$, and at every point on $\{y^2 = f(x)\}$ either the x-projection or the y-projection is a local isomorphism.

Next, we argue that f is proper. This is because f is obtained by restricting the continuous map $(\wp, \wp') : \mathbb{C}/\Gamma \to \mathbb{P}^1 \times \mathbb{P}^1$ to the subset $\mathbb{C} \times \mathbb{C}$ of the target. But on the other hand $\mathbb{C}/\Gamma$ is compact and $\mathbb{P}^1 \times \mathbb{P}^1$ is Hausdorff, so any such map is proper.

So f is proper. On the other hand, $\wp : \mathbb{C}/\Gamma \setminus \{0\} \to \mathbb{C}$ has degree two, and it factors as the composition of f with projection onto the x-axis, which also has degree two (since there are generically two choices for the square root giving y in terms of x). Thus, by multiplicity of degrees under composition, f must have degree 1. Thus it is an isomorphism. □

The one-sentence version of the above proof is that $(\mathbb{C}/\Gamma) \setminus \{0\}$ and $\{y^2 = f(x)\}$ are branched over $\mathbb{C}$ in the same way (via, respectively, $\wp$ and projection to the x-axis), so they must be isomorphic.

Now we're done, but let's step back for second and inspect the terrain. Consider the following three sets:

1. $Unif$: The set of all full lattices $\Gamma \subset \mathbb{C}$.
2. $Branch$: The set of all 3-element subsets $S \subset \mathbb{C}$ satisfying $\sum_{e \in S} e = 0$.
3. Eqn: The set of all pairs (g_2, g_3) of complex numbers satisfying $g_2^3 - 27 \cdot g_3^2 \neq 0$.

Then we have seen how to map $Unif \to Branch \to Eqn$. Namely, $Unif \to Branch$ sends Γ to the image under $\wp$ of the non-zero 2-torsion of $\mathbb{C}/\Gamma$. And $Branch \to Eqn$ sends S to

$$(g_2, g_3) = (-4 \cdot \sum_{\{e,e'\} \subset S, e \neq e'} e \cdot e', 4 \cdot \prod_{e \in S} e)$$

(so that $4x^3 - g_2 x - g_3 = 4 \cdot \prod_{e \in S}(x - e)$.) The reason the equation $g_2^3 - 27 \cdot g_3^2 \neq 0$ holds is because of the discriminant identity

$$\prod_{e \neq e' \in S} (e - e') = -16 \cdot (g_2^3 - 27 g_3^2).$$

We also saw another description of the composite $Latt \to Eqn$, namely

$$(g_2, g_3) = (60 \cdot \sum_{\gamma \in \Gamma \setminus \{0\}} \gamma^{-4}, 140 \cdot \sum_{\gamma \in \Gamma \setminus \{0\}} \gamma^{-6}).$$

Of course, these formulas look totally wild. But the three sets $Latt$, $Branch$, and Eqn nonetheless just reflect three different ways of looking at the same class of Riemann surfaces, and the formulas fell out from this. Namely, in $Latt$ we think of X as $\mathbb{C}/\Gamma$, in $Branch$ we think of X as the degree-two branched cover of $\mathbb{P}^1$ branched at $S \cup \{\infty\}$, and in Eqn we think of X as the one-point compactification of the Riemann surface of the equation $\{y^2 = 4x^3 - g_2 x - g_3\}$.

In fact, using this geometric perspective, we will see in the following lectures that all of the above maps are bijections, so that the three sets $Latt$, $Branch$, and Eqn can be identified. This will be done by introducing the fourth geometric set which will be in bijection with all of the above sets:

4. The set of triples (X, x, ω) consisting of a compact connected Riemann surface X, a point $x \in X$, and a non-vanishing holomorphic one-form ω, these triples being taken up to isomorphism.

Such a triple (X, x, ω) is known as an *elliptic curve with non-vanishing holomoprhic one-form*, the underlying pair (X, x) is known just as an *elliptic curve*, and the underlying Riemann surface X is known as a *curve of genus* 1. The curves of genus 1 can also be characterized topologically: they are the Riemann surfaces isomorphic to a torus.

The crucial thing is that we will see how to uniformize such an X by $\mathbb{C}$. This is what will let us invert the maps described above, hence showing they're bijections. The argument we use will also be a simple prototype for the general uniformization theorem.

But what if we're interested, not in triples as above, but just the underlying Riemann surfaces X, taken up to isomorphism? Fortunately, it's pretty easy to describe what happens when you forget the structure. For example, suppose one wants to forget about the one-form ω, and just understand when two elliptic curves (X, x) are isomorphic. The uniformization picture is the most useful for this: we represent X as $\mathbb{C}/\Gamma$, with x corresponding to 0. Then the set of isomorphisms between X and $X' = \mathbb{C}/\Gamma'$ sending 0 to 0 is in bijection with the set of automorphisms of $\mathbb{C}$ which fix 0 and send Γ to Γ'. These are just the non-zero complex numbers $\lambda \in \mathbb{C}^*$ such that $\lambda\Gamma = \Gamma'$.

So isomorphisms of elliptic curves $(\mathbb{C}/\Gamma, 0)$ correspond exactly to scalings of the lattice Γ, i.e. $\Gamma \mapsto \lambda \cdot \Gamma$. One can then push this description through to $Branch$ and Eqn: for example, given $S, S' \in Branch$, isomorphisms between the corresponding elliptic curves correspond exactly to $\lambda \in \mathbb{C}^*$ such that $\lambda^2 \cdot S = S'$; and given $(g_2, g_3), (g_2', g_3') \in Eqn$, isomorphisms between the corresponding elliptic curves correspond exactly to $\lambda \in \mathbb{C}^*$ such that $\lambda^4 \cdot g_2 = g_2'$ and $\lambda^6 \cdot g_3 = g_3'$.

(Note the exponents on λ: these are numbers known as *weights*. For example, g_3 is what's known as a *modular form of weight* 6.)