Lecture 15: Uniformization of elliptic curves, and moduli

June 24, 2015

In the last lecture we proved the following:

Theorem 0.1. *Let (X, x, ω) be a triple consisting of a compact connected Riemann surface X, a point $x \in X$, and a nowhere vanishing holomorphic one-form $\omega \in \Omega(X)$. Then there is a unique full lattice $\Gamma \subset \mathbb{C}$ and isomorphism*

$$f : \mathbb{C}/\Gamma \simeq X$$

such that $f(0) = x$ and $f^*(\omega) = dz$.

We also saw how to produce Γ and f explicitly. Namely, Γ consists of the so-called *periods* of ω:

$$\Gamma = \{\int_\gamma \omega \in \mathbb{C} \mid \ \gamma \in \pi_X(x, x)\},$$

and f is given by the solution to the vector field v dual to ω (so $\omega(v) = 1$ at every point).

In this lecture, we'll give an explicit example of this, taking X to be an *elliptic curve*. The result is the following.

Theorem 0.2. *Let $p(x) \in \mathbb{C}[x]$ be a cubic polynomial with distinct roots, and consider the Riemann surface*

$$U = \{(x, y) \in \mathbb{C}^2 \ \mid \ y^2 = p(x)\}.$$

There is a natural Riemann surface structure on the one-point compactification $X = U \cup \{\infty\}$. Moreover, the holomorphic one-form $\frac{dx}{y}$, a priori defined on an open subset of X, actually uniquely extends to a nowhere-vanishing holomorphic one form ω on X.

Thus, by the above theorem, we get a unique lattice $\Gamma \subset \mathbb{C}$ and isomorphism

$$\mathbb{C}/\Gamma \simeq X$$

which sends 0 to ∞ and pulls back ω to dz. This explicitly means that solutions to the equation $y^2 = p(x)$ can be naturally parametrized by complex numbers.

We will for simplicity of notation assume that $p(x)$ has leading term $4 \cdot x^3$. This doesn't really matter, but that's the leading term that came out of the Weierstrass p-function in lecture REF, and we'll want to match up with that discussion at some point.

The first thing to recall is why U is a Riemann surface. In lecture REF we showed that U acquires a Riemann surface such that the x and y projections are holomorphic functions provided that the partial derivatives of

$$P(x, y) = y^2 - p(x)$$

don't both vanish at any point $x, y \in U$. But $\partial_y P = 2y$ and $\partial_x P = p'(x)$, so any common point of vanishing will have $y = 0$ and $p'(x) = 0$; if it's on U, then we also have $y^2 = p(x)$, so this means $p'(x) = 0 = p(x)$. But by hypothesis p has distinct roots, so this never happens. Thus U is a Riemann surface as indicated. Explicitly, the x-projection is a local isomorphism away from the three points $(0, x)$ where $p(x) = 0$, and the y-projection is a local isomorphism away from the four points (y, x) where $p'(x) = 0$.

Now let us compactify U. To do this, we should identify an "open neighborhood of ∞" in U which is isomorphic to a punctured neighborhood of the origin in $\mathbb{C}$. Then we can glue on an actual neighborhood of the origin in order to get X. The key is that for large x and y, the leading term $4 \cdot x^3$ of $p(x)$ dominates, so the relation $y^2 = p(x)$ behaves in the same way as $y^2 = 4 \cdot x^3$. This in turn can be explicitly parametrized by $x = t^2, y = 2 \cdot t^3$, with inverse $t = \frac{y}{2x}$. A more precise analysis gives:

Lemma 0.3. *Let U be the Riemann surface of $y^2 = p(x)$ as above. There exists a compact subset $K \subset U$, an open neighborhood V of the origin in $\mathbb{C}$, and a holomorphic function $\varphi : V \to \mathbb{C}$ with $\varphi(0) = 1$ such that*

$$u \mapsto (\frac{1}{u^2}, \frac{1}{2 \cdot u^3} \cdot \varphi(u))$$

defines an isomoprhism from $V \setminus 0$ to $U \setminus K$.

Proof. We will arrive at this isomorphism in two steps. First, together with U we consider the simpler Riemann surface U' of the equation $y^2 = 4x^3$. This is a Riemann surface away from $(0, 0)$. On both U and U' we have the projections to the x-axis, which are of degree two. Call them π and π'.

Choose $R > 0$ large enough so that both

$$|\frac{p(x)}{4 \cdot x^3} - 1| < 1$$

and

$$|\frac{4 \cdot x^3}{p(x)} - 1| < 1$$

whenever $|x| > R$. Now, let D be the closed disk of radius R around the origin in $\mathbb{C}$, and set $K = \pi^{-1}(D)$ and $K' = \pi'^{-1}(D)$. Then if we use $\sqrt{z}$ to denote the holomorphic square root function in the open disk $|z - 1| < 1$ which takes 1 to 1, the functions

$$(x, y) \mapsto (x, y \cdot \sqrt{\frac{4 \cdot x^3}{p(x)}})$$

and

$$(x, y) \mapsto (x, y \cdot \sqrt{\frac{p(x)}{4 \cdot x^3}})$$

clearly define mutually inverse isomorphisms $U \setminus K \simeq U' \setminus K'$. On the other hand, if V denotes the open disk of radius $R^{-1/2}$ around 0 in $\mathbb{C}$, it's also simple to check that

$$(x, y) \mapsto \frac{y}{2x}$$

and

$$u \mapsto (u^{-2}, 2 \cdot u^{-3})$$

define mutually inverse isomorphisms $V \setminus \{0\} \simeq U' \setminus K'$. Composing, we obtain an isomorphism $U \setminus K \simeq V \setminus \{0\}$ of the desired form. ☐

It follows that this u-parametrization gives charts on a "neighborhood of ∞" in U, so we can glue on the whole of V along the u-parametrization to compactify U to $X = U \cup \{\infty\}$, as we wanted.

The next business is to consider the one-form

$$\omega = \frac{dx}{y}.$$

As it stands, this ω is defined and holomorphic on $X \setminus \{\infty, p, q, r\}$, where p, q, r are the points of U with $y = 0$. There are three of these, because $p(x)$ is a cubic polynomial with distinct roots. Furthermore, ω is nonzero at every point of $X \setminus \{\infty, p, q, r\}$: indeed, on these points x is a local isomorphism, so $dx \neq 0$.

What we need to see is that ω extends to a nowhere vanishing holomorphic one-form on all of X. Note that such an extension is necessarily unique, by the removable singularities theorem.

First let's analyze the points p, q, r. Applying d to the defining equation

$$y^2 = p(x)$$

and using the product rule, we get

$$2 \cdot y \cdot dy = p'(x) \cdot dx.$$

Thus, away from the locus where $p'(x) = 0$ we can write

$$\omega = \frac{2 \cdot dy}{p'(x)}.$$

Since p has distinct roots, this locus doesn't meet $\{p, q, r\}$, this shows that ω extends to a holomorphic one-form in a neighborhood of p, q, r. It is also nonzero there, because at those points y gives a local isomorphism, so $dy \neq 0$.

Finally we treat ∞. By the lemma and some calculation with the Leibniz rule, we find

$$\frac{dx}{y} = -\frac{du}{\varphi(u)}.$$

Since u at 0 gives local charts of X at ∞, and $\varphi(0) = 1$, this gives the desired extension over ∞.

Thus X carries the nowhere vanishing holomorphic one-form $\omega = dx/y$. Hence, by the theorem, there is a unique full lattice $\Gamma \subset \mathbb{C}$ and isomorphism

$$\mathbb{C}/\Gamma \simeq X$$

carrying 0 to ∞ and ω to dz.

On the other hand, in lecture REF we saw something of a converse: if $\Gamma \subset \mathbb{C}$ is any full lattice, then if we take the cubic polynomial

$$p(x) = 4 \cdot x^3 - g_2 \cdot x - g_3,$$

where

$$g_2 = 60 \cdot \sum_{z \in \Gamma \setminus 0} \frac{1}{z^4}$$

and

$$g_3 = 140 \cdot \sum_{z \in \Gamma \setminus 0} \frac{1}{z^6},$$

then $p(x)$ has distinct roots and we get an isomorphism

$$\mathbb{C}/\Gamma \simeq \{y^2 = p(x)\} \cup \{\infty\},$$

defined by taking $x(z)$ to be the Weierstrass p-function and $y(z)$ to be its derivative. This isomorphism does send 0 to ∞, and because $y(z)$ is the z-derivative of $x(z)$, we have

$$dz = \frac{dx}{y}.$$

Thus, by the uniqueness claim of the theorem we just proved, if you start with a full lattice Γ, then produce the polynomial $p(x)$ as above, then uniformize the corresponding Riemann surface, you get the same Γ back again. What about in the other direction, if you start with a polynomial, uniformize to get a lattice, then get another polynomial back again?

Proposition 0.4. *Suppose $p(x) = 4x^3 + bx + a$ is a cubic polynomial with leading coefficient 4 and vanishing x^2 coefficient, such that $p(x)$ has distinct roots. Let Γ be the lattice gotten by uniformizing $X = U \cup \{\infty\}$ as above. Then in terms of the uniformization isomorphism*

$$\mathbb{C}/\Gamma \simeq X,$$

the function x identifies with the Weierstrass p-function for the lattice Γ, and y identifies with its derivative. Thus $a = -g_3(\Gamma)$ and $b = -g_2(\Gamma)$.

Proof. By the relation $dz = dx/y$, the y-claim follows from the x-claim. And for that, by the characterization of the Weierstrass p-function we need to see that the Laurent expansion of $x(z)$ is of the form

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

However, the z parameter is gotten by integrating the form ω away from ∞, or $u = 0$. Since

$$\omega = -\frac{du}{\varphi(u)},$$

this means that z is given in terms of u as the unique antiderivative of $-1/\varphi(u)$ with value 0 at $u = 0$, and u is given in terms of z as

$$u(z) = G(z),$$

where $G(z) = -z + \ldots$ is the functional inverse to that antiderivative.

Remembering the definition of φ and tracing this through, one can calculate that since the x^2 term of $p(x)$ vanishes, the expression

$$x = \frac{1}{u^2} = \frac{1}{G(z)^2}$$

does have the required form, so that x is the Weierstrass p-function. $\square$

If you collect everything together, you'll find that we've proved the following remarkable result:

Theorem 0.5. *Define three sets A, B and C as follows.*

- *A is the set of isomorphism class of triples (X, x, ω) where X is a compact connected Riemann surface, x is a point of X, and ω is a nowhere vanishing holomorphic one-form on X.*
- *B is the set of full lattices $\Gamma \subset \mathbb{C}$.*
- *C is the set of cubic polynomials of the form $p(x) = 4 \cdot x^3 + bx + a$ having distinct roots.*

Then the following maps give mutually inverse bijections between A, B, and C:

- *From $A \to B$: associate to (X, x, ω) the set of periods*

$$\{\int_\gamma \omega \in \mathbb{C} \mid \ \gamma \in \pi_X(x, x)\}.$$

- *From $B \to C$: associate to Γ the cubic polynomial*

$$4 \cdot x^3 - g_2(\Gamma) \cdot x - g_3(\Gamma).$$

- *From $C \to A$: associate to $p(x)$ the compactification of the Riemann surface*

$$\{y^2 = p(x)\},$$

with basepoint ∞ and one-form dx/y.

These sets A, B, C are thus three ways of talking about the *moduli space of elliptic curves with non-vanishing one-form*. Actually, implicit in C is two other descriptions: we can either parametrize such $p(x)$'s by their coefficients, in which case they amount to two complex numbers (a, b) such that

$$\Delta := b^3 - 27a^2 \neq 0,$$

or else we can parametrize them by their roots, in which case they amount to a three-element subset $S \subset \mathbb{C}$ with center of gravity 0.

I said moduli *space*, because in fact these sets all have natural topologies (even more, they are complex manifolds), and the bijections above are homeomorphisms (even analytic isomorphisms). This can be fun to think about. For example, take the description in terms of 3-element subsets of $\mathbb{C}$. A path in this space is known as a *braid*, because if you plot the location of the three element subset as a function of time you'll see a braid on three strands. Therefore, to every such braid there corresponds some path in the space of full lattices $\Gamma \subset \mathbb{C}$, as well as a natural one-parameter family of Riemann surfaces. And in the (a, b) terms, you get a path in the complement of a $(3, 2)$-torus knot, which is in fact a trefoil knot. You can try to think about this overwhelming multiplicity of interpretations next time you're braiding your friend's hair.