LECTURE 13: MODULI STACK OF ELLIPTIC CURVES

STEPHEN MCKEAN

We're at the midway point of the semester, so the pace is going to pick up a bit. Please don't hesitate to reach out for help if you find the class is moving too quickly for you.

1. Modular forms from $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$

Recall that $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ is our moduli space of elliptic curves over $\mathbb{C}$. Quotients like this are perfectly good geometric objects (called *orbifolds* or *stacks*, depending on your context), but they might have some slightly strange behavior at singular points. This behavior is the *stabilizer* of the group action. When you have a regular covering of a manifold, the automorphism group acts with trivial stabilizers everywhere, and the quotient is again a manifold. But with $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$, there are a few points with finite but non-trivial stabilizers.

Exercise 1.1. Compute the stabilizers of i and $e^{\pi i/3}$ in $\mathbb{H}$ under the action of $\mathrm{SL}_2(\mathbb{Z})$.

Since $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ is a geometric object, we should be able to talk about vector bundles over it. These should be the same as vector bundles on $\mathbb{H}$ that are compatible with the action of $\mathrm{SL}_2(\mathbb{Z})$.

The trivial line bundle $\mathcal{L} \to \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ is defined as the quotient of $\mathbb{C}\times\mathbb{H}$ by the $\mathrm{SL}_2(\mathbb{Z})$ action

$$(z,\tau) \mapsto (z, \tfrac{a\tau+b}{c\tau+d}).$$

But we could just as well consider the action

$$(z,\tau) \mapsto ((c\tau+d)^{2k}z, \tfrac{a\tau+b}{c\tau+d}).$$

To see that this actually gives a line bundle, we would need to check the cocycle condition $(c_1\tau+d_1)^{2k}(c_2\tau+d_2)^{2k} = (c_3\tau+d_3)^{2k}$, where

$$\begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}.$$

I'll leave this to you as an exercise, but this all works out to give us a line bundle $\mathcal{L}_{2k}$. Sections of this line bundle are holomorphic functions on $\mathbb{H}$ such that $f(\gamma\cdot\tau) = (c\tau+d)^{2k}f(\tau)$, so modular forms of weight $2k$ naturally arise as sections of a line bundle on $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. For a more thorough discussion, see Milne's notes: `https://www.jmilne.org/math/CourseNotes/mf.html`.

2. The j-invariant

Recall that $g_2(\Lambda)$ and $g_3(\Lambda)$ are invariants of the lattice Λ, and hence of the elliptic curve $\mathbb{C}/\Lambda$. However, these are not invariant under homothety (and hence under isomorphism), as we saw previously. But if we take an appropriate ratio of polynomials in g_2 and g_3, we can cancel out the effect of scaling and get an invariant of lattices up to homothety (and hence of elliptic curves up to isomorphism). This leads us to the *j-invariant*.

Definition 2.1. The *j-invariant* of a lattice Λ or an elliptic curve $\mathbb{C}/\Lambda$ is the complex number

$$j(\Lambda) = 1728\frac{g_2^3}{g_2^3 - 27g_3^2}.$$

Note that $j(\Lambda)$ is invariant under homothety (or equivalently, under $\mathrm{SL}_2(\mathbb{Z})$ action), so we get a function

$$j(\tau) : \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \to \mathbb{C}.$$

We won't dive too deep into the amazing world of $j(\tau)$, but this would make a fun semester project if you're interested. For now, here are some important facts:

- $j(\tau) : \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \to \mathbb{C}$ is a complex analytic isomorphism. In particular, $\mathbb{C}$ is the moduli space of elliptic curves from the perspective of complex analysis.
- The Fourier expansion of $j(\tau)$ in $q = e^{2\pi i\tau}$ is
$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \ldots$$
Miraculously, all of these coefficients are *integers*. There's a good reason for this (which we'll talk about today), but for now I want you to imagine how baffling this must have been when it was first discovered.
- A *modular function* is a meromorphic function $\mathbb{H} \to \mathbb{C}$ that is invariant under $\mathrm{SL}_2(\mathbb{Z})$. It turns out that the set of all modular functions is the field of rational functions $\mathbb{C}(j)$, where j is the j-invariant.

Last time, we built the moduli space of elliptic curves over $\mathbb{C}$ by thinking carefully about lattices in $\mathbb{C}$. Over other fields, we can't use this approach. The j-function gives us an alternative route:

Theorem 2.2. *Let E and E' be elliptic curves over a field k. Then E and E' are isomorphic over $\overline{k}$ if and only if $j(E) = j(E')$. If $\mathrm{char}(k) \neq 2$ or 3 and $j(E) = j(E')$, then there is a field extension of degree at most 2 (if $j \neq 0, 1728$), 4 (if $j = 1728$), or 6 (if $j = 0$) such that E and E' are isomorphic over K.*

Proof. For the sake of simplicity, we'll assume $\mathrm{char}(k) \neq 2, 3$ for both parts of the theorem. This allows us to write $E = \mathbb{V}(y^2 - x^3 - Ax - B)$ and $E' = \mathbb{V}(y^2 - x^3 - A'x - B')$ for some $A, A', B, B' \in k$ (by an exercise from last time). One can show that

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2},$$

which we may also denote by $j(A,B)$. Using projective changes of coordinates (like last time), one can show that E and E' are isomorphic over k if and only if there exists $\mu \in k^\times$ such that $A' = \mu^4 A$ and $B' = \mu^6 B$.

If E and E' are isomorphic over $\overline{k}$, then we have such a μ, and

$$\begin{aligned} j(A', B') &= 1728 \frac{4(\mu^4 A)^3}{4(\mu^4 A)^3 + 27(\mu^6 B)^2} \\ &= 1728 \frac{4A^3}{4A^3 + 27B^2} \\ &= j(A, B). \end{aligned}$$

Conversely, suppose $j(A,B) = j(A',B') = J$. If $J = 0$, then $A = A' = 0$, and we need at most a degree 6 extension K/k to obtain μ such that $B' = \mu^6 B$. Similarly, if $j = 1728$, then $B = B' = 0$ and we need at most a degree 4 extension K/k to obtain μ such that $A' = \mu^4 A$.

The real trick comes when $J \neq 0, 1728$. Now we use a miraculous substitution $A'' = 3J \cdot (1728 - J)$ and $B'' = 2J \cdot (1728 - J)^2$. You can check that $j(A'', B'') = J$. Now substitute $J = 1728 \frac{4A^3}{4A^3 + 27B^2}$ into A'' and B'' to find that

$$\begin{aligned} A'' &= \left(\frac{2^7 3^5 AB}{4A^3 + 27B^2} \right)^2 A, \\ B'' &= \left(\frac{2^7 3^5 AB}{4A^3 + 27B^2} \right)^3 B. \end{aligned}$$

You get similar equations substituting with the expressions involving A' and B'. Now set

$$\mu^2 = \left(\frac{2^7 3^5 AB}{4A^3 + 27B^2} \right) \left(\frac{4A'^3 + 27B'^2}{2^7 3^5 A'B'} \right)$$

and check that $A' = \mu^4 A$ and $B' = \mu^6 B$. We need at most a degree 2 extension to find μ, as claimed. $\square$

Exercise 2.3. This theorem indicates that it is easier for two elliptic curves to be isomorphic over $\overline{k}$ than over k. Find an example of two elliptic curves E, E' over a field k such that E and E' are not isomorphic over k but are isomorphic over $\overline{k}$.

Remark 2.4. From the perspective of the j-function, the moduli space of elliptic curves is just $\mathbb{A}^1_{\mathbb{C}}$. But elliptic curves with $j = 0$ or 1728 have non-trivial automorphisms, whereas no points of $\mathbb{A}^1_{\mathbb{C}}$ have automorphisms. On the other hand, the quotient $\mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H}$ remembers the automorphisms at $\tau = i$ and $\tau = e^{\pi i/3}$, so this is a slightly richer moduli space of elliptic curves. Ultimately, the best constructions of this moduli space should admit automorphisms of points. This is where *stacks* come in.

3. Elliptic curves over a scheme

We're now going to talk about elliptic curves not just over a field, but over any scheme. For a more thorough treatment of this material, see [Ols16, Chapter 13]. Since $\operatorname{Spec}\mathbb{Z}$ is the initial scheme, a moduli space of elliptic curves over $\mathbb{Z}$ would be a best case scenario.

To work at this level of generality, we're going to start by defining this moduli "space" as a category whose objects represent elliptic curves (or rather as a functor out of such a category). In order to give geometric meaning to such a construction, we will need to show that this functor satisfies *descent* with respect to a certain topology (roughly, that we can define this functor on local open sets and then glue these opens together).

First, we have to say what an elliptic curve over a scheme is.

Definition 3.1. An *elliptic curve* over a scheme S is a smooth proper morphism $p : E \to S$, equipped with a chosen section $e : S \to E$ such that $(E, e) \times_S \operatorname{Spec}\overline{k(s)}$ is an elliptic curve for each $s \in S$.[1]

A *morphism* of elliptic curves $(p : E \to S, e) \to (p' : E' \to S', e')$ is a pair of scheme morphisms $f : S \to S'$ and $g : E \to E'$ such that $g \circ e = e' \circ f$, and such that the diagram

$$\begin{tikzcd} E \arrow[r, "g"] \arrow[d, "p"] & E' \arrow[d, "p'"] \\ S \arrow[r, "f"] & S' \end{tikzcd}$$

is Cartesian.

Exercise 3.2. If we take $S = \operatorname{Spec}\mathbb{Z}$, we need a smooth proper morphism $p : E \to \operatorname{Spec}\mathbb{Z}$ with a section $e : \operatorname{Spec}\mathbb{Z} \to E$ such that $(E, e) \times_{\mathbb{Z}} \operatorname{Spec}\overline{\mathbb{F}}_p$ is an elliptic curve for each prime p; we also need $(E, e) \times_{\mathbb{Z}} \operatorname{Spec}\overline{\mathbb{Q}}$ to be an elliptic curve.

What does this mean in practicality? We need an equation

$$y^2 + (a_1x + a_2)y = x^3 + a_3x^2 + a_4x + a_5 \in \mathbb{Z}[x, y]$$

with discriminant ± 1. The formula for the discriminant is

$$\Delta = \frac{\operatorname{disc}(4(x^3 + a_3x^2 + a_4x + a_5) + (a_1x + a_2)^2)}{256},$$

where disc denotes the discriminant of a univariate polynomial.

Try proving that $\Delta = \pm 1$ has no integral solutions. This is how Tate proved the following fact: there are no elliptic curves over $\mathbb{Z}$.

Now we can define a category of elliptic curves, which will function as the raw material for our moduli stack.

Definition 3.3. Let $\mathrm{Sch}_{\mathbb{Z}}$ denote the category of $\mathbb{Z}$-schemes. The *moduli stack of elliptic curves* $\mathcal{M}_{1,1}$ is the category over $\mathrm{Sch}_{\mathbb{Z}}$ with:

[1]This last condition means that the geometric fibers of $p : E \to S$ should all be elliptic curves.

- objects $(S, (p : E \to S, e))$, where S is a $\mathbb{Z}$-scheme and $(p : E \to S, e)$ is an elliptic curve over S, and
- morphisms of elliptic curves.

There is a forgetful functor $\pi : \mathcal{M}_{1,1} \to \mathrm{Sch}_{\mathbb{Z}}$ given on objects by $\pi(S, (p : E \to S, e)) = S$ and on morphisms by $F\pi(f, g) = f$.

Remark 3.4. The notation $\mathcal{M}_{1,1}$ signifies genus 1 and with 1 base point, as a special case of the very interesting moduli spaces $\mathcal{M}_{g,n}$. Sometimes $\mathcal{M}_{1,1}$ is denoted $\mathcal{M}_{\mathrm{ell}}$.

We've called $\mathcal{M}_{1,1}$ a stack, but we haven't said what a stack actually is. Very roughly, a stack over $\mathrm{Sch}_{\mathbb{Z}}$ is a sheaf on this category. To make sense of this, we have to talk about (i) what sort of values our sheaf takes and (ii) how to glue with respect to a topology.

For point (i), we need *categories fibered in groupoids.*

Definition 3.5. Let S be a scheme. A category $\mathcal{C}$ with a functor $\pi : \mathcal{C} \to \mathrm{Sch}_S$ is *fibered in groupoids* if:

(a) (Arrow lifitng) For all morphisms $f : U \to V$ in Sch_S and all $y \in \pi^{-1}(V)$, there exists a morphism $\phi : x \to y$ in $\mathcal{C}$ such that $\pi(\phi) = f$.

(b) (Diagram lifting) For all diagrams in $\mathcal{C}$ of the form

$$\pi\left(\begin{array}{ccc} & & x \\ & & \downarrow{\scriptstyle \phi} \\ y & \xrightarrow{\psi} & z \end{array}\right) = \begin{array}{ccc} & & U \\ & & \downarrow{\scriptstyle f} \\ V & \xrightarrow{g} & W, \end{array}$$

and for all $h : U \to V$ factoring f (so $f = g \circ h$), there exists a unique $\chi : x \to y$ in $\mathcal{C}$ such that $\phi = \psi \circ \chi$ and $\pi(\chi) = h$.

Given $U \in \mathrm{Sch}_S$, the *fiber over* U is the category $\mathcal{C}(U)$ whose objects are $\pi^{-1}(U)$ and whose morphisms are $\phi : x \to y$ with $x, y \in \pi^{-1}(U)$ and $\pi(\phi) = \mathrm{id}$.

Exercise 3.6. Here are a few features of this definition that are good to prove:

(i) The morphism $\phi : x \to y$ lifting $f : U \to V$ in part (a) is unique up to unique isomorphism. (Hint: use part (b).)

(ii) A morphism ϕ in $\mathcal{C}$ is an isomorphism if and only if $\pi(\phi)$ is an isomorphism in Sch_S.

(iii) The fiber $\mathcal{C}(U)$ is a *groupoid* (i.e. all morphisms in $\mathcal{C}(U)$ are isomorphisms). This justifies the terminology *fibered in groupoids.*

Next time, we'll finish this discussion by talking about Grothendieck topologies and how $\mathcal{M}_{1,1}$ is actually a sheaf.

Next time: wrapping up $\mathcal{M}_{1,1}$, then ring spectra and even periodic cohomology theories.

References

[Ols16] Martin Olsson. *Algebraic spaces and stacks*. Vol. 62. American Mathematical Society Colloquium Publications. American Mathematical Society, Providence, RI, 2016, pp. xi+298. URL: `https://doi.org/10.1090/coll/062`.

Department of Mathematics, Harvard University

Email address: `smckean@math.harvard.edu`

URL: `shmckean.github.io`