Topics in Algebraic Geometry: Modular Curves

Lectures by Richard Shadrach

transcribed by Jack Petok

Contents

1 8/31/2015: Yoneda Lemma

Let $\mathcal{C}$ be a category, and let X be an objet of $\mathcal{C}$. We define the following contravariant functor:

$$h_x \colon \mathcal{C} \to \text{Set}$$

$$T \mapsto \text{Hom}_{\mathcal{C}}(T, X)$$

It is contravariant because a morphism $T_1 \xrightarrow{f} T_2$ induces a morphism $\mathrm{Hom}_{\mathcal{C}}(T_2, X) \to \mathrm{Hom}_{\mathcal{C}}(T_1, X)$ given by

$$(T_2 \to X) \mapsto (T_1 \xrightarrow{f} T_2 \to X)$$

Our informal goal is as follows: knowing X is the same as knowing h_X. Let $f\colon X \to Y$ be a morphism in $\mathcal{C}$. Define

$$h_f\colon h_X \to h_Y$$

by

$$h_f(T)\colon h_X(T) \to h_Y(T)$$

$$(T \to X) \mapsto (T \to X \xrightarrow{f} Y).$$

We claim that $h_x \to h_y$ is a natural transformation of functors. Indeed, the diagram below commutes, for objects S, T in $\mathcal{C}$ and a morphism φ,

$$\begin{tikzcd}
h_X(S) \arrow[d, "h_f(S)"] & h_X(T) \arrow[l, "h_X(\varphi)"'] \arrow[d, "h_f(T)"] \\
h_Y(S) & h_Y(T) \arrow[l, "h_Y(\varphi)"']
\end{tikzcd}$$

Definition 1. The Yoneda embedding is the functor:

$$\eta\colon \mathcal{C} \to \mathrm{Hom}(\mathcal{C}^{op}, \mathrm{Sets})$$

$$X \mapsto h_X$$

Note that $\mathrm{Hom}(A, -,)$, $\mathrm{Hom}(-, B)$ are both covariant functors. Note that we haven't actually shown this is an embedding, i.e.

$$\mathrm{Hom} - \mathcal{C}(X, Y) \xrightarrow{\text{bijection}} \mathrm{Hom}(h_X, h_y)$$

$$f \mapsto h_f.$$

A key point here: the Yoneda embedding is **not** essentially surjective. Before proceeding to the proof, we present the idea of a representable functor.

Definition 2. A functor $h\colon \mathcal{C}^{op} \to \mathrm{Sets}$ is called **representable** if there exists an $X \in \mathcal{C}$ and a natural isomorphism $h \cong h_X$.

For example, let $\mathcal{C} = \text{Sets}$, and define

$$h\colon \text{Sets}^{op} \to \text{Sets}$$

$$T \mapsto \mathcal{P}(T)$$

where $\mathcal{P}(T)$ is the power set of T, and for $f\colon S \to T$, we have $\mathcal{P}(T) \to \mathcal{P}(S)$ given by $U \mapsto f^{-1}(U)$. Is h representable? Yes: let $X = \{0, 1\}$. Then $h \cong h_X$.

For a non-example, consider $\mathcal{C} = \text{Grp}, h\colon \text{Grp}^{op} \to \text{Sets}$ given by

$$G \mapsto \{H \leq G\}$$

and given a morphism $f\colon G \to H$, we have

$$h(f)\colon h(H) \to h(G)$$

$$\{K \leq H\} \mapsto \{f^{-1}(K) \leq G\}$$

Is h representable? If yes, let R represent it. Then $\text{Hom}(\mathbf{Z}/n\mathbf{Z}, R)$ is in natural bijection with subgroups of $\mathbf{Z}/n\mathbf{Z}$. Get contradiction with $n = 3$ as follows: $|\text{Hom}(\mathbf{Z}/3\mathbf{Z}, R)| = |R[3]| = 2$. So $R[3] = \{0, \sigma\}$. So we must either have $2\sigma = \sigma$ or $2\sigma = 0$. In either case, $\sigma = 0$ a contradiction.

Let X be an object of $\mathcal{C}$, $F\colon \mathcal{C}^{op} \to \text{Sets}$ a functor, and a morphism $f\colon U \to X$. Then we have a function α

$$\alpha\colon \text{Hom}(h_X, F) \to F(X)$$

$$(\tau\colon h_X \to F) \mapsto \tau(X)(\text{id}_X)$$

and a function

$$\beta\colon F(X) \to \text{Hom}(h_X, F)$$

$$\xi \mapsto [\tau_\xi\colon h_X \to F, \tau_\xi(U)(f) = F(f)(\xi)].$$

To be explicit about the source and the target for the function β, $\beta(\xi)(U) = \tau_\xi(U)\colon h_X(U) \to FU$. The following lemma will give rise to the Yoneda embedding.

Lemma 1. *Yoneda Lemma α and β are bijections of sets, with $\alpha \circ \beta = \text{id}_{F(X)}$, $\beta \circ \alpha = \text{id}_{\text{Hom}(h_X, F)}$.*

Proof. We have, for $\xi \in F(X)$,

$$(\alpha \circ \beta)(\xi) = \alpha(\tau_\xi) = \tau_\xi(X)(\text{id}_X) = F(\text{id}_X)(\xi) = \xi$$

So $\alpha \circ \beta = \mathrm{id}_{F(X)}$. Conversely,

$$\begin{aligned}(\beta \circ \alpha)(\tau) &= \beta(\tau(X)(\mathrm{id}_X)) \\ &= \tau_{\tau(X)(\mathrm{id}_X)} \colon h_X \to F \\ &\quad [\tau_{\tau(X)(\mathrm{id}_X)}(U)(U \xrightarrow{f} X) = F(f)(\tau(X)(\mathrm{id}_X))]\end{aligned}$$

We would like to show that $F(f)(\tau(X)(\mathrm{id}_X)) = \tau(U)(f)$. Indeed, we have the following commutative diagram, for $f \colon U \to X$,

$$\begin{tikzcd} h_X(U) \arrow[d, "\tau(U)"] & h_X(X) \arrow[l, "h_X(f)"'] \arrow[d, "\tau(X)"] \\ F(U) & F(X) \arrow[l, "F(f)"'] \end{tikzcd}$$

Chasing the element $\mathrm{id}_X \in h_X(X)$ both ways around the diagram gives

$$\tau(U)(h_X(f)(\mathrm{id}_X)) = F(f)(\tau(X)(\mathrm{id}_X))$$

$$\implies F(f)(\tau(X)(\mathrm{id}_X)) = \tau(U)(f)$$

Since the choice of U, f was arbitrary, it follows that $\beta \circ \alpha = \mathrm{id}_{\mathrm{Hom}(h_X, F)}$.

□

To prove the Yoneda embedding, we apply Yoneda's lemma.

2 9/2/2015: Universal objects

Lemma 2. The Yoneda Embedding *Let $X, Y \in \mathcal{C}$. Then*

$$\mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}(h_X, h_Y)$$

$(f \colon X \to Y) \mapsto (h_f \colon h_X \to h_Y, h_f(C) \colon h_X(C) \to h_Y(C)$ *given by* $(g \colon C \to X) \mapsto (f \circ g \colon C \to X \to Y))$ *is a bijection.*

Proof. Just apply Yoneda's Lemma with $F = h_Y$. □

The following is a corollary of Yoneda.

Corollary 1.

$$X \cong Y \iff h_X \cong h_Y.$$

Let us consider some examples from scheme theory. Let $\Gamma\colon \mathrm{Sch} \to \mathrm{Set}$ be given by

$$\Gamma(T) =: \Gamma(T, \mathcal{O}_T)$$

where $\mathcal{O}_T$ is the structure sheaf.

Is Γ representable? Yes. Let $X = \mathrm{Spec}(\mathbf{Z}[t])$. Then any morphism of schemes $T \to \mathrm{Spec}(\mathbf{Z}[t])$ is determined by the induced map on the global ring of functions:

$$\mathbf{Z}[t] \to \mathcal{O}_T(T)$$

and

$$\mathrm{Hom}(\mathbf{Z}[t] \to \mathcal{O}_T) \cong \mathcal{O}_T(T) = \Gamma(T, \mathcal{O}_T)$$

in the category of rings. Thus,

$$\mathrm{Hom}_{\mathrm{Sch}}(T, X) \xrightarrow{\text{bij}} \Gamma(T, \mathcal{O}_T).$$

Another example from scheme theory is the functor

$$\Gamma^{\times}\colon \mathrm{Sch} \to \mathrm{Set}$$

given by

$$T \mapsto \Gamma(T, \mathcal{O}_T)^{\times}$$

This $\Gamma^{\times}$ is again representable, for similar reasons, by $X = \mathrm{Spec}(\mathbf{Z}/(xy-1))$.

Recall that an *elliptic curve* is a proper smooth morphism of schemes $\pi\colon E \to S$ whose geometric fibers are connected curves of genus 1 together with a section $\sigma\colon S \to E$ (reminder: geometric fiber at a pony $p \in S$ is $E \times_S \mathrm{Spec}(\kappa(p))$, where $\kappa(p)$ is the function field at p).

We now define a functor

$$\mathcal{M}\colon \mathrm{Sch} \to \mathrm{Set}$$

$$S \mapsto \{\text{Elliptic curves } E/S\}/\sim$$

Note that a morphism $S_1 \to S_2$ induces a morphism $\mathcal{M}(S_2) \to \mathcal{M}(S_1)$, by pullback: $E/S_2 \to (E \times_{S_2} S_1)/S_1$ Is $\mathcal{M}$ representable by a scheme? The answer will turn out to be no.

Definition 3. Let $F\colon \mathcal{C}^{op} \to \mathrm{Set}$ be a functor. A universal object for F is a pair (X, ξ), where X is an object of $\mathcal{C}$, $\xi \in F(X)$ with the following universal property: For each pair (T, σ) where T is an object of $\mathcal{C}$ and $\sigma \in F(T)$, there is a unique morphism $f\colon T \to X$ such that $(F(f))(\xi) \to \sigma \in F(T)$

Proposition 1. $F\colon \mathcal{C}^{op} \to \mathrm{Set}$ *is representable iff there is a universal object for* F.

Proof. ($\Rightarrow$) Let X represent F. Then there is a natural isomorphism of functors $\Phi\colon h_X \to F$. We claim that $(X, \Phi(x)(\mathrm{id}_X))$ is a universal object. To show this, let (T, σ) be any pair, with $\sigma \in F(T)$. Then

$$\Phi(T)\colon h_X(T) \to F(T)$$

is an isomorphism. Let $f = (\Phi(T))^{-1}(\sigma)$. Then $f\colon T \to X$, and we have a commuting diagram from naturality

$$\begin{tikzcd}
h_X(X) \arrow[r, "h_X(f)"] \arrow[d, "\Phi(x)"] & h_X(T) \arrow[d, "\Phi(T)"] \\
F(X) \arrow[r, "F(f)"] & F(T).
\end{tikzcd}$$

Chasing the element $\mathrm{id}_X \in h_X(X)$ around this diagram both ways gives

$$\Phi(T)(f) = F(f)(\Phi(X)(\mathrm{id}_X)).$$

Note that

$$\Phi(T)(f) = \Phi(T)((\Phi(T))^{-1}(\sigma)) = \sigma$$

so $(X, \Phi(X)(\mathrm{id}_X))$ is indeed a universal pair, and f was unique because $\Phi(T)$ is a bijection.

($\Leftarrow$) Let (X, ξ) be a universal object for F. We claim that X represents F. To see this, define

$$\Phi\colon h_X \to F$$

by

$$\Phi(T)(T \xrightarrow{f} X) = F(f)(\xi) \in F(T).$$

For each object T of $\mathcal{C}$, $\Phi(T)$ is a bijection since (X, ξ) is universal. It is easy to check that Φ is a natural transformation of functors, since F is a functor. □

3 9/4/2015: Moduli spaces and representability, Elliptic Curves

To recap the course so far - let $\mathcal{C}$ be a category. The Yoneda embedding is the functor

$$\mathcal{C} \to \mathrm{Hom}(\mathcal{C}^{op}, \mathrm{Set})$$

$$X \mapsto h_X$$

Let $F\colon \mathcal{C}^{op} \to \text{Set}$ is representable if and only if there exists a universal pair (X, ξ), with X an object of $\mathcal{C}, \xi F(X)$. In fact, $\xi = F(X)(\text{id}_X)$.

We define the functor

$$\mathcal{M}\colon \text{Sch} \to \text{Set}$$

$$S \mapsto \{\text{Elliptic curves } E/S\}/\sim$$

Definition 4. Let $F\colon \mathcal{C}^{op} \to \text{Set}$. Then a **fine moduli space for** F is an X that represents F.

Note this automatically comes with a universal pair, and is unique up to unique isomorphism.

If $\mathcal{M}$ is representable by a scheme M, then there exists a universal object E^{univ}/M, which is an elliptic curve. Every elliptic curve E/s arises from E^{univ}, i.e. given any E/S, there is a section $S \to M$ and the fibered product:

$$\begin{tikzcd}
E = E \times_M S \arrow[r] \arrow[d] & E^{univ} \arrow[d] \\
S \arrow[r] & M
\end{tikzcd}.$$

Now, we sketch that $\mathcal{M}$ is not representable by a scheme. Since not everyone in the audience is comfortable with schemes, this argument has been simplified, so is not strictly correct. First, fix S a scheme, E a fixed elliptic curve. Suppose that in the fibered square below, the bottom map is the constant map. The bottom map is exactly what determines the elliptic curve E in the fiber. So the "fibered product is trivial" (sketchy). Now, view S^1 as $[0,1]/\sim$. Let E be an elliptic curve over $\mathbf{C}$ with nontrivial automorphism $\varphi\colon E \to E$. Define $\{E_\lambda\}_{\lambda \in [0,1]}$ by $E_\lambda = E$, then glue the endpoints using φ. Then $\{E_\lambda\} \to [0,1]$ defines

$$\begin{tikzcd}
\{E_\lambda\} \arrow[r] \arrow[d] & E^{univ} \arrow[d] \\
{[0,1]/\sim} \arrow[r] & M
\end{tikzcd}.$$

But then the bottom map is constant again, and so upper left scheme is trivially fibered, which is a contradiction.

So, how can we fix this problem for the nonexistence of fine moduli? One approach is to use stacks, which enlarge the category of schemes so that $\mathcal{M}$ is representable. Another way is to use extra data:

$$\mathcal{M}_{\Gamma(n)}\colon \text{Sch} \to \text{Set}$$

$$S \to \{\text{Elliptic curves } E/S, \varphi\colon (\mathbf{Z}/n\mathbf{Z})^2 \to E[N]\}$$

where a morphism $(E, \varphi) \to (E', \varphi')$ is the data of a morphism $E' \to E$ such that

$$\begin{tikzcd}
(\mathbf{Z}/N/Z)^2 \arrow[r, "\varphi'"] \arrow[dr, "\varphi"] & E'[N] \arrow[d] \\
 & E[N]
\end{tikzcd}$$

It is a theorem of Mumford or Serre that for $N \geq 3$, $\mathcal{M}_{\Gamma(N)}$ is representable.

There is one more way to get moduli space. This is the moduli space we study in this course: the **coarse moduli space**. M is a coarse module space of F if there exists a natural transformation $\Phi\colon F \to h_M$ such that $F(\mathrm{Spec}(\mathbf{C})) \to h_M(\mathrm{Spec}(\mathbf{C}))$ is a bijection., and such that for any other $\Phi'\colon F \to h_{M'}$, the diagram below is universal

$$\begin{tikzcd}
F \arrow[r, "\Phi'"] \arrow[dr, "\Phi"] & h_{M'} \\
 & h_M \arrow[u, "\exists!"]
\end{tikzcd}$$

Let k be an arbitrary field. An **elliptic curve** is a nonsingular projective algebraic curve of genus 1 that is geometrically connected with a point $\epsilon\colon \mathrm{Spec}(k) \to E$.

Theorem 1. *Every elliptic curve in* $\mathrm{char}(k) \neq 2, 3$ *can be put in the form below:*

Theorem 2. *Let $E/\mathbf{C}$ be an elliptic curve. Then*

$$E \xrightarrow{\sim} \mathbf{C}/\Lambda$$

where Λ is a full lattice in $\mathbf{C}$, i.e. $\Lambda = \langle \omega_1, \omega_2 \rangle$, i.e. Λ is a rank 2 $\mathbf{Z}$-module with $\Lambda \otimes_{\mathbf{Z}} \mathbf{R} = \mathbf{C}$.

In Mumford, it is sketched that a curve E is realized as the compact complex Lie group $(\mathbf{C}/\Lambda)$. Briefly, $\mathbf{C} = T_E$. Since E is a compact complex Lie group, look at the exponential map $\exp\colon \mathbf{C} \to E$ surjects, and $\ker \exp = \Lambda$.

For the other direction, $\mathbf{C}/\Lambda$ corresponds to E as follows: Define

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda^*} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

where $\Lambda^* = \Lambda \backslash \{0\}$. One can show that $\wp(z)$ converges uniformly on compact sets. Some calculus gives

$$\wp'_\Lambda(z) = -2 \sum_{\omega \in \Lambda^*} \frac{1}{(z-\omega)^3}$$

Then the lattice Λ is the set of periods for $\wp'_\Lambda(z)$, so that for all $\omega \in \Lambda$,

$$\wp'_\Lambda(z+\omega) = \wp'_\Lambda(z).$$

A more nontrivial result is that

$$\wp_\Lambda(z+\omega) = \wp_\Lambda(z)$$

, and all of this is to say that $\wp_\Lambda(z)$ and $\wp'_\Lambda(z)$ are *elliptic*. As such, they define meromorphic functions on the torus $\mathbf{C}/\Lambda$. As it turns out, if we let K be the set of meromorphic functions on $\mathbf{C}/\Lambda$, then

$$K = \mathbf{C}(\wp_\Lambda(z), \wp'_\Lambda(z)).$$

One can check using some basic elliptic function theory that if we let $y = \wp'_\Lambda(z), x = \wp_\Lambda(z)$, then

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

where g_2, g_3 come from normalized Eisenstein series. This in fact gives a complex analytic diffeomorphism of complex manifolds

$$\mathbf{C}/\Lambda \to E = \{(x,y) \in \mathbf{C}^2 \colon y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)\}$$

$$z \mapsto (\wp_\Lambda(z), \wp'_\Lambda(z)).$$

4 9/9/2015: Isogenies

Recap: let $\mathcal{M}$ be the moduli of elliptic curves. It is not represented by a scheme, but is a stack. We study instead just the $\mathbf{C}$ points of the moduli, and this is represented.

Also, an elliptic curve $/\mathbf{C}$ corresponds to $\mathbf{C}/\Lambda$, Λ a lattice.

Proposition 2. *Let $\varphi \colon \mathbf{C}/\Lambda \to \mathbf{C}/\Lambda'$ be a holomorphic map. Then there exist $m, b \in \mathbf{C}$ with $m\Lambda' \subseteq \Lambda'$ and*

$$\varphi(z+\Lambda) = mz + b + \Lambda'.$$

φ is invertible if and only if $m\Lambda = \Lambda'$.

Proof. φ lifts to

$$\begin{tikzcd}
\mathbf{C} \arrow[r, "\tilde{\varphi}"] \arrow[d] & \mathbf{C} \arrow[d] \\
\mathbf{C}/\Lambda \arrow[r, "\varphi"] & \mathbf{C}/\Lambda'.
\end{tikzcd}$$

because $\mathbf{C}$ is a universal cover. For any $\lambda \in \Lambda$, consider $f_\lambda \colon \mathbf{C} \to \mathbf{C}$ defined by

$$f_\lambda(z) = \tilde{\varphi}(z + \Lambda) - \tilde{\varphi}(z).$$

Push z around the diagram

$$\begin{tikzcd}
\mathbf{C} \arrow[r, "f_\lambda"] \arrow[d] & \mathbf{C} \arrow[d] \\
\mathbf{C}/\Lambda \arrow[r, "\overline{f_\lambda}"] & \mathbf{C}/\Lambda'.
\end{tikzcd}$$

to get $f_\lambda(z) \in \Lambda'$. Therefore, f_λ is constant. Thus,

$$\tilde{\varphi}'(z + \lambda) = \tilde{\varphi}(z)$$

meaning $\tilde{\varphi}'(z)$ is Λ-periodic. Thus, $\tilde{\varphi}'(z)$ is holomorphic and bounded, and thus constant, so

$$\tilde{\varphi} = mz + b.$$

Note that $m\Lambda \subset \Lambda'$ since $\tilde{\varphi}$ reduces to $\mathbf{C}/\Lambda \to \mathbf{C}/\Lambda'$.

Conversely, if $m\Lambda \subsetneq \Lambda'$, there exists $z' \in \Lambda'$ with $\frac{z'}{m} \notin \Lambda$. Then

$$\varphi(\frac{z}{m} + \Lambda) = b + \Lambda' = \varphi(\Lambda)$$

so φ is not injective. □

If $m\Lambda = \Lambda'$, then $\Lambda = m^{-1}\Lambda'$ induces

$$\mathbf{C}/\Lambda' \to \mathbf{C}/\Lambda$$

$$z \mapsto \frac{z - b}{m}$$

the inverse of φ.

Corollary 2. $\varphi\colon \mathbf{C}/\Lambda \to \mathbf{C}/\Lambda'$, $\varphi(z + \Lambda) = mz + b + \Lambda'$. *Then the following are equivalent:*

(1) φ is a group homomorphism.

(2) $b \in \Lambda$.

(3) $\varphi(0) = 0$

Proof. (1) $\iff$ (2): $\varphi(z + w + \Lambda) = m(z + w) + b + \Lambda$. Then

$$\varphi(z) + \varphi(w) = mz + bmw + b + \Lambda'$$

and these are equal if and only if $b + \Lambda' = b + b + \Lambda' \iff b \in \Lambda'$.

(2) $\iff$ (3) is clear □

Corollary 3. *A nonzero homomorphism* $\varphi\colon \mathbf{C}/\Lambda \to \mathbf{C}/\Lambda'$ *is surjective with finite kernel, often called an isogeny.*

Proof. Write $\varphi(z + \Lambda) = mz + \Lambda'$, $m\Lambda \subset \Lambda'$. Now

$$\varphi \not\equiv 0 \implies \ker\varphi \text{ is discrete.}$$

Since $\mathbf{C}/\Lambda'$ is compact, $\ker\varphi$ is finite. $\mathbf{C}/\Lambda$ is connected and compact, so $\varphi(\mathbf{C}/\Lambda)$ is connected and compact. Then the Riemann mapping theorem from complex analysis shows that $\varphi(\mathbf{C}/\Lambda)$ is open, and thus φ is surjective.

□

For example, $[n]\colon \mathbf{C}/\Lambda \to \mathbf{C}/\Lambda$ given by

$$z \mapsto nz + \Lambda$$

has

$$\mathbf{C}/\Lambda[n] := \ker([n]) = \{z + \Lambda \mid nz \in \Lambda\}.$$

As abstract groups,

$$(1/n)\Lambda/\Lambda \cong (1/n)\mathbf{Z}^2/\mathbf{Z}^2 \cong (\mathbf{Z}/n\mathbf{Z})^2$$

As another example, let $C \leq (\mathbf{C}/\Lambda)[n]$, $C \cong \mathbf{Z}/n\mathbf{Z}$. Then identify C with $\Lambda \subset C \subset \mathbf{C}$. C is a lattice. Then

$$\pi\colon \mathbf{C}/\Lambda \to \mathbf{C}/C$$

$$z + \Lambda \mapsto z + C$$

and we see $\ker\pi = C/\Lambda$. π is called a *cyclic quotient.*

Proposition 3. *Every isogeny is the composition of multiplication by* N *followed by a cyclic quotient.*

Proof. Let $\varphi(z+\Lambda) = nz + \Lambda'$, $m\Lambda \subset \Lambda'$. Set $K = \ker\varphi = m^{-1}\Lambda'/\Lambda$. Let $N = |K|$. Then $K \subset \ker([N]) \cong (\mathbf{Z}/N\mathbf{Z})^2$. By the fundamental theorem for finitely generated abelian groups, $K \cong (\mathbf{Z}/n\mathbf{Z}) \times (\mathbf{Z}/nn'/\mathbf{Z})$. Viewing K as $\Lambda \subset K \subset \mathbf{C}$, note that $\Lambda \subset nK$ and $mK = \Lambda'$. We now claim that φ is the composition

$$\mathbf{C}/\Lambda \xrightarrow{[n]} \mathbf{C}/\Lambda \xrightarrow{\pi} \mathbf{C}/nK \xrightarrow{\cong} \mathbf{C}/\Lambda'$$

where the last map is

$$z + nK \mapsto (m/n)z + (m/n)nK.$$

The last map is injective: $(m/n)z \in mK = \Lambda' \iff z/n \in K \iff z \in nK$.

Since $[n]K = nK$, we have $nK/\Lambda \cong \mathbf{Z}/n'\mathbf{Z}$. Thus, π is a cyclic quotient. Tracing the maps through, we get $z \mapsto (m/n)(nz) + (m/n)nK = mz + mK = mz + \Lambda'$. □

Proposition 4. *Isognies define an equivalence relation. That is, if $\varphi\colon \mathbf{C}/\Lambda \to \mathbf{C}/\Lambda'$ is an isogeny, then there exists a "dual isogeny" $\hat{\varphi}\colon \mathbf{C}/\Lambda' \to \mathbf{C}/\Lambda$ such that*

$$\varphi \circ \hat{\varphi} = \hat{\varphi} \circ \phi = [n],$$

$$[n] = \deg\varphi = |\ker\varphi|.$$

Proof. Let $\varphi(z+\Lambda) = mz + \Lambda'$, $m\Lambda \subset \Lambda'$. Write

$$\Lambda'/m\Lambda \cong (\mathbf{Z}/n_1\mathbf{Z}) \times (\mathbf{Z}/n_2\mathbf{Z}).$$

Let $\langle \omega_1, \omega_2 \rangle$ be a basis of Λ', so

$$\langle \overline{\omega_1}, \overline{\omega_2} \rangle \in (\mathbf{Z}/n_1\mathbf{Z}) \times (\mathbf{Z}/n_2\mathbf{Z}).$$

Choose $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$ with

$$a\overline{\omega_1} + b\overline{\omega_2} = (1,0)$$

$$c\overline{\omega_1} + d\overline{\omega_2} = (0,1).$$

Then $n_1\omega_1 \in m\Lambda, n_2\omega_2 \in m\Lambda$. So

$$\langle n_1\omega_1, n_2\omega_2 \rangle \subset m\Lambda \subset \Lambda'.$$

Since $\#(\Lambda'/\langle n_1\omega_1, n_2\omega_2\rangle) = \#(\Lambda'/m\Lambda) = n_2n_2$, we get $m\Lambda =< n_1\omega_1, n_2\omega_2 >$ So $n_1n_2\Lambda' \subset m\Lambda$, $(n_1n_2)/m\Lambda' \subset \Lambda$. Define

$$\hat{\varphi}\colon \mathbf{C}/\Lambda' \to \mathbf{C}/\Lambda.$$

$$z + \Lambda' \mapsto (n_1n_2)/m \cdot z + \Lambda$$

□

5 9/11/2015: Constructing a modular curve

In this section, we write $\Gamma = SL_2(\mathbf{Z}) = \Gamma(1)$.

Let

$$Y(1) = \{\text{elliptic curves over } \mathbf{C}\}/\text{iso}.$$

Let $\Lambda = \langle \omega_1, \omega_2 \rangle \subset \mathbf{C}$. There is an isomorphism

$$\mathbf{C}/\Lambda \simeq \mathbf{C}/\langle \frac{\omega_1}{\omega_2}, 1 \rangle.$$

If $\mathrm{Im}(\frac{\omega_1}{\omega_2}) < 0$, replace it with $-\frac{\omega_1}{\omega_2}$. So we may now assume that $\tau = \frac{\omega_1}{\omega_2}$, that $\mathrm{Im}(\tau) > 0$ and we, up to isomorphism,

$$\Lambda = \langle \tau, 1 \rangle.$$

If $m \in \mathbf{C}^\times$, $m\Lambda = \langle m\tau, m \rangle$, we normalize and get up to isomorphism that $\langle \tau, 1 \rangle$. So the action by $\mathbf{C}^\times$ is trivial.

For $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \Lambda = \Lambda$ and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \langle a\tau + b, c\tau + d \rangle.$$

Normalizing, we see this lattice is

$$\langle \frac{a\tau + b}{c\tau + d}, 1 \rangle.$$

An easy exercise shows that $\mathrm{Im}(\frac{az+b}{cz+d}) = \frac{\mathrm{Im}(z)}{|cz+d|^2}$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$.

Proposition 5. *$Y(1) \xrightarrow{bin} SL_2(\mathbf{Z}) \backslash \mathcal{H}$, where $\mathcal{H} = \{\tau \in \mathbf{C} \,\big|\, \mathrm{Im}\tau > 0\}$.*

Proof. Let $\Lambda = \langle \omega_1, \omega_2 \rangle, \Lambda' = \langle \omega_1', \omega_2' \rangle$ with

$$\frac{\omega_1}{\omega_2}, \frac{\omega_1'}{\omega_2'} \in \mathcal{H}.$$

Then we claim

$$\Lambda = \Lambda' \iff \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

One direction is obvious ($\Leftarrow$). To prove $\Rightarrow$,Write

$$\omega_2' = a\omega_1 + b\omega_2$$

$$\omega_2' = c\omega_1 + d\omega_2$$

$$\omega_1 = a'\omega_1' + b'\omega_2'$$

$$\omega_2' = c'\omega_1' + d'\omega_2'$$

with $a, b, c, d, a', b', c', d' \in \mathbf{Z}$. Then

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

which means that

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \mathrm{id}$$

and so

$$\det \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm 1.$$

It must be 1 since

$$\omega_1'/\omega_2' = \frac{a\omega_1/\omega_2) + b}{c(\omega_1/\omega_2) + d}$$

$$= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}.$$

By the easy exercise mentioned above, the determinant is 1. □

Insert picture for fundamental domain of $\Gamma(1)$.

Proposition 6. *$SL_2(\mathbf{Z})$ is generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.*

Proof. Set

$$\Gamma = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \rangle.$$

Note that

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in \Gamma$$

for all $n \in \mathbf{Z}$.

Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$. Note that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & nc + d \end{pmatrix}$$

so if $c \neq 0$, then we can find n so that we may assume $|d| \leq |c|/2$. Now

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}.$$

By applying $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, we may assume that $|c| \leq d/2$. Do this repeatedly until $c = 0$. So we may assume our matrix is of the form

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

with $a = d = \pm 1$, b arbitrary, with $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \text{id}$. So we can assume that $a = d = 1$, and $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in \Gamma$. □

6 9/13/2015: Congruence subgroups and moduli

A **congruence subgroup** $\Gamma \subseteq SL_2(\mathbf{Z})$ is a subgroup of $SL_2(\mathbf{Z})$ defined by congruence conditions. That is, Γ is the pre image of some subgroup of $SL_2(\mathbf{Z}/N\mathbf{Z})$ under the $\mod N$ reduction $SL_2(\mathbf{Z}) \to SL_2(\mathbf{Z}/N\mathbf{Z})$. We define $\Gamma(N)$ to be the kernel of $SL_2(\mathbf{Z}) \to SL_2(\mathbf{Z}/N\mathbf{Z})$.

Definition 5. The smallest N such that $\Gamma(N) \subseteq \Gamma$ is called the **level** of Γ.

Other key examples are

$$\Gamma_0(N) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Bigg| \, c \equiv 0 \mod N \}$$

$$\Gamma_1(N) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Bigg| \, c \equiv 0, a \equiv d \equiv 1 \mod N \}.$$

We can form

$$\Gamma(N)\backslash\mathbf{H} \to \Gamma_1(N)\backslash\mathbf{H} \to \Gamma_0(N)\backslash\mathbf{H}$$

Note that one can form a directed system $\Gamma(p^{m+1})\backslash\mathbf{H} \to \Gamma(p^m)\backslash\mathbf{H}$ to get a limit $\varprojlim_m \Gamma(p^n)\backslash\mathbf{H}$. This is sort of realized as one of Scholze's perfectoid spaces.

We have surjections

$$\Gamma_1(N) \to \mathbf{Z}/N\mathbf{Z}$$

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

$$\ker = \Gamma(N)$$

and

$$\Gamma_0(N) \to (\mathbf{Z}/N\mathbf{Z})^\times$$

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

$$\ker = \Gamma_1(N)$$

Therefore,

$$\Gamma_1(N)/\Gamma(N) \cong \mathbf{Z}/N\mathbf{Z}$$

$$\Gamma_0(N)/\Gamma_1(N) \cong (\mathbf{Z}/N\mathbf{Z})^\times$$

We now define the moduli

Definition 6. Define the set

$$S_0(N) = \{(E,C) \mid E \text{ is an elliptic curve}/\mathbf{C}, C \subset E[N]\text{is a cyclic subgroup of order } N\}/\sim.$$

A morphism $(E,C) \to (E',C')$ is the data of a homomorphism $\varphi\colon E \to E'$ of elliptic curves such that $\varphi\colon E \to E'$ and such that $\varphi(C) \subseteq C'$.

$$S_1(N) = \{(E,Q) \mid E \text{ is an elliptic curve}/\mathbf{C}, Q \in E[N] \text{ is of order } N\}/\sim$$

and morphisms are given by

$$(E,Q) \to (E',Q')$$

as the data of a homomorphism of elliptic curves $E \to E'$ and $\varphi(Q) = Q'$.

We need to discuss the Weil pairing. Let $E = \mathbf{C}/\Lambda, \Lambda = \langle \omega_1, \omega_2 \rangle$, $\omega_1/\omega_2 \in \mathbf{H}$. Then

$$E[N] = \{\frac{\omega_1}{N} + \Lambda\} \times \{\frac{\omega_2}{N} + \Lambda\}.$$

Define

$$e_N\colon E[N] \times E[N] \to \mu_N = N\text{-th roots of unity}$$

as follows. Choose a matrix $M \in M_2(\mathbf{Z})$ such that

$$\begin{pmatrix} P \\ Q \end{pmatrix} = M \begin{pmatrix} \omega_1/N \\ \omega_2/N \end{pmatrix}.$$

Then $e_N(P,Q) = e^{\frac{2\pi i \det M}{N}}$.

We claim that e_N is independent of the choice of ω_1, ω_2, as long as $\frac{\omega_1}{\omega_2} \in \mathbf{H}$. Let ω_1', ω_2' be some other basis for Λ with $\omega_1'/\omega_2' \in \mathbf{H}$. Then

$$\omega_1 = a\omega_1' + b\omega_2'$$

$$\omega_2 = c\omega_1' + d\omega_2'$$

with $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$. Then

$$\begin{pmatrix} P \\ Q \end{pmatrix} = M \begin{pmatrix} a\omega_1' + b\omega_2' \\ c\omega_1' + d\omega_2' \end{pmatrix}$$

$$= M \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1'/N \\ \omega_2'/N \end{pmatrix}$$

which gives

$$\det M = \det(M \begin{pmatrix} a & b \\ c & d \end{pmatrix}).$$

Note that $e_N(P,Q)^N = 1$, and that $e_N(P,Q)$ is a primitive N-th root of unity if and only if $\langle P, Q \rangle = E[N]$.

Definition 7.

$$S(N) = \{(E,P,Q) \,\big|\, E \text{ elliptic curve}/\mathbf{C}, P, Q \in E[N] \text{ such that} e_N(P,Q) = e^{2\pi i/N}\}/\sim$$

with morphisms

$$(E,P,Q) \to (E,P',Q')$$

given by the data as expected, i.e. $\varphi\colon E \to E', \varphi(P) = P', \varphi(Q) = Q'$.

Here is an alternate description of $S(N)$ which works more generally. Choosing an N-th primitive root of unity is the same as giving

$$\mathbf{Z}/N\mathbf{Z} \to \mu_N$$

$$1 \mapsto \zeta_N.$$

Then

$$S(N) = \{(E,\alpha) \,\big|\, E \text{ elliptic curve } /\mathbf{C}, \alpha\colon (\mathbf{Z}/N\mathbf{Z})^2 \xrightarrow{\simeq} E[N]\}$$

where

$$\begin{tikzcd}
(\mathbf{Z}/N\mathbf{Z})^2 \times (\mathbf{Z}/N\mathbf{Z})^2 \arrow[r] \arrow[d, "\alpha\times\alpha"] & \mathbf{Z}/N\mathbf{Z} \arrow[d, "\simeq"] \\
E[N] \times E[N] \arrow[r] & \mu_N
\end{tikzcd}$$

The following theorem is the key to constructing our moduli, will be one of the centerpieces of the course:

Theorem 3. *Let $N \in \mathbf{Z}_{>0}$.*

(a)

$$S_0(N) = \{(\mathbf{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau\rangle) \mid \tau \in \mathbf{H}\}/\sim$$

where $(\mathbf{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau\rangle) \sim (\mathbf{C}/\Lambda_{\tau'}, \langle 1/N + \Lambda_{\tau'}\rangle)$ if and only if $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$.

(b)

$$S_1(N) = \{(\mathbf{C}/\Lambda_\tau, 1/N + \Lambda_\tau) \mid \tau \in \mathbf{H}\}/\sim$$

where $(\mathbf{C}/\Lambda_\tau, 1/N + \Lambda_\tau) \sim (\mathbf{C}/\Lambda_{\tau'}, 1/N + \Lambda_{\tau'})$ if and only if $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$.

(c)

$$S(N) = \{(\mathbf{C}/\Lambda_\tau, 1/N + \Lambda_\tau, \tau/N + \Lambda_\tau) \mid \tau \in \mathbf{H}\}/\sim$$

where $(\mathbf{C}/\Lambda_\tau, 1/N + \Lambda_\tau, \tau/N + \Lambda_\tau) \sim (\mathbf{C}/\Lambda_{\tau'}, 1/N + \Lambda_\tau, \tau/N + \Lambda_\tau)$ if and only if $\Gamma(N)\tau = \Gamma(N)\tau'$.

We will see bijections

$$S_0(N) \to Y_0(N) = \Gamma_0(N)\backslash\mathbf{H}$$

$$S_1(N) \to Y_1(N) = \Gamma_1(N)\backslash\mathbf{H}$$

$$S(N) \to Y(N) = \Gamma(N)\backslash\mathbf{H}$$

and furthermore, each of $Y_0(N), Y_1(N), Y(N)$ will be given the structure of a complex manifold. Eventually, we will compactify these manifolds.

7 9/16/2015: Modular curves as parametrizing spaces

We wish to prove Theorem 3. We prove only (c), as it is similar to (a), and (b) is in the book.

Proof. **(Theorem 3 (c)):** We want to show

$$\{(\mathbf{C}/\Lambda_\tau, 1/N + \Lambda_\tau, \tau/N + \Lambda_\tau) \mid \tau \in \mathbf{H}\}/\sim \to \ S(N)$$

is well defined. Let $\tau' \in \Gamma(N)\cdot\tau$, say $\tau' = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\tau$. We need to construct an isomorphism

$$\mathbf{C}/\Lambda_{\tau'} \to \mathbf{C}/\Lambda_\tau$$

sending

$$\tau'/N + \Lambda_{\tau'} \to \tau/N + \Lambda_\tau$$

$$1/N \to \Lambda_{\tau'} \to 1/N + \Lambda_\tau$$

Set $m = c\tau + d$. We claim:

$$[m]\colon \mathbf{C}/\Lambda_{\tau'} \to \mathbf{C}/\langle a\tau + b, c\tau + d\rangle = \mathbf{C}/\Lambda_\tau$$

is an isomorphism. Note:

$$m\tau' = (c\tau + d)\begin{pmatrix} a & b \\ c & d \end{pmatrix}\tau = a\tau + b$$

$$m \cdot 1 = c\tau + d$$

Now

$$[m](\tau'/N + \Lambda_{\tau'}) = \frac{a\tau + b}{N} + \Lambda_\tau$$

$$[m](1/N + \Lambda_{\tau'}) = \frac{c\tau + d}{N} + \Lambda_\tau.$$

Since $a \equiv d \equiv 1 \mod N$ and $b \equiv c \equiv 0 \mod N$,

$$\frac{a\tau + b}{N} + \Lambda_\tau = \tau/N + \Lambda_\tau$$

$$\frac{c\tau + d}{N} + \Lambda_\tau = 1/N + \Lambda_\tau$$

which proves well-definedness.

Now to prove injectivity, suppose $(\mathbf{C}/\Lambda_\tau, \tau/N + \Lambda_\tau, 1/N + \Lambda_\tau) \xrightarrow{\sim} (\mathbf{C}/\Lambda_{\tau'}, \tau'/N + \Lambda_{\tau'}, 1/N + \Lambda_{\tau'})$. We'll show that $\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\tau'$. for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(N)$. There exists $m \in \mathbf{C}^\times$ inducing $[m]\colon \mathbf{C}/\Lambda_\tau \to \mathbf{C}/\Lambda_{\tau'}$, sending

$$m(\tau/N + \Lambda_\tau) = \tau'/N + \Lambda_{\tau'}$$

$$m(1/N + \Lambda_\tau) = 1/N + \Lambda_{\tau'}$$

where $m\Lambda_\tau = \Lambda_{\tau'}$.

Now

$$\begin{pmatrix} m\tau \\ m1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \tau' \\ 1 \end{pmatrix}$$

for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$. Since

$$m\tau/N = \frac{a\tau' + b}{N} = \frac{\tau'}{N} \mod \Lambda_{\tau'}$$

, $a \equiv 1 \mod N, b \equiv 0 \mod N$. Similarly,

$$m \cdot 1/N = \frac{c\tau' + d}{N} = \frac{1}{N} \mod \Lambda_{\tau'},$$

so $c \equiv 0 \mod N, d \equiv 1 \mod N$. Thus, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(N)$.

From $m\tau = a\tau' + b$, $m \cdot 1 = c\tau' + d$, we got

$$\tau = m\tau/m = \frac{a\tau' + b}{c\tau' + d} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau'.$$

Finally, we prove surjectivity. Given (E, P, Q) with $e_N(P, Q) = e^{2\pi i/N}$, set $E \cong \mathbf{C}/\Lambda_{\tau'}$. Then

$$\begin{pmatrix} P \\ Q \end{pmatrix} = M \begin{pmatrix} \tau'/N \\ 1/n \end{pmatrix}$$

for some $M \in M_2(\mathbf{Z}/N\mathbf{Z})$. Since $e_N(P, Q) = e^{2\pi i/N}$, we must have

$$e^{2\pi i \det M/N} = e^{2\pi i/N}$$

$$\implies \det M = 1.$$

Thus, $M \in SL_2(\mathbf{Z}/N/\mathbf{Z})$. Now $SL_2(\mathbf{Z}) \to SL_2(\mathbf{Z}/N\mathbf{Z})$ is surjective. So choose a lift for M to $SL_2(\mathbf{Z})$, say $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Set $\tau = M\tau'$, $m = c\tau' + d$. Note that

$$m\tau = mM\tau' = a\tau' + b.$$

Thus,

$$[m] \colon \mathbf{C}/\Lambda_\tau \xrightarrow{\sim} \mathbf{C}/\langle a\tau' + b, c\tau' + d\rangle = \mathbf{C}/\Lambda_{\tau'}$$

sends

$$\begin{aligned} \tau/N + \Lambda_\tau &\mapsto \frac{a\tau' + b}{N} + \Lambda_{\tau'} = P \\ 1/N + \Lambda_\tau &\mapsto \frac{c\tau' + d}{N} + \Lambda_{\tau'} = Q. \end{aligned}$$

□

Let us now give our modular curves structure as Riemann surfaces. Let $\Gamma \subset SL_2(\mathbf{Z})$ be a congruence subgroup.

$$Y(\Gamma) = \{\Gamma\tau \mid \tau \in \mathbf{H}\} = \Gamma\backslash\mathbf{H}\}.$$

Our goals are to give $Y(\Gamma)$ a complex structure as a manifold and to compactify to make it a Riemann surface.

First, we need to give $Y(\Gamma)$ a topology, which we choose to be the quotient topology:

$$\pi \colon \mathbf{H} \to \Gamma\backslash\mathbf{H}.$$

We declare that $V \subseteq Y(\Gamma)$ is open $\iff$ $\pi^1(V)$ is open in $\mathbf{H}$.

π is an open mapping. To see this, let $U \subseteq \mathbf{H}$ be open. Then $\pi^{-1}(\pi(U)) = \cup_{\gamma\in\Gamma}\gamma U$. Since $U \subseteq \mathbf{H}$ is open, we have $\gamma U \subseteq \mathbf{H}$ open. Thus, $\pi(\pi^{-1}(\pi(U))) = \pi(U)$ is open.

Another property: $\pi(U_1) \cap \pi(U_2) = \emptyset \iff \Gamma \cdot U_1 \cap U_2 = \emptyset$. The proof is easy. $\pi(U_1) \cap \pi(U_2) \neq \emptyset \iff$ there exists $\alpha \in U_1, \beta \in U_2, \gamma \in \Gamma$ such that $\gamma\alpha = \beta \iff (\Gamma U_1) \cap U_2 \neq \emptyset$.

8 9/18/2015: Topology of the modular curve

Today we will show that $\Gamma\backslash\mathbf{H}$ is Hausdorff.

Definition 8. A continuous action of a group G on a topological space X is properly discontinuous if, for each $x, y \in X$, there exists neighborhoods U_x, U_y such that there are only finitely many $g \in G$ with $g(U_x) \cap U_y \neq \emptyset$.

Proposition 7. *Let $\tau_1, \tau_2 \in \mathbf{H}$. Then there exists neighborhoods U_i of τ_i such that for all $\gamma \in \Gamma$, if $\gamma(U_1) \cap U_2 \neq \emptyset$, the $\gamma(\tau_1) = \tau_2$ (note $\tau_1 = \tau_2$ is allowed).*

Proof. Let U_i' be any open neighborhood of τ_i with compact closure. Our goal is to show: *for al but finitely many $\gamma \in SL_2(\mathbf{Z})$, $\gamma(U_1') \cap U_2' = \emptyset$.* An exercise from the book is: *For all but finitely many $(c, d) \in \mathbf{Z}^2$ with $gcd(c, d) = 1$, we have*

$$\sup\{\mathrm{Im}(\gamma(\tau))| \; \gamma \in SL_2(\mathbf{Z}), \gamma \begin{pmatrix} * & * \\ c & d \end{pmatrix}, \tau \in U_1'\} < \inf\{\mathrm{Im}(\tau) \mid \tau \in U_2'\}.$$

Let us prove this inequality. Set

$$y_1 = \inf\{\mathrm{Im}(\tau) \mid \tau \in U_1'\}$$

$$Y_1 = \sup\{\mathrm{Im}(\tau) \mid \tau \in U_1'\}$$

$$y_2 = \inf\{\mathrm{Im}(\tau) \mid \tau \in U_2'\}.$$

Using

$$\mathrm{Im}(\gamma(\tau)) = \frac{\mathrm{Im}\tau}{|c\tau + d|^2}$$

for $\tau \in U_1'$, we have

$$\frac{\mathrm{Im}\tau}{|c\tau+d|^2} \leq \frac{\mathrm{Im}\tau}{(c\mathrm{Re}\tau + d)^2 + c^2(\mathrm{Im}\tau)^2} \leq \frac{Y_1}{(c\mathrm{Re}\tau+d)^2}$$

and

$$\frac{\mathrm{Im}\tau}{|c\tau+d|^2} \leq \frac{\mathrm{Im}\tau}{(c\mathrm{Re}\tau + d)^2 + c^2(\mathrm{Im}\tau)^2} \leq \frac{1}{c^2 y_1}.$$

Thus,

$$\mathrm{Im}(\gamma\tau) \leq \min(\frac{Y_1}{(c\mathrm{Re}\tau+d)^2}, \frac{1}{c^2 y_1}).$$

So $\mathrm{Im}(\gamma\tau) < \inf\{\mathrm{Im}\tau \mid \tau \in U_2'\} = y_2$ for all but finitely many values of c (remember that y_2 is fixed here). For each such value of c in this exceptional set, there are only finitely many d that violate the desired inequality, since

$$\mathrm{Im}(\gamma\tau) \leq \frac{Y_1}{c\mathrm{Re}\tau + d^2}.$$

This completes the exercise.

So we now know that for all but finitely many $(c, d) \in \mathbf{Z}^2$ with $\gcd(c, d) = 1$, and all $\begin{pmatrix} * & * \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$,

$$\gamma(U_1) \cap U_2 = \emptyset.$$

But for any (c, d) with $\gcd(c, d) = 1$, we can write any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$ in the form

$$\begin{pmatrix} a+kc & b+kd \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}).$$

Thus, $\gamma(U_1') \cap U_2' = (\begin{pmatrix} a & b \\ c & d \end{pmatrix} U_1' + k) \cap U_2'$. Sicne there are finitely many $(a, b) \in \mathbf{Z}^2$ needed to write evey matrix $\begin{pmatrix} * & * \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$ as

$$\begin{pmatrix} * & * \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}, k \in \mathbf{Z}.$$

There are only finitely many $\gamma \in SL_2(\mathbf{Z})$ such that

$$\gamma(U_1') \cap U_2' \neq \emptyset.$$

Thus,

$$F := \{\gamma \in SL_2(\mathbf{Z}) \mid \gamma(U_1') \cap U_2' \neq \emptyset \text{ and } \gamma(\tau_1) \neq \tau_2\}$$

is finite. For each $\gamma \in F$, let $U_{1,r}$ and $U_{2,r}$ be disjoint open neighborhoods of $\gamma(\tau_1), \tau_2$ respectively. Set

$$U_1 = U_1' \cap (\bigcap_{\gamma \in F} \gamma^{-1}(U_{1,\gamma}))$$

$$U_1 = U_2' \cap (\bigcap_{\gamma \in F} U_{2,\gamma}).$$

Recall we want that if $\gamma U_1 \cap U_2 \neq \emptyset$, then $\gamma\tau_1 = \tau_2$. Suppose $\gamma U_1 \cap U_2 \neq \emptyset$. We need to show that $\gamma \neq F$. Suppose $\gamma \in F$. Then $\gamma(U_1) \subseteq U_{1,\gamma}$ and $U_2 \subseteq U_{2,\gamma}$. Thus, $\gamma(U_1) \cap U_2 = \emptyset$. Contradicton. Therefore $\gamma \neq F$. □

Corollary 4. *$Y(\Gamma)$ is Hausdorff.*

Proof. Take $\tau_1, \tau_2 \in \mathbf{H}$ such that $\pi(\tau_1) \neq \pi(\tau_2)$ (distinct points in the quotient). Take U_1, U_2 as in the proposition, so

$$\gamma(U_1) \cap U_2 \neq \emptyset \implies \gamma(\tau_1) = \tau_2.$$

Since $\pi(\tau_1) \neq \pi(\tau_2)$, $\gamma\tau_1 \neq \tau_2$ for all $\gamma \in \Gamma$. Therefore, $\gamma(U_1) \cap U_2 = \emptyset$. Thus, $\pi(U_1) \cap \pi(U_2) = \emptyset$. □

9 Fundamental domain of $Y(\Gamma)$

Let G be a group acting on a set X. Then the **isotropy subgroup** of $x \in X$ is $G_x = \{g \in G \mid gx \in x\}$. G_x is also known as the stabilizer.

We wish to endow $\Gamma\backslash\mathbf{H}$ with a complex structure. First, let's prove that

$$D = \{\tau \in \mathbf{H} \mid |\mathrm{Re}\tau| \leq \frac{1}{2}, |\tau| = 1\}$$

Definition 9. Let $\Gamma \subset SL_2(\mathbf{Z})$ be a congruence subgroup. Then $\tau \in \mathbf{H}$ is called an **elliptic point** if $\{\pm\mathrm{id}\} \subsetneq \Gamma_\tau$.

Our goal today is to prove the following proposition.

Proposition 8. $\Gamma_\tau \subset \Gamma$ *is cyclic.*

First we'll prove the result for $\Gamma = SL_2(\mathbf{Z})$. We need a series of lemmata and propositions

Lemma 3. *The map* $D \to \Gamma\backslash\mathbf{H}$ *is surjective.*

Proof. Given $\tau \in \mathbf{H}$, we show $(SL_2(\mathbf{Z}) \cdot \tau) \cap D \neq \emptyset$. By applying $\begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}$ to τ, we may assume $|\mathrm{Re}\tau| \leq \frac{1}{2}$. If $\tau \notin D$, then $|\tau| < 1$. So

$$\mathrm{Im}(\frac{-1}{\tau}) = \mathrm{Im}(\frac{\overline{-\tau}}{|\tau|^2}) = \mathrm{Im}(\frac{\tau}{|\tau|^2}) > \mathrm{Im}(\tau).$$

Note that $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tau = \frac{-1}{\tau}$. So we can repeatedly replace τ with $-1/\tau$, making the imaginary part larger. Repeating these two steps, we claim the process terminates after finitely many steps.

To see this, it suffices to show that there are finitely many elements of $SL_2(\mathbf{Z}) \cdot \tau$ with larger imaginary part. For this, $\mathrm{Im}(\gamma\tau) = \frac{\mathrm{Im}\tau}{|c\tau+d|^2}$, and there are finitely many $(c, d) \in \mathbf{Z}^2$ such that

$$|c\tau + d| < 1$$

as $\Lambda_\tau = \langle \tau, 1 \rangle$ is a lattice. □

We need one more lemma.

Lemma 4. *Let* $\tau_1 \neq \tau_2$ *in* D. *such that* $\tau_2 = \gamma\tau_1$ *for some* $\gamma \in SL_2(\mathbf{Z})$. *Then either*

(1) $\mathrm{Re}(\tau_1) = \pm\frac{1}{2}, \tau_2 = \tau_1 = 1$, *or*

(2) $|\tau_1| = 1$ *and* $\tau_2 = \frac{-1}{\tau_1}$

Proof. Without loss of generality, $|\tau_2| \geq |\tau_1|$. Set $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. So

$$\mathrm{Im}(\tau_2) = \frac{\mathrm{Im}\tau_1}{|c\tau + d|^2} \geq \mathrm{Im}(\tau_1)$$

$$\implies |c\tau_1 + d| \leq 1.$$

Since $\tau \in D$, $\mathrm{Im}(\tau_1) \geq \frac{\sqrt{3}}{2}$. Thus,

$$|c|\frac{\sqrt{3}}{2} \leq |c|\mathrm{Im}\tau 1 = |\mathrm{Im}(c\tau_1 + d)| \leq |c\tau_1 + d| \leq 1$$

$$\implies |c| \in \{0, 1\}$$

First case: $c = 0$: Here, $\gamma = \pm \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. Thus, $\mathrm{Re}\tau - 2 = \mathrm{Re}(\tau_1) + b$. So $|b| = 1$, giving 1.

Second case: $c = \pm 1$: Since $|c\tau_1 + d| \leq 1$, we have $|\tau_1 \pm d| \leq 1$. Thus,

$$(\mathrm{Re}\tau_1 + d)^2 \leq 1 - \mathrm{Im}(\tau_1)^2 \leq 1 - \frac{3}{4} = \frac{1}{4}$$

giving $|d| \leq 1$.

Subcase 1: $c = \pm 1, |d| = 1$: We have $|\mathrm{Re}\tau_1| \leq \frac{1}{2}$, and $|\mathrm{Re}\tau_1 \pm d| \leq \frac{1}{2}$, so

$$\mathrm{Re}\tau_1 = \pm\frac{1}{2}, d = \mp 1.$$

Thus, $\mathrm{Im}\tau_1 = \frac{\sqrt{3}}{2}$, giving both (1) and (2).

Subcase 2: $d = 0$: Since $|c\tau_1 + d| \leq 1$, $|\tau_1| \leq 1 \implies |\tau_1| = 1$. Thus,

$$\tau_2 = \begin{pmatrix} a & \mp 1 \\ \pm 1 & 0 \end{pmatrix} \tau_1 = \pm a - (\overline{\tau_1})$$

$$= (\pm a - \mathrm{Re}(\tau_1)) + i\mathrm{Im}\tau_1.$$

So $|a| \leq 1$, and if $|a| = 1$, then $\mathrm{Re}\tau_2 = \pm\mathrm{Re}\tau_1 = \pm\frac{1}{2}$, giving (1). If $a = 0$, this is (2).

□

Proposition 9. *If τ is an elliptic point $\gamma\tau = \tau$ with $\gamma \neq \pm\mathrm{id}$, then $|\gamma| = 3, 4$ or 6.*

Proof. As $\tau = \frac{a\tau + b}{c\tau + d}$, we have $c\tau^2 + d\tau = a\tau + b$. Therefore,

$$i\mathrm{Im}(\tau) = \frac{\pm\sqrt{(d-a)^2 + 4bc}}{2c}.$$

We claim that $|a+d| < 2$. Indeed, taking $\tau \in \mathbf{H}$, we have

$$(d-a)^2 + 4bc < 0$$

$$\implies (d-a)^2 + 4(ad-1) < 0$$

Thus, $d^2 + 2ad + a^2 - 4 < 0$, proving our claim.

Note that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 = \begin{pmatrix} a(a+d)-1 & b(a+d) \\ c(a+d) & d(a+d)-1 \end{pmatrix} = (a+d)\begin{pmatrix} a & b \\ c & d \end{pmatrix} - \mathrm{id}$$

Thus,

$$\gamma^2 0 - (a+d)\gamma) + \mathrm{id} = 0$$

Algebra shows that, given the possibilities $a+d \in \{-1, 0, 1\}$, then the possibilities are $\gamma^4 = 1$, $\gamma^6 = 1$, $\gamma^3 = 1$. Thus $|\gamma| = 2, 3, 4, 6$. But if $|\gamma| = -\mathrm{id}$. Indeed, in this case, $b(a+d) = c(a+d) = 0$, and $a + d \neq 0$. Thus $b + c = 0$. Also, $a(a+d) = d(a+d) = 2$, and $ad = 1$. So $a^2 = d^2 = 1$.

□

10 9/23/2015: Elliptic points

To summarize last time, for $\tau \in H$, we have the subgroup $\Gamma_\tau = \{\gamma \in \tau \mid \gamma\tau = \tau\}$. τ is called elliptic with respect to Γ if Γ_τ is nontrivial, i.e. if $\{\pm\mathrm{id}\} \subsetneq \{\pm\mathrm{id}\}\Gamma_\tau$. We showed last time that if $\gamma\tau = \gamma$, then γ has order 1, 2, 3, 4, or 6.

Proposition 10. *Let $\gamma \in SL_2(\mathbf{Z})$.*

(a) If $|\gamma| = 3$, γ is conjugate in $SL_2(\mathbf{Z})$ to $\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}^{\pm}$.

(b) If $|\gamma| = 4$, γ is conjugate in $SL_2(\mathbf{Z})$ to $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{\pm}$.

(d) If $|\gamma| = 6$, γ is conjugate in $SL_2(\mathbf{Z})$ to $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}^{\pm}$.

Proof. (c) Let $\mathbf{Z}^2$ be the lattice of integral column vectors, a $\mathbf{Z}[\mu_6]$ -module via

$$(a + b\mu_6) \cdot v = (a\mathrm{id} + b\gamma) \cdot v.$$

Now $\mathbf{Z}[\mu_6]$ is a PID (cyclotomic rings of integers have class number 1), and L is a finitely generated $\mathbf{Z}[\mu_6]$-module. The structure theorem for finitely generated modules over a PID gives that $L \simeq \bigoplus_k \mathbf{Z}[\mu_6]/I_k$, $I_k \subseteq \mathbf{Z}[\mu_6]$ are ideals. $\mathbf{Z}[\mu_6]$ has rank 2 as an abelian group generated by $\{1, \mu_6\}$. If $I \subset \mathbf{Z}[\mu_6]$ is a nonzero ideal, then $\mathrm{rank}(I) \geq 2$ since for $0 \neq \alpha \in I$, $\{\alpha, \mu_6\alpha\}$ are $\mathbf{Z}$-linearly independent. Thus, $\mathbf{Z}[\mu_6]/I$ is torsion.

With L torsion-free, $I_k = 0$ for each k. By comparing ranks, $\varphi \colon L \xrightarrow{\simeq} \mathbf{Z}[\mu_6]$. Set $u = \varphi^{-1}(1)$, $v = \varphi^{-1}(\mu_6)$. Let $[u, v]$ denote the 2×2 matrix with these columns. Since $L = \mathbf{Z}u \oplus \mathbf{Z}v$, $\det[u, v] = \pm 1$.

Computing, we get

$$\gamma u = \mu_6 \phi(1) = \phi(\mu_6) = v$$

$$\gamma v = \mu_6 \phi(\mu_6) = \phi(\mu_6^2) = \phi(\mu_6^2) - \phi(1) = -u + v$$

Thus, $\gamma[u, v] = [v, -u + v] = [u, v] \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$., so $\gamma = [u, v] \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} [u, v]^{-1}$. Note that $[u, v]$ need not be in $SL_2(\mathbf{Z})$, but then $[v, u] \in SL_2(\mathbf{Z})$ and $\gamma = [v, u] \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}^{-1} [v, u]^{-1}$.

(b) Similar to (*c*), using $\mathbf{Z}[\gamma] \cong \mathbf{Z}[i]$ is a PID.

(a) $|\gamma| = 3$, so $|-\gamma| = 6$, so $-\gamma$ is conjugate to $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}^{\pm 1}$. Thus, γ is conjugate to $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. □

Corollary 5. *The elliptic points for $SL_2(\mathbf{Z})$ are $SL_2(\mathbf{Z})i$ and $SL_2(\mathbf{Z})\mu_3$. Thus, $Y(1)$ has two elliptic points, and each of*

$$SL_2(\mathbf{Z})i = \langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \rangle$$

$$SL_2(\mathbf{Z})\mu_3 = \langle \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \rangle$$

is finite cyclic.

Note that if τ is an elliptic point with respect to Γ, then γ_τ is as well with Γ_τ and $\Gamma_{\gamma\tau}$ being conjugates: Let $\alpha \in \Gamma$. Then

$$\alpha\tau \in \tau \iff \alpha\gamma^{-1}\gamma\tau = \tau$$

$$\iff (\gamma\alpha\gamma^{-1})(\gamma\tau) = \gamma\tau$$

$$\implies \Gamma_\tau = \gamma\Gamma_{\gamma\tau}\gamma^{-1}$$

Proof. Recall that if τ is a fixed point of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then $a\tau + b = c\tau^2 + d\tau$. There are three cases

(1) $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$: $\tau^2 + \tau + 1 = 0 \implies \tau = e^{2\pi i/3}$ or $e^{4\pi i/3}$, throwout the second.

(2) $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$: $\tau^2 + 1 \implies \tau = \pm i$

(3) $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$: $\tau^2 - \tau + 1 \implies \tau = e^{\pi i/3}$ or $\tau = e^{2\pi i/3}$, throwout the first since it gets identified with the second.

Calculating isotropy subgroups,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} i = i \implies a = d, b = -c, a^2 + b^2 = 1$$

$$\implies \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \text{ or } \begin{pmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{pmatrix}$$

and the other gives

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} e^{2\pi i/3} = e^{2\pi i/3}$$

$$\implies ae^{2\pi i/3} + b = ce^{4\pi i/3} + de^{2\pi i/3}$$

Set the real and imaginary parts equal to each other:

$$-\frac{1}{2}a + b = \frac{1}{2}c - \frac{1}{2}d$$

$$\frac{\sqrt{3}}{2}a = -\frac{\sqrt{3}}{2} + \frac{\sqrt{3}}{2}d.$$

Solving these gives

$$a = -c + d$$

$$b = -c$$

and so

$$d^2 - cd + c^2 = 1(*)$$

$$(d-c)^2 + cd = 1(**).$$

There are three cases. (1) $c = 0$, so $d = \pm 1$. (2) $d = 0$, so $c = \pm 1$. (3) $c \neq 0$ and $d \neq 0$. (*) implies that c and d have the same sign, while (**) implies that if $c \neq d$, then c and d have opposite signs. Thus, $c = d \implies c = d = \pm 1$. This gives

$$\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} \mp 1 & \mp 1 \\ \pm 1 & \pm 0 \end{pmatrix}, \begin{pmatrix} \pm 0 & \mp 1 \\ \pm 1 & \pm 1 \end{pmatrix}$$

and these are all generated by $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$.

□

Corollary 6. *Let $\gamma \subseteq SL_2(\mathbf{Z})$ be a congruence subgroup. The modular curve $Y(\Gamma)$ has finitely many elliptic points. Moreover, each isotropy subgroup is cyclic.*

Proof. $\Gamma \subseteq SL_2(\mathbf{Z})$ is of finite index, so $SL_2(\mathbf{Z}) = \bigcup_{j=1}^{d} \Gamma\gamma_j$ where $\gamma_j \in SL_2(\mathbf{Z})$. If τ is an elliptic point, there exists $\gamma \in \Gamma$ such that $\gamma \neq \pm\mathrm{id}$, $\gamma\tau = \tau$. Thus, $\tau \in SL_2(\mathbf{Z})$ or $SL_2(\mathbf{Z})e^{2\pi i/3}$. Thus, the elliptic points of Γ are in $\{\Gamma\gamma_j \cdot i, \Gamma\gamma_j \cdot e^{2\pi i/3} \mid 1 \leq j \leq d\}$ and thus are finite. Each isotropy group is a subgroup of $SL_2(\mathbf{Z})_\tau$ and hence finite cyclic. □