General Elliptic Curves

Jemin You

We follow Katz and Mazur, 'Arithmetic Moduli of Elliptic Curves'.

0 Introduction

We formulate an algebro-geometric viewpoint towards elliptic curves. An essential ingredient is the notion of moduli problems and fine moduli spaces.

Unfortunately, another essential ingredient, the languages of scheme theory, will not be explained at all. They are to be thought of 'glued rings', in analogue to manifolds being 'glued disks', except there are less functions on rings so local structures are nontrivial. Think of glued rings to be coordinate rings of affine algebraic varieties over $\mathbb{C}$. We will explain the underlying concepts through examples.

1 Category of Elliptic Curves

Definition 1.1. An *elliptic curve* is a morphism of schemes $E \to S$ together with a section, where the morphism is proper smooth of dimension 1 having geometric fibres(=fibres over algbraically closed fields) connected curves of genus 1.

Example 1.2. The morphism of complex algebraic varieties

$$\{([X_0 : X_1 : X_2], j) \in \mathbb{CP}^2 \times (\mathbb{C}\backslash\{0, 1728\}) : X_2^2X_0 - X_1^3 - \frac{27}{4}\frac{1728 - j}{j}(X_1X_0^2 + X_0^3) = 0\} \to \{j \in \mathbb{C}\backslash\{0, 1728\}\}$$

given by the projection onto j-coordinates is an elliptic curve over $\mathbb{C}$, and also over $\mathbb{Q}$ if we restrict the js to be rational. If we fix any $j \neq 0, 1728$, the fibre of the above morphism is a complex elliptic curve of that j-invariant value.

Example 1.3 (Legendre family)**.** Another morphism of varieties

$$\{([X_0 : X_1 : X_2], \lambda) \in \mathbb{P}^2_k \times (k \setminus \{0, 1\}) : X_2^2X_0 = X_1(X_1 - X_0)(X_1 - \lambda X_0)\} \to \{\lambda \in k \setminus \{0, 1\}\}$$

given also by the projection is an elliptic curve for a (algebraically closed) field k. The j-invariant is given by

$$j = 2^8\frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

This family can be defined for any schemes where 2 is invertible, and is universal among them.

So scheme-theoritic notion of elliptic curves is a generalized version of algebraically varying families of complex elliptic curves. This is how we formulate familiy of varying schemes with parameters.

Notation 1.4. We denote by X/Y a morphism $X \to Y$ of schemes, and call X, or more precisely the morphism itself, a *scheme over* Y, or a Y*-scheme*. Also, by scheme over a ring A we mean a scheme over the spectrum $\mathrm{Spec}(A)$ of A, which is a geometric space(a local-ringed space) associated to A.

Definition 1.5. Let A be a ring. The category Ell/A of elliptic curves consist of the followings:
(1)The objects are elliptic curves $E \to S$ where S is an A-scheme.
(2)The morphism set from an elliptic curve $F \to T$ to another $E \to S$ are Cartesian diagrams

$$\begin{array}{ccc} F & \longrightarrow & E \\ \downarrow & & \downarrow \\ T & \longrightarrow & S \end{array}$$

where $T \to S$ is an A-morphism. When $A = \mathbb{Z}$, we just write Ell instead of $Ell/\mathbb{Z}$.

Example 1.6. If we let a reduced complex point go into the "j-line" from the previous example so $j = 1728 \cdot \frac{27}{31}$, then we obtain a morphism of complex elliptic curves that embeds

$$\{[X_0 : X_1 : X_2] \in \mathbb{CP}^2 : X_2^2 X_0 - X_1^3 - X_1 X_0^2 - X_0^3 = 0\}$$

into the previous example.

Thus a morphism of elliptic curves is a "mapping of continuous families of elliptic curves" that elliptic curves as geometric fibres are mapped isomorphically.

2 Moduli Problems

Definition 2.1. Let $\mathscr{C}$ be a category where the collections of morphisms between objects are sets("small"). A *moduli problem* on $\mathscr{C}$ is a contravariant functor,

$$\mathscr{P} : \mathscr{C}^{op} \to Sets$$

from the category $\mathscr{C}$ to the category of sets. We call this moduli problem $\mathscr{P}$ *representable* if there exist an object X of $\mathscr{C}$ such that

$$\mathscr{P} \simeq h_X$$

where $h_X(Y) := \mathrm{Hom}_{\mathscr{C}}(Y, X)$ and $\simeq$ denoteds the isomorphism of functors("natural equivalences"). The X above is called the *fine moduli space* of the moduli problem $\mathscr{P}$.

Remark 2.2. Due to a well-known result which states that $\mathscr{C}$ is embedded as full subcategory via

$$h : \mathscr{C} \to Sets^{\mathscr{C}^{op}}, \;\; X \mapsto h_X$$

(the Yoneda embedding), X is unique up to isomorphism.

Example 2.3 (The Grassmannian)**.** Let V be a complex vector space of dimension n and let k be an nonnegative integer not bigger than n. Let $\mathscr{C} = Sch/\mathbb{C}$ be the category of schemes over $\mathbb{C}$. The functor

$$\mathfrak{Gr}(k, V) : S \to \{\text{closed subschemes of } S \times \mathbb{P}(V) \text{ that are flat over } S \text{ with linear } (k-1)\text{-dimensional fibres}\}$$

(*flat=algebro-geometric version of continuously varying familiy*, and dimension drops to $k-1$ since we are in the projective space) is represented by the complex Grassmannian

$$\mathrm{Gr}(k, V) = \{k\text{-planes of } V\} \subseteq \mathbb{P}(\wedge^k V)$$

which is a complex projective manifold of dimension $k(n-k)$. Thus $\mathrm{Gr}(k, V)$ is the fine moduli space of $\mathfrak{Gr}(k, V)$.

So the functorial point of view lets us study moduli problems, which should intuitively be taken as classifying geometric object and structures, in a way that enlightens us how families can vary in a given category. For example, studying one-parameter family of k-planes of V is equivalent to studying maps from a complex affine/projective line to the Grassmannian $\mathrm{Gr}(k, V)$.

3 The Main Result

Theorem 3.1. *There exists a scheme-theoritic interpretation of* Γ*-structures where* Γ *is one of* $\Gamma_0(N)$*,* $\Gamma_1(N)$*,* $\Gamma(N)$*s from the last week. These define moduli problems on Ell, of which we denote by* $[\Gamma]$*. Fix an elliptic curves* $E \to S$*. Then the moduli problem on* Sch/S

$$T \mapsto [\Gamma](E_T/T)$$

(and E_T *is the fiber product of* $E \to S$ *and* $T \to S$*) is representable by a regular finite flat* S*-scheme.*

Remark 3.2. The Γ-structures mentioned above over $\mathbb{C}$ are precisely the ones from the last week.

Example 3.3 (Legendre moduli problem)**.** (cf.Example1.3) There is a moduli problem

$$E/S \mapsto \text{pairs } (\phi, \omega)$$

where $\phi : (\mathbb{Z}/2\mathbb{Z})^2 \to E[2]$ is a S-group-scheme isomorphism, ω is a S-basis of $\omega_{E/S}$, an invertible sheaf canonically associated to E/S with suitable adaptedness conditions. This is a representable moduli problem, and the Legendre family represents it when 2 is invertible on S.

Closely related is the $\Gamma[2]$-moduli problem. This associates E/S with group homomorphisms

$$\phi : (\mathbb{Z}/2\mathbb{Z})^2 \to E[2](S)$$

such that the 4 points mapped by ϕ form a "full set of sections", in the sense that they coincide with $E[2]$ as relative effective (Cartier) divisors of E/S.

Definition 3.4. A moduli problem $\mathscr{P}$ on Ell/A is *relatively representable* if the results of the theorem holds. That is, for any elliptic curve E/S over A, the functor on Sch/S given by

$$T \mapsto \mathscr{P}(E_T/T)$$

is representable. Therefore, $[\Gamma]$s above are relatively representable.

The theorem hence tells us that for families of which the continuous varying is controlled by a fixed family of Γ-structured elliptic curves are represented by a fixed family of elliptic curve parametrized by a S-scheme.

Unfortunately, we cannot do this for all bases schemes S: the moduli problems $[\Gamma]$ are not representable on Ell. This is because schemes relatively representing $[\Gamma]$(in the above sense) have nontrivial automorphisms, in analogue to non-existence of a fine moduli space of complex elliptic curves due to a nontrivial automorphism -1 (or more for $j = 0, 1728$).

Hence, the approach taken is to find the "best-approximating" schemes for the moduli problems $[\Gamma]$. These are called *coarse moduli schemes*. They correspond to the "j-line" $\mathbb{A}^1_{\mathbb{C}} = \mathbb{C}$ from the last week. Their geometric points(think them of complex points) correspond bijectively to Γ-structured elliptic curves. Then the coarse moduli schemes turn out to be finite over the "j-line" (over $\mathbb{Z}$) and can be *compactified* via "adding the cusps $j = \infty$". This is what we've done last week when we compactified $\mathbb{A}^1_{\mathbb{C}} = \mathbb{C}$ to $\mathbb{CP}^1$.

Starting from next week, we will go through the study of the compactifications near the cusps.