TITLE

DAVID HOLMES

ABSTRACT.

1. INTRODUCTION

2. STARTING POINT: FAMILIES OF ELLIPTIC CURVES

Start by saying: we are interested in families of elliptic curves, for example families of a riemann surface. To make the notation consistent, we should therefore think of a 'normal' elliptic curve over C as a 'family over a point'. We start by defining and giving examples of some families of elliptic curves.

Let R be a commutative unital ring. An elliptic curve over R is given by an equation $y^2 = x^3 + Ax + B$ where A, B are a pair of elements A, $B \in R$ such that $\Delta \overset{\text{def}}{=} -16(4A^3 - 27B^2)$ is a unit in R, together with a 'point at infinity'which is the identity for the group law.

Example: Let $R = \mathbb{C}$, then an elliptic curve is given by the data of a pair of complex numbers A and B such that the discriminant does not vanish. This defines an elliptic curve as the projective closure of the affine curve given by the eauqtion $y^2 = x^3 + Ax + B$ inside $\mathbb{C} \times \mathbb{C}$.

Example: $R = \mathbb{Q}$, $A = 2$, $B = 3$. Then $\Delta = -4400$ is a unit, so we obtain an elliptic curve given by the equation

$$y^2 = x^3 + 2x + 3. \tag{1}$$

Example: Let $R = \mathbb{Z}[1/2, 1/5, 1/11]$, $A = 2$, $B = 3$. Then $\Delta = -4400 = -2^4 \cdot 5^2 \cdot 11$ is a unit, so so obtain an elliptic curve given by the equation

$$y^2 = x^3 + 2x + 3. \tag{2}$$

Example: Let $A, B \in \mathbb{C}[t]$, and set $R = \mathbb{C}[t]_\Delta$, the localisation of $\mathbb{C}[t]$ by the multiplicatively closed set $\{\Delta^n : n \in \mathbb{Z}\}$. This defines an elliptic curve over R. It is cut out in $\mathbb{P}^2_R$ by the equation $y^2 = x^3 + Ax + B$. The important point is this: let t_0 be any complex number such that $\Delta(t_0) \neq 0$. Then $A(t_0)$, $B(t_0)$ defines an elliptic curve over $\mathbb{C}$. In other words, we have specified a *family* of elliptic curves over the complex plane minus a few points (the points where Δ vanishes.

Date: July 2, 2012.

We can think of this as a non-compact Riemann surface S (the complex plane minus the roots of Δ, together with a closed map from a 2-complex dimsnaional complex manifold E to S. The fibre of this map over a point t_0 in $\mathbb{C}$ is exactly the elliptic curve given by $y^2 = x^3 + A(t_0)x + B(t_0)$.

From now on, we will mainly be interested in this example and variations.

Example of the example: Let $A = 0$, $B = t$. Then $\Delta = 16 \cdot 27t^2$, which vanishes exactly when $t = 0$. As such, we have defined a family of elliptic curves over the punctured complex plane.

2.1. **Notational confusion.** We will write E/R for an elliptic curve over the ring R. However, above we said that an elliptic curve $E/\mathbb{C}[t]$ can be though of as a family of elliptic curves over the Riemann surface whose complex points are exactly elements of $\mathbb{C}$. Now clearly and elliptic curve over $\mathbb{C}$ and an elliptic curve over $\mathbb{C}[t]$ are completely different; for example, the former has dimension 1 as a complex manifold, and the latter has dimension 2. We therefore need to be careful that when we write $E/\mathbb{C}$ we mean an elliptic curve over the ring $\mathbb{C}$, NOT a family of elliptic curves over the Riemann surface which looks like $\mathbb{C}$.

Since the Riemann surfaces we will consider will for now all be punctured versions of the complex plane, we can avoid this confucion by sticking rigidly to our notation that E/R means an elliptic curve over the ring R, and if S is a complex plane punctured at the roots of a polynomial f then an elliptic curve over S is the same as an elliptic curve over $\mathbb{C}[t][f^{-1}]$. In general, this confusion is unfortunate but unavoidable.

Two obvious questions:

1) Can we give some kind of 'uniform description of all of these families of elliptic curves over punctured complex planes?

2) What about the 'missing points' where Δ vanished - can we 'fill these in' to get an elliptic curve over the whole complex plane?

3. Question 1: seeking a uniform description

What would an answer to this question look like? It will be a punctured plane Y and an elliptic curve E_{univ}/Y (as in our examples above) with the property that for $S = \text{Spec}(\mathbb{C})$ (a point) or any punctured plane with an elliptic curve E/S, there exists a unique map $\phi : S \to Y$ such that the following square is Cartesian in the category of complex manifolds:[*1]

$$\begin{array}{ccc} E & \longrightarrow & E_{\text{univ}} \\ \downarrow & & \downarrow \\ S & \longrightarrow & Y \end{array}$$

1: need a remark that an elliptic curve over $\mathbb{C}$ is an alliptic curve over a point, $\operatorname{Spec} C$.

[Recall the definition of a Cartesian square via the univeral property:

In other words, $E = S \times_Y E_{\text{univ}}$.]

Remark 1. *It turns out that this is impossible; we are trying to represent a functor that is not a sheaf in the fpcq topology, which is impossible. This can be rectified by imposing a 'level structure' on our elliptic curves - essentially fixing certain torsion points in order to pin down their automorphisms. However, in these lectures we will not worry about this issue.*

3.1. **Properties of the universal elliptic curve.**

Lemma 2. *Suppose that E_{univ}/Y exists as above. Then*
1) for all elliptic curves $E/\mathbb{C}$, there exists a unique point p_E in Y such that the fibre of E_{univ} over p_E is isomorphic to E as a complex manifold.
2) for every point $q \in Y$, the fibre $(E_{\text{univ}})_q$ is an elliptic curve.

Proof. Existance: Given an elliptic curve $E/\mathbb{C}$ defined by A, $B \in \mathbb{C}$, the universal property yields a cartesian square

$$\begin{array}{ccc} E & \longrightarrow & E_{\text{univ}} \\ \downarrow & & \downarrow \\ \text{Spec}(\mathbb{C})\text{point} & \longrightarrow & Y. \end{array}$$

Writing q for the image of the given map $\text{Spec}(\mathbb{C}) \to Y$, we see that by definition the fibre of E_{univ} over q is E.

Uniqueness: If two points q_1 and q_2 of Y have fibres isomorphic to E, then E can be constructed as either $\text{Spec}(\mathbb{C}) \times_{q_1,Y} E_{\text{univ}}$ or $\text{Spec}(\mathbb{C}) \times_{q_2,Y} E_{\text{univ}}$, contridicting the uniqueness part of the universal property of Y.

2) From the definition of elliptic curves and pullbacks, we see that E_{univ} is defined by two elements A_{univ}, $B_{\text{univ}} \in \mathbb{C}[t]$, and we have the discriminant polynomial $\Delta_{\text{univ}} \in C[t]$. THe point q corresponds to a complex number which we shall also write as q, and moreover we know that $\Delta(q) \neq 0$, henve $A_{\text{univ}}(q)$, $B_{\text{univ}}(q)$ defines an elliptic curve over $\mathbb{C}$. □

Summarising this lemma, we see that the universal elliptic curve (if it exists) is a 2-dimensional comples manifold with a map to a punctured complex plane, with the property that

- the fibre over each point is a complex elliptic curve

- every elliptic curve over $\mathbb{C}$ appears exactly once as such a fibre.

3.2. **Algebraic construction of the universal elliptic curve.**

3.2.1. *Definition of the j-invariant.*

Definition 3. *Given an elliptic curve E over a ring R defined by $y^2 = x^3 + aX + B$, the j-invariant of E is given by*

$$j(E) = -1728(4A)^3/\Delta. \tag{3}$$

Note that $j(E) \in R$ since Δ is a unit.

Lemma 4. *Let $R = \mathbb{C}$. Then two elliptic curves E_1, E_2 over R are isomorphic if and only if $j(E_1) = j(E_2)$.*

Proof. This is elementary, and is Proposition 1.4 b of [Silverman, Topics in the arithmetic of elliptic cuvres]. □

Lemma 5. *Let $R = \mathbb{C}[t][1/t, 1/(t-1728)]$, and let E be given by $A12 \cdot 27^2 t/(t-1728)$, $B = -54 \cdot 216 \cdot 27t/(t-1728)$. Then we almots have $E = E_{\text{univ}}$, in the sense that for any elliptic curve $E_0/\mathbb{C}$ with $j(E_0) \neq 0$, 1728 we have a unique point q_0 in $\mathbb{C} \setminus \{0, 1728\}$ such that the fibre of E over q_0 is isomorphic to E_0.*

Proof. We should begin by checking that E/R is an elliptic curve, namely that the discriminant is a unit. An easy calculation [Exercise] yields that

$$\Delta = t^2/(t-1728)^3 \tag{4}$$

up to a constant. A smilar calculation [Exercise] also shows that

$$j(E) = t \tag{5}$$

(up to a constant).

The result is now easy; for any E_0 as in the statement, we simply take q_0 to be the point of the punctured complex plane corresponding to the j-invariant of E_0, and we know the fibre of E over q_0 must have the same j-invariant as E_0, so by the previous lemma we know it is isomorphic to E_0.

□

3.3. **Compactification of the moduli space.**

In this section, we will sketch and argument using the fundamental group to show that it is impossible to 'fill in the holes' in the universal elliptic curve.

For the remainder of this section, we will assume (pretend) that the universal elliptic curve over $R = \mathbb{C}[t][1/t, 1/(t-1728)]$ exists and satisfies the universal property. This is not quite true, but it does not matter for the purposes of our argument; either enhance the moduli space with a level structure or just take the underlying coarse moduli space, then the argument that follows will go through almost unchanged.

Proposition 6. *There does not exist an elliptic curve* $\tilde{E}_{univ}/\mathbb{P}^1$ *such that*

$$\tilde{E}_{univ} \times_{\mathbb{P}^1} R = E_{univ}. \tag{6}$$

We will prove this using a sequence of lemmas.

Lemma 7. *Let* $S = \mathbb{C}[t][1/t]$*. To prove Prop 6, it suffices to construct an elliptic curve* E/S *such that there does not exist an elliptic curve* $\tilde{E}/\mathbb{C}[t]$ *with*

$$\tilde{E} \times_{\mathbb{C}[t]} S = E. \tag{7}$$

Proof. Suppose we have such E/S, and the universal compactification $\tilde{E}_{univ}/\mathbb{P}^1$ exists. The universal property yields a cartesian square

$$\begin{array}{ccc} E & \longrightarrow & E_{\mathrm{univ}} \\ \downarrow & & \downarrow \\ S & \xrightarrow{\phi} & Y, \end{array}$$

and extending ϕ to $\mathbb{C}[t]$ we obtain a compactification $\tilde{E}_{univ} \times_{\tilde{Y},\phi} S$ of E/S, a contradiction. □

Let E_0/S be the elliptic curve given by $A = 0$, $B = -t$:

$$y^2 = x^3 - t. \tag{8}$$

We will prove that there does not exist an elliptic curve $E_1/\mathbb{C}[t]$ such that $E_1 \times_{\mathbb{C}[t]} S = E_0$. FIrst we should point out that this statement is not obvious; taking the naive limit of the family $E_0(t)$ as $t \to 0$ does not yield an elliptic curve, but (since the complex dimension of E_0 is greater than 1) this does not preclude the existence of E_1.

We will suppose that such an E_1 exists, and then study the torsion and monodromy to derive a contradiction.

3.3.1. *Torsion in families.* Let E/R be any elliptic curve over a punctured plane. Then given any integer $n > 0$, we define the *n-torsion* to be the set of points $p \in E$ which are n-torsion in the elliptic curves in which they lie. Now the property 'begin n-torsion' is defined by a collection of algebraic equations, and by writing down these equations one can see that the set of n-torsion points forms a *sub-manifold* of E (Exercise), which we denote $E[n]$.

For example by looking at the Weierstrass uniformisation, one can see that there are exactly n^2 points in each fibre of $E[n]$. In particular there are a finite number, so we obtain a cover of the punctured plane. The key observation is that this is an *unbranched* cover (Exercise).

We can apply this argument to our elliptic curve E_0, and also the hypothetical compactification E_1; we see that $E_0[2]$ is an unbranched degree-4 cover of a punctured plane, and $E_1[2]$ is an unbranched degree-4 cover of the whole complex plane (if it exists).

3.3.2. *Fundamental group.* Let l be a loop going once around the origin in the complex plane, parametrised by $l(a) = e^{2\pi i a}$ for $a \in [0, 1]$. Let $p_0 \in E_0$ be the point given by $t = 1, x = 1, y = 0$, and similarly $p_1 \in E_1$ be given by the same coordinates. It is easy to check that p_0 and p_1 are 2-torsion in their respective families. Using that $E_0[2]$ and $E_1[2]$ are both covering spaces of neighbourhoods of the loop l, we apply path lifting starting at p_0 and also at p_1, obtaining paths l_0 and l_1 respectively.

Now $E_1[2]$ is an unbranched cover over a contractible space, and so the path l_1 must in fact be a loop. On the other hand, we can work out 'by hand' the path l_0: since we must remain inside $E_0[2]$, which is given by equations $y = 0$, $x^3 - t = 0$ (Exercise), we can see that $x(l_0(a)) = e^{2\pi i a/3}$. In particular, l_0 does not get back to where it started, so is not a loop.

Now a contradiction is immediate; away from the origin in the complex plane, E_0 and E_1 are the same, so it is impossible for a loop to lift to a loop in $E_1[2]$ but not in $E_0[2]$. Thus E_1 cannot exist.

4. Next lecture:

The analytic version of theis story.

References