18.727, Topics in Algebraic Geometry (rigid analytic geometry)
Kiran S. Kedlaya, fall 2004
Introduction: the Tate curve

We are going to start the course precisely where the subject of rigid analytic geometry itself has its origin, with Tate's groundbreaking work on parametrization of elliptic curves. Of course this will be somewhat informal since we haven't done any theory yet; the idea is to give some sense both of the "how" (of doing analytic geometry over nonarchimedean fields) and the "why" (with an application due to Serre).

This is only one of the applications I hope to discuss during the semester; this one is pretty much number theory, as are many of the others I'm fond of, but there are lots of other applications that get into other areas. I'll provide a long (if not exhaustive) list sometime soon.

Note that we are starting with the very *last* section of [BGR]! That should give you some sense of the difference between their attitudes and mine.

References: Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves* (cited as [Sil]), whose development of the Tate curve in Section V.3 is liberally plagiarized here. References in the language of rigid geometry won't do you any good yet, but here they are for future use: [BGR, Section 9.7], [FvdP, 5.1]. Note that here and throughout the course, [BGR] means *Non-Archimedean Analysis*, by Bosch, Güntzer, and Remmert, while [FvdP] means *Rigid Analytic Geometry and its Applications*, by Fresnel and van der Put. (The former is unfortunately out of print. Then again, maybe that's just as well; it's a useful reference book but of no pedagogical value, as it's pretty dry, devoid of examples, devoid of exercises, and aside from the Tate curve, devoid of geometry and of applications!)

Warmup: Weierstrass parametrizations

An *elliptic curve* over a field is a genus 1 algebraic curve over that field equipped with the choice of a distinguished point on the curve (the *origin*). Over $\mathbb{C}$, this is the same as a Riemann surface of genus 1 equipped with a choice of a distinguished point.

Once upon a time, Weierstrass discovered that every elliptic curve E over $\mathbb{C}$ can be viewed in a canonical fashion as a complex torus, i.e., as a quotient of $\mathbb{C}$ by a lattice of the form $\mathbb{Z}\alpha + \mathbb{Z}\beta$. This parametrization makes a lot of facts about genus 1 curves over $\mathbb{C}$ much more transparent, e.g., the group law, the shape of the torsion subgroups, and the possibilities for the ring of endomorphisms.

Once upon a somewhat more recent time, Tate realized that one could do something similar over the field $\mathbb{Q}_p$ of p-adic numbers. (I'm not going to define $\mathbb{Q}_p$ here; if you don't know what it is, probably this is not the course for you!) This is not at all clear from the "$\mathbb{C}$ mod a lattice" description above; we have to break a little symmetry first. Namely, by rescaling the lattice, we may as well assume that it is generated by 1 and τ, where $\tau \in \mathcal{H}$ and $\mathcal{H}$ is the upper half-plane

$$\mathcal{H} = \{z \in \mathbb{C} : \Im(z) > 0\}.$$

The Weierstrass functions on $\mathbb{C}$, which generate the field of meromorphic functions on E, are now doubly periodic, and in particular they are invariant under translation by 1. So why not write them as Fourier series? In other words, apply the exponential map:

$$\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}) \stackrel{\exp}{\to} \mathbb{C}^*/q^{\mathbb{Z}},$$

where $q = e^{2\pi i\tau}$.

In the Weierstass setting, there are special functions of the parameter τ that describe the elliptic curve, but of course we can write them in terms of q also. Namely, set

$$s_k(q) = \sum_{n=1}^{\infty} \frac{n^k q^n}{1-q^n} \qquad (k \in \mathbb{N})$$

and put

$$a_4(q) = -s_3(q), \qquad a_6(q) = -\frac{5s_3(q)+7s_5(q)}{12}.$$

Then [Sil, V.1.1] the elliptic curve $E_q \cong \mathbb{C}^*/q^{\mathbb{Z}}$ is isomorphic to

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q), \tag{1}$$

its discriminant is

$$\Delta(q) = q\prod_{n=1}^{\infty}(1-q^n)^{24}, \tag{2}$$

and its j-invariant is

$$j(E_q) = q^{-1} + 744 + 196884q + \cdots . \tag{3}$$

The parametrization $\mathbb{C}^*/q^{\mathbb{Z}} \to E_q$ is given by the functions (rewrites of the Weierstrass $\wp$ function and its derivative)

$$X(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2s_1(q) \tag{4}$$

$$Y(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^3} + s_1(q); \tag{5}$$

that is, if you fix q, for each u the point $(X(u,q), Y(u,q))$ lies on E_q, and these form an analytic isomorphism between the complex torus and the elliptic curve. (The point $1 \in \mathbb{C}^*/q^{\mathbb{Z}}$ maps to the point at infinity on the Weierstrass equation (1).)

Tate curves

Now suppose K is a finite extension of the field $\mathbb{Q}_p$, and let $|\cdot|$ denote the absolute value on K normalized so that $|p| = p^{-1}$. Then the series $s_k(q)$ converges whenever $|q| < 1$, so one might wonder whether in that case we get an "isomorphism" between on one hand the quotient of the multiplicative group by the subgroup generated by $q^{\mathbb{Z}}$, and on the other hand

the elliptic curve (1). To make this really make sense, we need to have some category of geometric objects in which we can take the quotient $\mathbb{G}_m/q^{\mathbb{Z}}$; certainly we can't do it using schemes. One of the purposes of this course is to construct precisely the sorts of geometric objects that one needs to form the quotient and say that it's isomorphic to the elliptic curve.

But in the meantime, one can prove that everything works correctly at the level of points.

Theorem 1. *For $q \in K$ with $|q| < 1$, the equation (1) defines an elliptic curve over K with discriminant (2) and j-invariant (3); the series $X(u,q)$ and $Y(u,q)$ defined in (4) and (5) converge for all $u \in (K^{\mathrm{alg}})^* \setminus q^{\mathbb{Z}}$; and the map $\phi : (K^{\mathrm{alg}})^* \to E_q(K^{\mathrm{alg}})$ given by*

$$u \mapsto \begin{cases} (X(u,q), Y(u,q)) & u \notin q^{\mathbb{Z}} \\ O & u \in q^{\mathbb{Z}} \end{cases}$$

(where O is the point at infinity on E_q) is a Galois-equivariant surjection with kernel $q^{\mathbb{Z}}$. (In fact, the same is true with K^{alg} replaced by any finite extension of K, which says a bit more.)

Proof. This is verified in detail in [Sil, Theorem V.3.1], but it's a bit cumbersome (precisely because we don't have any of the rigid geometric machinery available yet!). So I'll only summarize for now.

I already noted that s_k converges for $|q| < 1$, so a_4 and a_6 are defined. The computation of Δ and j from a_4 and a_6 is formal, so the series expressions don't change between the complex case and this case. Oh, and

$$|\Delta(q)| = |q - 24q^2 + 252q^3 + \cdots| = |q| \neq 0$$

since all the other terms are of strictly smaller size, so $\Delta(q) \neq 0$ and E_q really is an elliptic curve.

To see that $X(u,q)$ and $Y(u,q)$ converge, it is easiest to rewrite them as in [Sil, (V.1.2)]:

$$\begin{aligned} X(u,q) &= \frac{u}{(1-u)^2} + \sum_{n=1}^{\infty} \left(\frac{q^n u}{(1-q^n u)^2} + \frac{q^{-n} u}{(1-q^{-n}u)^2} - 2\frac{q^n}{(1-q^n)^2} \right) \\ &= \frac{1}{u + u^{-1} - 2} + \sum_{n=1}^{\infty} \left(\frac{q^n u}{(1-q^n u)^2} + \frac{q^n u^{-1}}{(1-q^n u^{-1})^2} - 2\frac{q^n}{(1-q^n)^2} \right) \\ Y(u,q) &= \frac{u^2}{(1-u)^3} + \sum_{n=1}^{\infty} \left(\frac{(q^n u)^2}{(1-q^n u)^3} + \frac{(q^{-n} u)^2}{(1-q^{-n}u)^3} + \frac{q^n}{(1-q^n)^2} \right) \\ &= \frac{u^2}{(1-u)^3} + \sum_{n=1}^{\infty} \left(\frac{(q^n u)^2}{(1-q^n u)^3} + \frac{(q^n u^{-1})^2}{(1-q^n u^{-1})^3} + \frac{q^n}{(1-q^n)^2} \right). \end{aligned}$$

From this description the convergence for $u \in (K^{\mathrm{alg}})^* \setminus q^{\mathbb{Z}}$ is clear: everything is converging like a geometric series as long as none of the denominators vanish.

Aside, but an important one: the fact that I'm plugging in values from K^{alg} makes the previous conclusion much stronger than if I only took values from K, because there's a hard limit on how close together two elements of K can be (because K is discretely valued). So in general, you can't really assess convergence properties (like the radius of convergence of a power series) by testing values in a finite extension of $\mathbb{Q}_p$.

Anyway, one can check from the series above that $X(qu,q) = X(u,q) = X(u^{-1},q)$, that $Y(qu,q) = Y(u,q)$, and that $Y(u^{-1},q) = -Y(u,q) - X(u,q)$, as you would expect of points on E_q.

To check that the image of ϕ lands on E_q amounts to checking that plugging $X(u,q)$ and $Y(u,q)$ into E_q yields an identity of formal power series; this can be deduced from the complex side. Ditto for the fact that multiplication in $(K^{\text{alg}})^*$ converts into the addition law on E_q.

The only bit that remains is to check surjectivity of ϕ. Unfortunately, this is the hardest part, and the proof in [Sil, V.4] is too ugly and not insightful enough to be worth reproducing here. I would recommend looking at it just to gain an appreciation for why one needs a real theory of analytic spaces over nonarchimedean fields. □

In case you know what this means: one interesting feature of the ugly calculation in [Sil, V.4] is the fact that he sorts the points on E_q into classes as follows. (Here π is a uniformizer of K.)

$$\begin{aligned} E_{q,0}(K) &= \{(x,y) \in E_q(K) : \max\{|x|,|y|\} \geq 1\} \\ U_n &= \{(x,y) \in E_q(K) : |\pi|^n = |y| > |x+y|\} \\ V_n &= \{(x,y) \in E_q(K) : |\pi|^n = |x+y| > |y|\} \\ W &= \{(x,y) \in E_q(K) : |y| = |x+y| = |q|^{1/2}\} \end{aligned}$$

The point is that these classes are "neighborhoods" of the various components of the special fibre of the Néron model of E_q. Note that $|q| < 1$ means that $|j| > 1$, so E_q necessarily has bad reduction; in fact, its reduction is multiplicative of type I_n, where n is the valuation of q in K.

The parametrization theorem

Here's the point of the construction we just made.

Theorem 2 (Tate). *Let K be a finite extension of $\mathbb{Q}_p$, and let E be an elliptic curve with $|j(E)| > 1$.*

(a) There is a unique $q \in K^*$ with $|q| < 1$ such that $E \cong E_q$ over K^{alg}.

(b) For q as in (a), $E \cong E_q$ over K if and only if E has split multiplicative reduction.

Proof. For (a), note that one can invert the series for j given in (3) to solve for j in terms of q. For (b), see [Sil, Theorem V.5.3]. □

In other words, Tate's construction gives a universal description of elliptic curves with bad reduction at a prime! Furthermore, it's clear from the description that the parametrization commutes with the action of $\mathrm{Gal}(K^{\mathrm{alg}}/K)$; that's one reason why number theorists like this parametrization more than the Weierstrass parametrization, which has no such property.

Application: j-invariants and complex multiplication

As an application of Tate's construction, we mention the following argument due to Serre.

Proposition 3. *Let K be a finite extension of $\mathbb{Q}_p$ with normalized valuation v, let E be an elliptic curve over K with $|j(E)| > 1$, and let $\ell \geq 3$ be a prime not dividing $v(j(E))$ (but $\ell = p$ is allowed). Then there exists σ in the inertia subgroup of $\mathrm{Gal}(K^{\mathrm{alg}}/K)$ and a basis P_1, P_2 of the ℓ-torsion $E[\ell]$ of E over K^{alg} such that*

$$P_1^\sigma = P_1, \qquad P_2^\sigma = P_1 + P_2.$$

Proof. There is no harm in replacing K by a finite extension of degree prime to ℓ (doing so multiplies $v(j(E))$ by some divisor of that degree, namely the degree of the residual extension). In particular, by going up a quadratic extension, we can ensure that E is congruent to its corresponding Tate curve E_q over K; and we may assume that K contains a primitive ℓ-th root of unity ζ_ℓ.

Let $Q = q^{1/\ell} \in K^{\mathrm{alg}}$ be a fixed ℓ-th root of q. Then the ℓ-torsion in $(K^{\mathrm{alg}})^*/q^{\mathbb{Z}}$ is generated by ζ_ℓ and Q. So all we have to do is notice that the Kummer extension $K(Q)/K$ is totally ramified of degree ℓ, so there exists σ in the inertia subgroup of $\mathrm{Gal}(K^{\mathrm{alg}}/K)$ such that $Q^\sigma = Q\zeta_\ell$ (and $\zeta_\ell^\sigma = \zeta_\ell$ since we put ζ_ℓ into K); the images P_1 and P_2 of ζ_ℓ and Q, respectively, do what we wanted. □

Aside: strictly speaking, we didn't need the surjectivity of the Tate parametrization, since we were able to produce enough ℓ-torsion within $(K^{\mathrm{alg}})^*/q^{\mathbb{Z}}$. (That's the part where I was whining earlier because we haven't done any rigid geometry yet.) But in other applications we may not be so lucky!

Anyway, here's what Serre deduced from this. (There are other proofs too; see [Sil, V.6] for more discussion.)

Theorem 4. *Let $K/\mathbb{Q}$ be a number field, and let E/K be an elliptic curve whose j-invariant is not an integer in K. Then $\mathrm{End}(E) = \mathbb{Z}$.*

By contrast, an elliptic curve over a field of characteristic zero can also have endomorphism ring equal to an order in an imaginary quadratic field (the "complex multiplication" case). This theorem proves that the j-invariants of CM-curves, which one can show are algebraic numbers, are actually algebraic integers!

Proof. Suppose on the contrary that $\mathrm{End}(E)$ includes an endomorphism $\psi \notin \mathbb{Z}$. Then (see exercises) ψ must satisfy some polynomial of the form

$$a\psi^2 + b\psi + c = 0 \qquad (a, b, c \in \mathbb{Z}).$$

Moreover, the polynomial ax^2+bx+c must have distinct nonreal roots, which generate some quadratic imaginary field L.

In particular, there are lots of primes ℓ which split (and are not ramified) in ℓ, and which don't divide a. Pick one: then ψ acts on the ℓ-torsion $E[\ell]$ (which is a two-dimensional vector space over $\mathbb{F}_\ell$) via a matrix which is diagonalizable with distinct roots.

On the other hand, if we pass from K to its completion $K_\mathfrak{p}$ at some prime ideal $\mathfrak{p}$ (of the ring of integers of K) at which $j(E)$ is nonintegral, then by our proposition, there is an element of $\mathrm{Gal}(K_\mathfrak{p}^{\mathrm{alg}}/K_\mathfrak{p})$ which acts via a nontrivial unipotent matrix. But this element of Galois has to commute with ψ, which is clearly impossible! Contradiction. $\square$

Exercises

1. Verify some of the formal stuff that I didn't check, like the fact that multiplication on $(K^{\mathrm{alg}})^*/q^{\mathbb{Z}}$ translates into addition on the Tate curve. Or if you prefer, just look it up in [Sil, Chapter V].

2. Check all the statements I made about the endomorphism ψ of an elliptic curve, e.g., that it satisfies a quadratic polynomial whose roots are nonreal. (Hint: use the Weierstrass parametrization.)

3. (Sil, Exercise 5.10) Prove that if the Tate curves E_q and $E_{q'}$ are isogenous, then some power of q equals some power of q'. The converse is also true, but is a bit complicated to show without doing the construction more honestly (i.e., actually using rigid geometry).