Gross–Zagier reading seminar

Lecture 10 • Andrew Snowden • November 18, 2014

The purpose of this lecture is to prove the Serre–Tate theorem. This theorem says that deforming an abelian variety is equivalent to deforming its p-divisible group. We will focus on elliptic curves for simplicity, although the proof in the general case is really no more difficult.

1. Statement of theorem

To state the theorem precisely, we introduce some notation. Let R be a ring in which N (a power of p) vanishes, let I be an ideal such that $I^{n+1} = 0$, and let $R_0 = R/I$. Recall two basic definitions:

- An **elliptic curve** over R is a pair (E, P) where E is a proper smooth scheme over R whose geomtric fibers are genus 1 curves, and $P \in E(R)$ is a point.
- A **p-divisible group** over R of height h is a family $G = (G_i)$ of finite flat group schemes over R such that G_i has order p^{ih} and G_i is identified with the p^i torsion of G_{i+1}.

If E/R is an elliptic curve then we obtain a p-divisible group G of height 2 by putting $G_i = E[p^i]$. We denote this p-divisible group G by $E[p^\infty]$.

Let $\mathcal{E}$ be the category of elliptic curves over R. Let $\mathcal{G}$ be the category of triples (E_0, G, i), where E_0 is an elliptic curve over R_0, G is a p-divisible group over R, and $i\colon E[p^\infty] \to G_0$ is an isomorphism of p-divisible groups. The theorem is then:

Theorem 1 (Serre–Tate)**.** *The functor $\mathcal{E} \to \mathcal{G}$ taking E to $(E_0, E[p^\infty], \mathrm{id})$ is an equivalence of categories.*

2. Some lemmas

We follow Drinfeld's proof, as given in Katz's article "Serre–Tate local moduli." For an elliptic curve E/R and an R-algebra A, let $E_I(A) = \ker(E(A) \to E(A/IA))$.

Lemma 2. *The group $E_I(A)$ is killed by N^n.*

Proof. Recall that if X is a local parameter for E at the origin, then the multiplication-by-N map on E takes the form $[N](X) = NX +$ higher order terms. A point of $G_I(A)$ has $X \in I$, by definition. Since $NX = 0$ (as N kills R), we thus see that $[N](G_I(A)) \subset G_{I^2}(A)$, and more generally, $[N](G_{I^k}(A)) \subset G_{I^{k+1}}(A)$. Since $I^{n+1} = 0$, the result follows. □

Lemma 3. *The map $\psi\colon E(A/IA) \to E(A)$ defined by mapping x to $N^n\widetilde{x}$, where $\widetilde{x} \in E(A)$ is any lift of x, is a well-defined group homomorphism.*

Proof. We first note that any $x \in E(A/IA)$ admits a lift $\widetilde{x} \in E(A)$, since E is smooth. Suppose that $\widetilde{x}'$ is a second lift. Then $\widetilde{x} - \widetilde{x}' \in E_I(A)$, and therefore killed by N^n, and so $N^n\widetilde{x} = N^n\widetilde{x}'$. Thus $\psi(x)$ is well-defined. It is clear that it is a homomorphism. □

For the next few lemmas, fix elliptic curves E and E' over R, and let $G = E[p^\infty]$ and $G' = E'[p^\infty]$. The Hom's in the following lemma's can be taken to mean maps of functors.

Lemma 4. *The groups $\mathrm{Hom}(*, *')$ for $* \in \{G, G_0, E, E_0\}$ have no p-torsion.*

Proof. This follows immediately from the fact that $*$ is p-divisible. □

Lemma 5. *The natural maps* $\mathrm{Hom}(G, G') \to \mathrm{Hom}(G_0, G'_0)$ *and* $\mathrm{Hom}(E, E') \to \mathrm{Hom}(E_0, E'_0)$ *are injective.*

Proof. A morphism in the kernel of one of these maps would take values in E'_I. Since the groups are p-torsion free and E'_I is killed by a power of p, the result follows. □

We now study the problem of lifting a map $G_0 \to G'_0$ or a map $E_0 \to E'_0$. Note that the previous lemma implies that any a map admits at most one lift.

Lemma 6. *Let* $f_0 \colon G_0 \to G'_0$ *be a given map. Then* $N^n f_0$ *lifts to a map* $g \colon G \to G'$*. For* f_0 *to lift, it is necessary and sufficient that* $g(G[N^n]) = 0$*. The same statements hold maps* $E_0 \to E'_0$*.*

Proof. Take g to be to be the composition

$$G(A) \to G(A/IA) \stackrel{f_0}{\to} G'(A/IA) \subset E'(A/IA) \stackrel{\psi}{\to} E'(A).$$

Note that the image must be contained in $G'(A)$, and so g is a map $G \to G'$. It is clearly a lift of $N^n f_0$. If f_0 lifts to f, then $g = N^n f$ by the uniqueness of lifts, and therefore $g(G[N^n]) = 0$. Conversely, suppose that $g(G[N^n]) = 0$. Then $g = N^n f'$ for some homomorphism $f' \colon G \to G'$. Note that $N^n f_0 = N^n f'_0$, and so $f_0 = f'_0$ since $\mathrm{Hom}(G_0, E'_0)$ has no p-torsion. Thus $f = f'$ is a lift of f_0. The exact same proof applies to maps $E_0 \to E'_0$. □

3. Proof of the theorem

We begin by proving that the functor $\Phi \colon \mathcal{E} \to \mathcal{G}$ is faithful. Suppose $f \colon E \to E'$ is a map of elliptic curves over R such that $\Phi(f) = 0$. Then $f_0 = 0$, and so $f = 0$ by Lemma 5.

We now show that Φ is full. Thus suppose we are given elliptic curves E and E' over R, a map $f[p^\infty] \colon E[p^\infty] \to E'[p^\infty]$ of p-divisible groups, and a map $f_0 \colon E_0 \to E'_0$ of elliptic curves, such that $f[p^\infty]_0$ and $f_0|_{E[p^\infty]}$ agree. Let $g \colon E \to E'$ be the unique lift of $N^n f_0$ provided by Lemma 6. Then $g|_{E[p^\infty]}$ is a lift of $N^n f[p^\infty]_0$, and so, by uniqueness of lifts, $g|_{E[p^\infty]} = N^n f[p^\infty]$. This implies that g kills $E[p^n]$, and so $g = p^n f$ for some $f \colon E \to E'$ lifting f_0. Of course, the restriction of f to $E[p^\infty]$ must agree with the given $f[p^\infty]$, since the two have the same restriction to R_0.

We finally show that Φ is essentially surjective. Thus let $(E_0, G, i) \in \mathcal{G}$ be given. We must produce E/R giving rise to this data. Since the moduli of elliptic curves is smooth, we can find some deformation E' of E_0 over R. The isomorphism $E'_0 \to E_0$ induces an isomorphism $\alpha_0 \colon E'_0[p^\infty] \to E_0[p^\infty] = G_0$ of p-divisible groups. Let $\beta \colon E'[p^\infty] \to G$ be the unique lifting of $N^n \alpha_0$ provided by Lemma 6, and let $\gamma \colon G \to E'[p^\infty]$ be the unique lifting of $N^n \alpha_0^{-1}$. Since $\beta\gamma$ and $\gamma\beta$ both lift N^{2n}, they are both equal to N^{2n} by the uniqueness of lifts. Thus β is an isogeny of p-divisible groups. The reduction of β modulo I is the composition of N^n and an isomorphism, and therefore flat. It follows that β is flat. [Not clear on details, uses fact that formal completion of G is flat over R, since it's a formal Lie group]

Let K be the kernel of β. This is a closed subgroup of $E'[N^n]$, and so finite over R, and flat over R since β is flat; thus K is a finite flat group scheme over R. Define $E = E'/K$. Since $K_0 = E'_0[N^n]$, E is a lift of $E'_0/E'_0[N^n] = E'_0 = E_0$. The exact sequence

$$0 \to K \to E'[p^\infty] \to G \to 0$$

shows that $E[p^\infty]$ is isomorphic to G. The fact that the isomorphisms are compatible is straightforward.

4. The canonical lift

Suppose that E/k is an ordinary elliptic curve, where k is a perfect field (e.g., algebraically closed or finite) of characteristic p. Let R be a local artinnian ring with residue field k. By the Serre–Tate theorem, lifting E to R is the same as lifting its p-divisible group $G = E[p^\infty]$. Now, G fits into a connected-étale sequence

$$0 \to G^\circ \to G \to G_{\mathrm{et}} \to 0.$$

Because E is ordinary, G° is dual to G_{et} and is of multiplicative type. Because k is perfect, this extension is canonically split, i.e., $G = G_{\mathrm{et}} \times G^\circ$. Now, étale groups deform uniquely to any nilpotent thickening. The same is true for multiplicative groups, as they are Cartier dual to étale groups. Thus there are unique lifts $\widetilde{G}_{\mathrm{et}}$ and $\widetilde{G}^\circ$ to R. Their product $\widetilde{G} = \widetilde{G}_{\mathrm{et}} \times \widetilde{G}^\circ$ is a lift of G to a group over R, and therefore corresponds, by Serre–Tate, to a lift $\widetilde{E}$ of E over R. This is called the **canonical lift.**

The canonical lift is, as the name implies, canonical. If $f\colon E \to E'$ is a map of ordinary elliptic curves over k, then f induces maps $G_{\mathrm{et}} \to G'_{\mathrm{et}}$ and $G^\circ \to (G')^\circ$. These lift uniquely to maps $\widetilde{G}_{\mathrm{et}} \to \widetilde{G}'_{\mathrm{et}}$ and $\widetilde{G}^\circ \to (\widetilde{G}')^\circ$, and thus induce a map $\widetilde{G} \to \widetilde{G}'$. By Serre–Tate, this corresponds to a map $\widetilde{E} \to \widetilde{E}'$ of elliptic curves over R. This lifted map is unique (Lemma 5). We have thus shown that the reduction map

$$\mathrm{Hom}_R(\widetilde{E}, \widetilde{E}') \to \mathrm{Hom}_k(E, E')$$

is an isomorphism.

A common choice for R in the above theory is $W_n(k)$, the nth truncation of the Witt vectors. By taking a limit over all n, one obtains a formal lift to $W(k)$, and this is algebraic (as all formal curves are). Thus one obtains a canonical lift to $W(k)$. The isomorphism on Hom's remains true at this level. In particular, one sees that the Frobenius morphism of E lifts to a morphism of $\widetilde{E}$ over $W(k)$, and so the generic fiber of $\widetilde{E}$ has complex multiplicaiton. (Note: since E is ordinary, the Frobenius map does not belong to $\mathbf{Z} \subset \mathrm{End}(E)$.)

5. Deligne's theorem

I will briefly explain here one neat application of the canonical lift, given by Deligne in "Variétés abéliennes ordinaires sur un corps fini" (his second paper). Let k be a finite field with q elements. Fix a complex embedding $i\colon W(k)[1/p] \to \mathbf{C}$. Given an ordinary abelian variety A/k of dimension g, one can form its canonical lift $\widetilde{A}/W(k)$, and then the base change $\widetilde{A}_{\mathbf{C}}$ via i. This is an abelian variety over the complex numbers with complex multiplication. One can then take its singular cohomology $\Lambda = \mathrm{H}^1(\widetilde{E}(\mathbf{C}), \mathbf{Z})$. This is a free $\mathbf{Z}$-module of rank $2g$. Furthermore, it has natural endomorphisms F coming from the Frobenius of E.

Let $\mathcal{C}$ be the category of triples (Λ, F), where Λ is a free $\mathbf{Z}$-module of rank $2g$, and F and V are endomorphisms of Λ such that the following conditions hold:

- F is semi-simple and its complex eigenvalues have modulus $q^{1/2}$.
- Half of the eigenvalues of F are p-adic units.
- There exists an endomorphism V of Λ such that $FV = q$.

The above construction defines a functor

$$\{\text{ordinary abelian varieties over } k \text{ of dimension } g\} \to \mathcal{C}.$$

Deligne's theorem is that this is an equivalence of categories.

6. More on ordinary elliptic curves

Using the Serre–Tate theorem, we constructed canonical lifts of ordinary elliptic curves. However, one can go farther and give a useful description of all lifts. Let k be an algebraically closed field and let R be a local artinian ring with residue field k. Suppose E_0/k is an ordinary elliptic curve and E/R is a lift. Let $G_0 = E_0[p^\infty]$ and $G = E[p^\infty]$. The group G has a connected étale sequence, and its connected and étale parts are the unique lifts of the corresponding parts of G_0 to R. The étale part of G or G_0 can be identified with the constant étale sheaf $T_p(E(k)) \otimes \mathbf{Q}_p/\mathbf{Z}_p$. Let $\widehat{G}$ be the formal completion of G; thus $\widehat{G}(S)$, for an R-algebra S, is the kernel of $G(S) \to G(S \otimes_R k)$. Then G^0 can be identified with $\widehat{G}$.

We have a natural map $\widetilde{\varphi}\colon T_p(E(k)) \otimes \mathbf{Q}_p \to \widehat{G}[p^\infty](R)$, defined as follows. Let $x = (x_1, x_2, \ldots)$ be an element of $T_p(E(k))$. Thus $x_i \in E[p^i](k)$ and $px_{i+1} = x_i$. Then $\widetilde{\varphi}(p^{-k} \otimes x)$ is defined to be $p^{i-k}\widetilde{x}_i$ where $i \gg 0$ and $\widetilde{x}_i$ is a lift of x_i. Let us check that this is well-defined. If $\widetilde{x}_i'$ is a second lift then $\widetilde{x}_i - \widetilde{x}_i'$ belongs to $\widehat{G}(R)$, which is annihilated by a fixed power of p. Thus $p^{i-k}\widetilde{x}_i$ is independent of the choice of lift if i is sufficiently large. Next, we have $p^{i+1-k}\widetilde{x}_{i+1} = p^{i-k}\widetilde{x}_i$, where $\widetilde{x}_i = p\widetilde{x}_{i+1}$, and so the definition is independent of the choice of i. Note that if $k = 0$ then $p^i\widetilde{x}_i$ maps to $p^i x_i = 0$ in $G(k)$, and so $\widetilde{\varphi}(x)$ lands in $\widetilde{G}(R)$. Thus $\widetilde{\varphi}$ induces a map $\varphi\colon T_p(E(k)) \to \widehat{G}$. We have a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \widehat{G} & \longrightarrow & G[p^\infty] & \longrightarrow & T_p(E(k)) \otimes \mathbf{Q}_p/\mathbf{Z}_p & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle\varphi} & & \uparrow{\scriptstyle\widetilde{\varphi}} & & \uparrow & & \\
0 & \longrightarrow & T_p(E(k)) & \longrightarrow & T_p(E(k)) \otimes \mathbf{Q}_p & \longrightarrow & T_p(E(k)) \otimes \mathbf{Q}_p/\mathbf{Z}_p & \longrightarrow & 0
\end{array}$$

The upper row is in fact the push-out of the lower row along the map φ. Thus $G[p^\infty]$ is completely determined by φ.

The group $\widehat{G}$ is the Cartier dual of the étale group $T_p(E(k)) \otimes \mathbf{Q}_p/\mathbf{Z}_p$. (For abelian varieties, we'd use the dual abelian variety here.) Thus the Weil pairing induces a pairing $\widehat{G} \times T_p(E(k)) \to \widehat{\mathbf{G}}_m$. Given φ as above, this can be converted into a pairing $T_p(E(k)) \times T_p(E(k)) \to \widehat{\mathbf{G}}_m(R)$. Conversely, given a pairing like this, one obtains a map of group schemes $T_p(E(k)) \to \mathrm{Hom}_R(T_p(E(k)), \widehat{\mathbf{G}}_m) = \widehat{G}$.

We have thus shown that there is a bijection between isomorphism classes of lifts of E to R and pairings $T_p(E(k)) \times T_p(E(k)) \to \mathbf{G}_m(R)$. In particular, the formal deformation space of E is canonically isomorphic to $\widehat{\mathbf{G}}_m$. The identity element corresponds to the canonical lift.