Family of elliptic curves

June 18, 2019

Abstract

In this expository article, we discuss the rigidity, the autoduality, and the deformation of a family of elliptic curves, as in [KM], Chapter 2. In particular, we prove the Serre-Tate theorem, following the one given by Drinfeld in the Section 1 of [Katz].

Contents

1 Abel's Theorem

Let S be an arbitrary scheme. An *elliptic curve* E/S is a proper smooth scheme E over S together with a section $0 : S \to E$, such that each fiber is a geometrically connected genus one curve.

Recall that the relative Picard functor Pic^0 assigned any S-scheme T to the group given by

$$\mathrm{Pic}^0(E \times_S T)/f^*\mathrm{Pic}(T),$$

where the $\mathrm{Pic}^0(E \times_S T)$ is the group of isomorphic classes of line bundles over $E \times_S T$ that is fiberwise degree 0 over T, and $f : E_T \to T$ is the structure morphism. It is known that the functor Pic^0 is representable by a proper smooth group scheme of relative dimension one over S, but we will not assume this in our article.

For each section (S-valued point of E) $P \in E(S)$, we denote by $\mathcal{I}(P)$ to be the ideal sheaf of $P : S \to E$, and $\mathcal{I}(P)^{-1}$ the effective line bundle associated to P.

We start by recalling the Abel's Theorem, which assigning the (unique) group structure to a family of genus one curve over a scheme.

Theorem 1.0.1 (Abel)**.** *There exists a unique structure of commutative group scheme on E/S such that for any S-scheme T, and any three points P, Q, R in $E(T)$, we have $P + Q = R$ if and only if there exists an invertible sheaf $\mathcal{L}_0$ on T and an isomorphism of invertible sheaves on E_T*

$$\mathcal{I}(P)^{-1} \otimes \mathcal{I}(Q)^{-1} \otimes \mathcal{I}(0) \cong \mathcal{I}(R)^{-1} \otimes f^*\mathcal{L}_0.$$

In other words, the map

$$\begin{aligned} E(T) &\longrightarrow \mathrm{Pic}^0(E_T); \\ P &\longmapsto \mathcal{I}(P)^{-1} \otimes \mathcal{I}(0) \end{aligned}$$

induces the unique group structure on E/S.

Assuming the isomorphism of the map $E(T) \to \mathrm{Pic}^0(E_T)$ above, we then deduct the representability of the Picard scheme of the elliptice curve in this case; or in another words, the autoduality of E/S.

Corollary 1.0.2. *The relative Picard functor* Pic^0 *associated to the elliptic curve E/S on the category of schemes over S is representable by E/S itself. Moreover, the pullback functor associated to a S-homomorphism $f : E \to E'$ induces a dual homomorphism $f^t : E' \to E$.*

We use the notation $\mathrm{Pic}^0_{E/S}$ to denote the Picard scheme of E over S. Then the above result give an isomorphism of S-group schemes between E and $\mathrm{Pic}^0_{E/S}$.

2 Rigidity

We then focus on the rigidity of elliptic curves, that is of mixed characteristic setting.

We start by the triviality of deformations of the zero homomorphism.

Lemma 2.0.1. *Let R be a ring, I an ideal of R, p a prime number, such that the ideal (I, p) is nilpotent in R. Let $f : E_1 \to E_2$ is a R-homomorphism of elliptic curves. Assume $f \equiv 0 \mod I$. Then the map f itself is 0.*

Proof. We first assume the ideal (pI, I^2) vanishes in R. Since the multiplication by p map $[p]$ is $fppf$ surjective, it suffices to show the composition $f \circ [p]$ is zero.

Consider the following diagram

$$\begin{tikzcd}
E_1 \arrow[r, "f\circ[p]"] & E_2 \\
\mathrm{Spf}(R[[X]]) \arrow[u] \arrow[r] & \mathrm{Spf}(R[[X]]) \arrow[u]
\end{tikzcd}$$

where the bottom map is the induced morphism of formal groups at zeros. Here the morphism of the formal group has the form

$$X \longmapsto pX + \textit{higher terms} \in (pX, X^2).$$

We then notice that the image of X is contained in the ideal $I\mathcal{O}_{E_2}$. To see this, we base change the diagram above along $\mathrm{Spec}(R/I) \to \mathrm{Spec}(R)$. Then by the assumption $f_0 : E_1/I \to E_2/I$ factors through the zero map. In particular, the map of formal groups associated to f_0 takes the local coordinates $\overline{X}$ to zero in R/I. So the image of X in $R[[X]]$ is contained in the ideal I.

In this way, the map of formal groups associated to $f \circ [p]$ takes X to the ideal (pI, I^2), which vanishes under the assumption. So the map of the formal group factors through the zero map $\mathrm{Spec}(R) \to \mathrm{Spf}(R[[X]])$. Thus by the dominance of the map $\mathrm{Spf}(R[[X]]) \to E_1$ (resp E_2), the image of E_1 along the homomorphism $f \circ [p]$ in E_2 is contained in the closure of the zero. Hence we get the conclusion.

At last, to deal with the general setting, we only notice that we can form the following filtration of ideals

$$I^{(0)} = I;\ I^{(1)} := (pI, I^2);\ \ldots;\ I^{(n+1)} = (pI^{(n)}, (I^{(n)})^2); \ldots.$$

Then by induction we can reduce to the formal setting. □

Theorem 2.0.2 (Rigidity). *Let $f : E_1 \to E_2$ be a S-homomorphism of elliptic curves over S. Then Zariski locally on S, either $f = 0$ or f is an isogeny, i.e. is finite and locally free.*

Proof. Since everything is of finitely presented over S, by the spreading-out technique we may assume $S = \mathrm{Spec}(R)$ for R a finite type algebra over $\mathbb{Z}$.

By the general theory of Hilbert functors, for any two projective schemes X, Y over S, the functor

$$\mathrm{Hom}_S(X, Y)$$

is representable by a separated S-scheme, which is a countable disjoint union of projective schemes over S. Besides, given any two S-morphism $f, g : X \to Y$, by taking the diagonal inside the self fiber product, the locus for $f = g$ is a closed subscheme in S.

Now we apply this to $X = E_1$ and $Y = E_2$. Then the locus for $f = 0$ is a closed subscheme Z of S. It then suffices to show that Z is stable under the generalization, which then implies that Z is open. This is done by taking the direct limit in the Lemma 2.0.1.

At last, over the complement of the zero locus, the map f is fiberwise a homomorphism of elliptic curves over a field that is non-vanishing, which is finite and flat. The map f itself is proper, which combines the above implies that f is finite. So the game is complete by the fiberwise criterion of the flatness for flat schemes of finite presentation over the base, as [Sta] Tag 039E. □

Here we provides two applications with the use of the rigidity.

It is known that a map $f : X \to Y$ of projective smooth varieties over a field will induce a homomorphism of their Picard groups, by pulling back the the degree zero line bundles. In the case when f is a morphism of elliptic curves, the autoduality (namely the isomorphism between elliptic curves and their relative Picard schemes) lead to the observation that any morphism is a homomorphism of group schemes. Precisely, we have

Theorem 2.0.3 (Autoduality). *Let E/S be an elliptic curve. Then the group structure given by the Abel's Theorem 1.0.1 is the unique structure of S-group scheme on E/S, for which the section $0 : S \to E$ is the origin.*

Moreover, any S-morphism of schemes between two elliptic curves $f : E \to E'$ over S with $f(0) = 0$ is a S-group homomorphism.

Proof. For the first part, a S-group structure $K : E \times_S E \to E$ induces an S-automorphism

$$f_P : E \to E;\ Q \mapsto K(P, Q) - P.$$

Since $E \to S$ is a fppf covering, by the base change of E/S along $E \to S$, it suffices to show that $f_P - id : E_E \to E_E$ is equal to zero. This then follows from the Rigidity Theorem 2.0.2, and the observation that on the zero section $E \times 0$, $f_P - id$ vanishes.

For the second part, by spreading out and taking a small enough open subset, we may assume $S = \mathrm{Spec}(A)$ for A a finite type $\mathbb{Z}$-algebra. Then a fppf covering given by the produce of complete local rings at every closed points allows thus to reduce to A is an artin local ring with residue field k, which is of characteristic $p > 0$.

We then discuss two possible cases, where the special fiber $f_0 : E \times k \to E \times k'$ is either equals to 0 or not. In the first case, it is not hard to see that f factors through $E'[p^n] \to E'$, where the former is an affine scheme over S. As E is proper over S, the morphism $E \to E'[p^n]$ is controlled by a ring morphism of global sections, and thus f is constant. For the second case, the fiberwise criterion of flatness [Sta] 039E implies that f is flat; and it is finite since it is proper with finite fibers. So f is locally free of degree N for some $N \in \mathbb{N}$. The Abel's Theorem 1.0.1 produces a homomorphism $f^t : E' \to E$ from the map of Picard groups. We can show that the composition $f^t \circ f$ is the multiplication by N, and the map

$$f_P : E \to E';\ Q \mapsto f(P + Q) - f(P) - f(Q)$$

is constant, taking values in $\ker(f^t)$, which is finite and flat. So $f_P = 0$.

□

Another application is the following, due to Hasse.

Proposition 2.0.4. *Let $f : E \to E'$ be a homomorphism of elliptic curves over a connected base S, and let f^t be its dual (Corollary 1.0.2). Then we have*

$$f^t \circ f = \begin{cases} 0, & if\ f = 0; \\ [N], & if\ f\ is\ an\ isogeny\ of\ degree\ N. \end{cases}$$

Proof. The proof is identical to the proof of the first part of the Theorem 2.0.3, where we use the rigidity to show that $f^t \circ f - [N]$ is zero. □

Corollary 2.0.5. *Let $f : E \to E'$ be a homomorphism of S-elliptic curves.*

(i) If f is an isogeny of degree N, then so is f^t, and $f^{tt} = f$.

(ii) Given another S-homomorphism g, we have

$$(f + g)^t = f^t + g^t.$$

(iii) For any integer $N \in \mathbb{Z}$, we have $[N]^t = [N]$.

(iv) There exists an integer $\mathrm{Tr}(f)$ *(which we call the* trace of f, *such that*

$$f + f^t = [\mathrm{Tr}(f)].$$

Proof. (i) We recall that the degree is multiplicative, which combines with the Proposition 2.0.4 gives the first part. The second part can be done by looking at the composition $f \circ f^t \circ f$, using the fact that any isogeny is fppf surjective.

(ii) Following Hasse, we may regard $f, g, f + g$ as E-valued points of E'. So after the base change, it suffices to prove that for $P, Q \in E(S)$, and $\mathcal{L}$ a line bundle over E', we have the equality on S

$$P^*\mathcal{L} \otimes Q^*\mathcal{L} \cong (P + Q)^*\mathcal{L} \otimes 0^*\mathcal{L}.$$

The statement is invariant after a base change of a line bundle from S, so we may assume $\mathcal{L} = \mathcal{I}(R)^{-1} \otimes \mathcal{I}(0)$. The rest leaves to the reader.

(iii) By the fppf surjectivity of isogenies.

(iv) Consider $\deg(1 + f)$.

□

The next result connects the $\deg(f)$ and $\mathrm{Tr}(f)$ together, by the characteristic polynomial of the given homomorphism

Proposition 2.0.6. *Let $f : E \to E'$ be a S-homomorphism of elliptic curves over a connected base.*

(i) Inside $\mathrm{End}(E)$, *the homomorphism f satisfies*

$$X^2 - [\mathrm{Tr}(f)]X + [\deg(f)] = 0.$$

(ii) We have the equality

$$\mathrm{Tr}(f)^2 \leq 4 \deg(f).$$

Proof. The part two comes from the density of $\mathbb{Q}$ in $\mathbb{R}$, and the computation of a composition with the dual that for any $n, n \in \mathbb{Z}$, we have

$$(n - mf)(n - mf^t) = \deg(n - mf) \geq 0.$$

□

Corollary 2.0.7. *If E is an elliptic curve over a finite field $\mathbb{F}_q$, then we have*

$$|\#E(\mathbb{F}_q) - (q + 1)| \leq 2\sqrt{q}.$$

Proof. Notice that

$$\#E(\mathbb{F}_q) = \deg(1 - F) = (1 - F)(1 - F^t),$$

where F is the Frobenius of $\mathbb{F}_q$. The rest follows from the inequality in the Proposition 2.0.6 above. □

3 Rigidity of level structures

We use the previous results to deduct the rigidity of the level structure.

Corollary 3.0.1. *Let $\epsilon : E \to E$ be an automorphism of an elliptic curve over a connected base S. Then ϵ satisfies the following equation*

$$X^2 - \mathrm{Tr}(\epsilon)X + 1 = 0,$$

with $\mathrm{Tr}(\epsilon)$ *equals to* $0, \pm 1, \pm 2$.

We first deduct the rigidity of $\Gamma(N)$-level structure.

Proposition 3.0.2 (Rigidity of $\Gamma(N)$-level structure)**.** *Let $\epsilon : E \to E$ be an automorphism of an elliptic curve over a connected base S. Let $N \geq 2$ be an integer. Suppose ϵ induces the identity on the sub group scheme $E[N]$. Then we have*

(i) If $N \geq 3$, then $\epsilon = \mathrm{id}$.

(ii) If $N = 2$, then $\epsilon = \pm 1$.

Proof. Since ϵ is the identity on $E[N]$, the homomorphism $\epsilon - \mathrm{id}$ factors through $[N]$, namely

$$\epsilon - \mathrm{id} = [N] \circ f,$$

for some endomorphism f of E/S. So we have

$$\begin{aligned}[N^2 \cdot \deg(f)] &= (\epsilon^t - \mathrm{id})(\epsilon - \mathrm{id}) \\ &= [\deg(\epsilon)] - [\mathrm{Tr}(\epsilon)] + \mathrm{id} \\ &= 2\,\mathrm{id} - [\mathrm{Tr}(\epsilon)].\end{aligned}$$

This implies that

$$N^2 \deg(f) = 2 - \mathrm{Tr}(\epsilon).$$

In the case (i), since $N \geq 3$, by the Corollary 3.0.1 we have $\mathrm{Tr}(\epsilon) = 2$. Take this back to the equation in Corollary 3.0.1, we see ϵ=id.

In the case (ii), when $f = 0$ we have $\mathrm{Tr}(\epsilon)$, and when $\deg(f) = 1$ we have $\mathrm{Tr}(\epsilon) = -2$. Take these back to the equation as above we get $\epsilon = \pm\,\mathrm{id}$. □

The next result is the rigidity of the $\Gamma_1(N)$-level structure.

Proposition 3.0.3 (Rigidity of $\Gamma_1(N)$-level structure)**.** *Let $\epsilon : E \to E$ be an S-automorphism of E/S, where S is connected. Let $N \geq 4$ be an integer and $G \subset E$ a closed subgroup scheme which is finite and locally free of rank N over S. If ϵ induces an identity on G, then either $\epsilon = \mathrm{id}$, or $N = 4$, $G = E[2]$, and $\epsilon = -\,\mathrm{id}$.*

Proof. As the proof of the last Proposition, we see when $N \geq 5$, ϵ has to be the identity. When $N = 4$ and $2 - \mathrm{Tr}(\epsilon) = 0$ or 4, so the only case when ϵ is not the identity is $\epsilon = -\,\mathrm{id}$. Under the latter situation, $\epsilon - \mathrm{id} = -2\,\mathrm{id}$ kills the subgroup G. Thus the rank 4 subgroup G must be the whole $E[2]$. □

Corollary 3.0.4. *Let $\epsilon : E \to E$ be a S-automorphism over the connected base S. Let $N \geq 4$ be an integer, and $G = \mathbb{Z}/N\mathbb{Z} \to E$ (resp. $G = \mu_N \subset E$) be a closed subgroup of E. If ϵ induces the identity on G, then $\epsilon = \mathrm{id}$.*

Proof. As above, the only case when ϵ is not the identity is when $G = E[2]$, which is not isomorphic to either $\mathbb{Z}/N\mathbb{Z}$ or μ_N. □

4 Supersingular elliptic curve

We take some time to discuss the special case when $S = \mathrm{Spec}(k)$ for k being an algebraically closed field in characteristic $p > 0$.

The first one is about the classification of the Tate module $E[p^\infty]$.

Theorem 4.0.1. *Let k be an algebraically closed field of characteristic $p > 0$, E/k an elliptic curve. Then the p-divisible Tate module $E[p^\infty]$ of E is, up to k-isomorphism, one of the following two:*

- *$\mu_{p^\infty} \times \mathbb{Q}_p/\mathbb{Z}_p$;*
- *or the unique 1-parameter formal Lie group over k of height two.*

Before the proof of the result, we first recall the following fact.

Fact 4.0.2 (Classification of p-divisible groups)**.** Let k be an algebraically closed field in characteristic $p > 0$. Then the category of p-divisible groups are semisimple such that for any pair of coprime integers $r, s \in \mathbb{N}$, there exists a simple object of rank r and height s, up to isomorphism.

We refer the [Dem] Chap IV for detailed discussion.

Now we give the proof of the Theorem 4.0.1.

Proof. The statement is essentially an application of the classification of p-divisible groups over an algebraically closed field. By the local-étale decomposition of p-divisible groups, any p-divisible group over an algebraically closed field is the product of a p-divisible commutative Lie group and a finite number of copies of $\mathbb{Q}_p/\mathbb{Z}_p$. So we at least have

$$E[p^\infty] = \hat{E} \times (\mathbb{Q}_p/\mathbb{Z}_p)^a,$$

for some $a \in \mathbb{N}$. Since the multiplication by p map is finite flat of degree p^2, we have

$$\mathrm{height}(\hat{E}) + a = 2.$$

Now we discuss all possible situations. If $\hat{E}$ has height one, then since we are over the algebraically closed field, we have

$$\widehat{E} \cong \widehat{\mathbb{G}}_m = \mu_{p^\infty}.$$

If $\hat{E}$ has height two, then by the uniqueness of rank one formal Lie group of any given height (up to k-isomorphisms), we get the second case. At last, since the multiplication by p can be written as $[p] = F \circ V$, where F is the absolute Frobenius that is purely inseparable, the kernel $E[p]$ has nontrivial local part. This implies that the height of $\widehat{E}$ is at least one. So we are done. □

For an elliptic curve over $k = \overline{k}$ in characteristic p, as in the proof above it is *ordinary* if its $E[p^\infty]$ is isomorphic to the type (i) above, and it is *supersingular* for the second case. This gives a criterion of being ordinary/supersingular in terms of the p-divisible group, or the structure of the subgroup $E[p]$. The next results show the existence and finiteness of supersingular elliptic curves.

Theorem 4.0.3. *In every characteristic $p > 0$, the second case in the Theorem 4.0.1 occurs, and it occurs only a finite number of times.*

Proof.

Existence The existence follows from a classical computation of Hasse invariants. In characteristic 2, the Fermat curve $X^3 + Y^3 + Z^3 = 0$ of degree 3 is supersingular. When $p \geq 3$, we consider the Legendre equation of the ellptic curve,

$$y^2 = x(x-1)(x-\lambda).$$

The Verschiebung morphism $V = F^t : E^{(1)} \to E$ is either étale of degree p, or purely inseparable of degree p, where $E^{(1)}$ is the Frobenius twist of E. So by looking at the tangent map of the V, E is supersingular if and only if the tangent map of V vanishes (Hasse invariant). At last, the result follows from the fact that in terms of the Legendre equation, the Hasse invariant is a polynomial in λ of degree $\frac{p-1}{2}$. Moreover, it is showed by Igusa that this polynomial has distinct roots away from $0, 1, \infty$. Thus there are exactly $\frac{p-1}{2}$ distinct values of λ for $p \geq 3$ where the elliptic curve of the corresponding Legendre equation is supersingular.

Finiteness Though Igusa's computation already implies the finiteness, here we present a fun proof using the rigidity of the level structure, as in [KM].

As in the proof of the Theorem 4.0.1, E is supersingular if and only if the $E[p]$ has trivial étale quotient, or equivalently, the Verschiebung morphism $V = F^t : E^{(1)} \to E$ is purely inseparable of degree p. This implies that the kernel of V and the kernel of $F^{(1)} : E^{(1)} \to E^{(2)}$ coincides, and we get an isomorphism

$$A : E \longrightarrow E^{(2)},$$

which after composing with F fits into the commutative diagram below

$$\begin{tikzcd} & E \arrow[ld, "{[p]}"'] \arrow[rd, "F^2"] & \\ E \arrow[rr, "A"'] & & E^{(2)}. \end{tikzcd}$$

We compose the above maps several times, to get

$$\begin{tikzcd} & E \arrow[ld, "{[p^n]}"'] \arrow[rd, "F^{2n}"] & \\ E \arrow[rr, "A(n)"'] & & E^{(2n)}. \end{tikzcd}$$

Now the idea of the proof is to use the rigidity of the $\Gamma(N)$-level structure to show that the for some $N \geq \mathbb{N}$, the datum E with a $\Gamma(N)$-level structure is defined over $\mathbb{F}_q$, or be "fixed" by a power of Frobenius morphisms.

Let $N, n \in \mathbb{N}$ such that $N \geq 3$ is prime to p, and $p^n \equiv 1 \bmod N$. Then the N-torsion group $E[N]$ is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$, and we fix such an isomorphism $\phi : (\mathbb{Z}/N\mathbb{Z})^2 \to E[N]$. Then y the diagram above, we have

$$\begin{gathered} \phi^{(2n)} = \\ F^{2n} \circ \phi = A(n) \circ [p^n] \circ \phi. \end{gathered}$$

By the choice of N and n, the multiplication by p^n is the identity on $E[N]$, and we get

$$[p^n] \circ \phi = \phi.$$

Thus by composing with the isomorphism $A(n) : E \to E^{(2n)}$, the $2n$-th Frobenius induces the isomorphism of pairs

$$A(2n) : (E, \phi) \longrightarrow (E^{(2n)}, \phi^{(2n)}),$$

where the latter is a $\Gamma(N)$-level structure on $E^{(2n)}$. In this way, the rigidity of the $\Gamma(N)$-level structure Proposition 3.0.2 and the Galois descent(!!) implies that (E, ϕ) is defined over F^{2n}. In particular, the elliptic curve E is defined over $\mathbb{F}_{p^{2n}}$. Thus by the finiteness of choices of coefficients in the universal Weierstrass equation, we get the finiteness.

□

5 Serre-Tate Theorem

The rest of our article devotes to the discussion of the Serre-Tate Theorem, following the Section 2.9 in [KM] and the Section 1 in [Katz].

5.1 The theorem

Let R be a ring, I and ideal of R, and p a prime number, such that (I, p) is nilpotent in R. Assume E_0 is an elliptic curve over $R_0 = R/I$. Then it is natural to ask to the following two questions:

Question 5.1.1. (i) Is there an elliptic curve over R whose reduction mod I equals to E_0?

(ii) If so, how to parametrize all of those lifts?

The answer to the first question is positive, which falls into the smoothness of the deformation space of E_0. We are going to focus on the second questions.

The surprising observation of Serre-Tate is that to give a lift of E_0, it is equivalent to give a lift of its Tate groups. Let $N \geq 1$ be an integer that is divisible by p. Consider the following three categories:

- The category $\mathfrak{A}$, whose objects are elliptic curves $E/\operatorname{Spec}(R)$, with maps being R-homomorphisms.
- The category $\mathfrak{B}_N$, whose objects consist of tuples $(E_0/R_0,\ G,\ (,),\ i)$, where E_0/R_0 is an elliptic curve, $G = \cup_{\nu=0} G[N^\nu]$ is an N-divisible group over R, $(,)$ is a compatible family of alternating autodual pairings $(,)_{N^\nu}$ on $G[N^\nu]$ with
$$(NP, NQ)_{N^{\nu-1}} = ((P, Q)_{N^\nu})^N,$$
and i is an isomorphism of N-divisible groups over R_0 between $E_0[N^\infty]$ and $G \otimes_R R_0$ that carries the canonical pairing e_N to $(,)$ on G. The morphism is defined as morphism of each term compatible with the relation above.
- The category $\mathfrak{C}_N$, whose objects are tuples $(E_0/R_0, G, i)$, where E_0/R_0 is an elliptic curver, G/R is an N-divisible group, and i is an R_0-isomorphism $E_0[N^\infty] \to G \otimes_R R_0$ of N-divisible groups. The morphism is defined as a compatible morphism of pairs.

By the construction, there exists natural functors
$$\mathfrak{A} \longrightarrow \mathfrak{B}_N \longrightarrow \mathfrak{C}_N,$$
where the first one send E/R to its reduction together with its N^∞-torsion group and the canonical pairing e_N, and the second functor is the forgetful functor. The remarkable fact is the following:

Theorem 5.1.2 (Serre-Tate). *The two functors*
$$\mathfrak{A} \longrightarrow \mathfrak{B}_N \longrightarrow \mathfrak{C}_N$$
are all equivalences of categories.

Remark 5.1.3. The theorem can be generalized to abelian schemes of any dimension.

Corollary 5.1.4. *For an elliptic curve E over R, up to isomorphism there exists a unique alternating autodual pairing on $E[N]$ (or a compatible family of pairing on $E[N^\infty]$) that lifts the Weil pairing of $E_0[N]$ (of $E[N^\infty]$), namely the Weil paring e_N.*

Proof. This follows from the equivalence of the forgetful functor $\mathfrak{B} \to \mathfrak{C}$. □

5.2 Proof of the theorem

At last, we prove the Serre-Tate theorem 5.1.2, following that of Drinfeld in [Katz]. As in [Katz], we show the result for abelian schemes, not just of dimension one.

We first fix some notations. Let R be a ring, with N an integer such that N kills the ring R. Let I be an ideal in R with $I^{\nu+1} = 0$. We denote by R_0 to be the quotient ring R/I, and $\pi : \mathrm{Spec}(R_0) \to \mathrm{Spec}(R)$ to be the associated closed immersion.

For any functor of abelian groups G on the category Alg_R of R algebras, we define the subfunctor G_I by

$$G_I(A) := \ker(G(A) \to G(A/IA)).$$

We let $\widehat{G}$ to be another subfunctor defined by

$$\widehat{G}(A) := \ker(G(A) \to G(A_{\mathrm{red}}).$$

Note that G includes all of the presheaves of abelian groups on the category $\mathrm{Sch}_{\mathrm{Spec}(R)}$. This includes for example functors of points representable by abelian schemes or their formal Lie groups.

We start with a lemma showing that in some cases the subfunctor G_I is torsion.

Lemma 5.2.1. *Let G be a functor of commutative formal Lie group over Alg_R. Then the subfunctor G_I is killed by N^ν.*

Proof. The proof is similar to the proof of the Lemma 2.0.1. The idea is to write down the coordinates. Let X_i be the coordinates of G. Since G_I is the kernel of the map $G(-) \to G(- \otimes_R R/I)$, $G_I(A)$ is the subcollection of formal Lie group where each X_i is mapped inside of the ideal I. We use the multiplication by N, to get

$$[N]X_i = NX_i + \textit{higher terms} \in (NI, I^2) = (I^2).$$

So after applying this ν times, since $I^{2^\nu} \subset I^{\nu+1} = 0$, we get the result. □

The main ingredient of the proof of the Serre-Tate theorem is the following observation, which says that up to an isogeny, there exists a canonical lifting for formally smooth abelian group over R.

Lemma 5.2.2. *Let H be an formally smooth fppf abelian sheaf over Alg_R, such that the subfunctor $\widehat{H}$ is locally representable by a formal Lie group. Then there exists a R-homomorphism of fppf abelian sheaves $\widetilde{\iota}(A) : H(A/I) \to H(A)$, such that the composition with the base change map $H(A) \to H(A/I)$ is equal to the multiplication by N^ν.*

Proof. Let A be any R-algebra. By the formal smoothness of G over R, for any A-valued point $x \in G(A/I)$, there exists a lift of x to an A-valued point $y \in G(A)$. We notice that for another such lift y', the difference $y' - y$ is contained in the subfunctor $G_I(A) = \widehat{G}_I(A)$. However, by the Lemma 5.2.1, the subfunctor G_I is killed by the $[N^\nu]$. In particular, the element $N^\nu y$ is independent of the choice of the lift y. This produces a well-defined map

$$\begin{aligned} \iota : \widetilde{N^\nu} H(A/I) &\longrightarrow H(A); \\ x &\longmapsto N^\nu y. \end{aligned}$$

Furthermore, it is clear the map is functorial for $A \in \mathrm{Alg}_R$. Thus we get an R-homomorphism of abelian sheaves

$$\iota : \pi_* H \longrightarrow H,$$

which after the reduction mod I is the multiplication by N^ν. □

The Lemma 5.2.2 allows us to produce a lift for relative situation where the source is N-divisible, and the target is of the type above. Precisely, we have:

Proposition 5.2.3. *Let G and H be two fppf abelian sheaves over Alg_R, such that*

- *The functor G is N-divisible.*

- *The functor H is formally smooth.*
- *The subfunctor $\widehat{H}$ is locally representable by a formal Lie group.*

Denote by G_0 and H_0 to be the functors over Alg_{R_0}, defined by the reduction mod I at G and H separately (i.e. they are the restriction of $\pi_* G$ and $\pi_* H$ at the subcategory $\mathrm{Alg}_{R_0} \subset \mathrm{Alg}_R$). Then we have:

(a) Both the groups

$$\mathrm{Hom}_{R-gp}(G, H), \ \ \mathrm{Hom}_{R_0-gp}(G_0, H_0),$$

are N-torsion free.

(b) The reduction mod I map

$$\mathrm{Hom}_{R-gp}(G, H) \longrightarrow \mathrm{Hom}_{R_0-gp}(G_0, H_0),$$

is injective.

(c) For any R_0-homomorphism $f_0 : G_0 \to H_0$, there exists a unique R-homomorphism $\widetilde{N^\nu f}$, lifting $[N^\nu] \circ f_0$.

(d) Given an R_0-homomorphism $f_0 : G_0 \to H_0$, it can be lifted to an R-homomorphism $f : G \to H$ if and only if the homomorphism $\widetilde{N^\nu f}$ kills the subfunctor $G[N^\nu] := \ker([N^\nu] : G \to G)$ of G.

Before the proof, we note that the Proposition applies when G and H are abelian schemes or their N-divisible groups.

Proof. (a) Since G is N-divisible, the multiplication by N is surjective on G. Note that any homomorphism commutes with the $[N]$, so we get the result.

(b) The kernel of the reduction map consists of those R-homomorphisms $f : G \to H$ that factors through $H_I \to H$, which is killed by $[N^\nu]$ by the Lemma 5.2.1. So any R-homomorphism in the kernel will be killed by $[N^\nu]$, which by the Part (a) must be trivial.

(c) We apply the Lemma 5.2.2 in the following diagram

$$\begin{tikzcd}
G(A) \arrow[r, dotted] \arrow[d] & H(A) \\
G(A/I) = G_0(A/I) \arrow[r, "f_0"] & H(A/I) = H_0(A/I), \arrow[u, "\iota"']
\end{tikzcd}$$

which is functorial with respect to $A \in \mathrm{Alg}_R$. We define the dotted map above as $\widetilde{N^\nu f}$. Then by the construction, $\widetilde{N^\nu f}$ is an R-homomorphism such that the reduction mod I is exactly $[N^\nu] \circ f_0$. The uniqueness follows from the injection in the Part (b)

(d) Assume there exists a lift f, then the composition $[N^\nu] \circ f$ lifts $[N^\nu] \circ f_0$, which by the uniqueness in the Part (c) is identical to $\widetilde{N^\nu f}$. So the map $\widetilde{N^\nu f} = [N^\nu] \circ f$ kills the N^ν-torsion subgroup $G[N^\nu]$.

Conversely, assume $\widetilde{N^\nu f}$ kills the subgroup $G[N^\nu]$. Then $\widetilde{N^\nu f}$ induces an R-homomorphism $g : G/G[N^\nu] \to H$ and we have the following commutative diagram

$$\begin{tikzcd}
G \arrow[rr, "\widetilde{N^\nu f}"] \arrow[dr] & & H \\
& G/G[N^\nu] \arrow[ur, "g"'] & .
\end{tikzcd}$$

But notice that since G is N-divisible, the quotient $G/G[N^\nu]$ equals to G, and we get $g : G \to H$. At last, by taking the reduction mod I, the reduction $g_0 : G_0 \to H_0$ satisfies the condition below

$$g_0 \circ [N^\nu] = f_0 \circ [N^\nu],$$

i.e. $[N^\nu] \circ (f_0 - g_0) = 0$. In this way, by the N-torsion freeness of $\mathrm{Hom}_{R_0-gp}(G_0, H_0)$, we have $g_0 = f_0$, and g is a lift of f_0.

□

Now we are able to prove the Serre-Tate Theorem as follows.

Proof of the Theorem 5.1.2. We first notice that it suffices to prove the equivalence for the composition functor $\mathfrak{A} \to \mathfrak{C}_N$. This is because the functor $\mathfrak{B}_N \to \mathfrak{C}_N$ is the forgetful functor, which is faithful. SInce $\mathfrak{A} \to \mathfrak{C}_N$ factors through $\mathfrak{B}_N \to \mathfrak{C}_N$, the equivalence between $\mathfrak{A}$ and $\mathfrak{C}_N$ implies that $\mathfrak{B}_N \to \mathfrak{C}_N$ is both full and essentially surjective. So we get the equivalence of $\mathfrak{B}_N$ and $\mathfrak{C}_N$.

We then notice that by writing N as $p^n \cdot m$ for m prime to p, it suffices to show the case for p^n, which follows from the similar observation that the functor $\mathfrak{C}_N \to \mathfrak{C}_{p^n}$ is faithful.

Now we focus on the functor $\mathfrak{A} \to \mathfrak{C}_N$ for $N = p^n$, sending an elliptic curves over R to the datum $(E_0/R_0, E[N^\infty], \mathrm{id}_{E[N^\infty]})$.

Fully faithfulness Let A and B be two abelian schemes over R. Assume we have an R_0-homomorphism $f_0 : A_0 \to B_0$ and an R-homomorphism of p-divisible groups $f[p^\infty] : A[p^\infty] \to B[p^\infty]$, which are compatible on $A_0[p^\infty]$. We apply the Proposition 5.2.3 (c) at $(G, H) = (A, B)$, then there exists an R-homomorphism $\widetilde{N^\nu f} : A \to B$, lifting $[N^\nu] \circ f_0$. We restrict this homomorphism to the Tate module $A[p^\infty]$, then we get an R-homomorphism $\widetilde{N^\nu f} : A[p^\infty] \to B[p^\infty]$, lifting $[N^\nu] \circ f_0 : A_0[p^\infty] \to B_0[p^\infty]$. Apply the Proposition 5.2.3 (b) at $(G, H) = (A[p^\infty], B[p^\infty])$, we see the map $\widetilde{N^\nu f}$ equals to $[N^\nu] \circ f[p^\infty]$, which kills the subgroup $A[N^\nu]$. Thus by the Proposition 5.2.3 (d), we can lift the f_0 to an R-homomorphism $f : A \to B$, compatible with $f[p^\infty]$. This proves that the functor $\mathfrak{A} \to \mathfrak{B}$ is full.

The faithfulness follows from the Proposition 5.2.3 (a), applying at $(G, H) = (A, B)$.

Essential surjectivity The idea is similar to the proof of the Lemma 5.2.2. Let $(A_0/R_0, G, i)$ be an object in $\mathfrak{C}_N$. We first recall the existence of the lifting.

Fact 5.2.4. For a given abelian scheme A_0 over R_0, there exists an abelian scheme B over R lifting A_0 along $R \to R/I$.

This essentially follows from the fact the deformation space of an abelian scheme over a field k of positive characteristic is formally smooth over $W(k)$. This then induces an isomorphism

$$\alpha_0 : B_0 \to A_0,$$

which induces a homomorphism of p-divisible groups $\alpha_0[p^\infty] : B_0[p^\infty] \to A_0[p^\infty]$ over R_0. We compose this with the reduction of the isomorphism $i : A[p^\infty] \to G$ along $R \to R/I$, to get an isomorphism

$$j_0 = i_0 \circ \alpha_0 : B_0[p^\infty] \to G_0.$$

Again, by the Proposition 5.2.3 at $(B[p^\infty], G)$, we can get a lift $\widetilde{N^\nu j}$ of $[N^\nu] \circ j_0$. This is not necessarily liftable, since B is not always the one lifting the whole datum $(A_0/R_0, G, i)$. To adjust this, we notice that the kernel $K = \ker(\widetilde{N^\nu j})$ is a finite subgroup of B which lifts the N^ν-torsion subgroup of B_0.

We then have the following claim

Claim 5.2.5. The subgroup scheme K is flat over $\mathrm{Spec}(R)$.

As the base change of the homomorphism $\widetilde{N^\nu j}$ along the zero section $\mathrm{Spec}(R) \to G$, it suffices to show that the homomorphism $\widetilde{N^\nu j}$ is flat. But by the fiberwise criterion of the flatness ([Sta] Tag 039E), since the reduction mod I is flat, we get the result.

Now then the finite subgroup scheme K is flat, we can form the quotient abelian scheme $A := B/K$. The induced homomorphism $g[p^\infty] : A[p^\infty] \to G$ by $\widetilde{N^\nu j}$ is an isomorphism that lifts $j_0 : B_0[p^\infty] = B_0[p^\infty]/B_0[N^\nu] \to G$, which is isomorphic to i_0 by α_0. Thus the abelian scheme A satisfies the condition that the reduction mod I is $B_0 \cong A_0$, and its Tate module $A[p^\infty]$ is isomorphic to G by $g[p^\infty] : A[p^\infty] \to G$, whose reduction is isomorphic to i_0. Hence we are done.

□

Remark 5.2.6. It is easy to forget the Claim 5.2.5 and consider the quotient B/K directly. However, such a quotient may not exist as a scheme over $\mathrm{Spec}(R)$, when the kernel K is not flat.

References

[Dem] M. Demazure. Lectures on p-divisible groups.

[KM] N. Katz; B. Mazur. Arithmetic moduli of elliptic curves. Annals of Mathematics Studies, 108. Princeton University Press, Princeton, NJ, 1985. xiv+514 pp.

[Katz] N. Katz. Serre-Tate local moduli. Algebraic surfaces (Orsay, 197678), pp. 138202, Lecture Notes in Math., 868, Springer, Berlin-New York, 1981.

[Sta] The Stacks Project Authors. Stacks Project, `http://stacks.math.columbia.edu.`