1-ADIC REPRESENTATIONS OF GALOIS GROUPS*

by Raymond T. Hoobler

Let $K$ be a number field and $E$ an elliptic curve defined over $K$. If $E$ has complex multiplications over $K$, that is, if $\text{End}_K(E) \neq \mathbb{Z}$, then the theory of complex multiplications describes certain abelian extensions of the real quadratic number field $\text{End}_K(E) \otimes \mathbb{Q}$. This part of class field theory was classically obtained by consideration of the lattice in $\mathbb{C}$ defining $E$ and the associated elliptic functions [3]. Because of the beautiful blending of algebra and analysis, it must be considered as one of the prime accomplishments of the last century.

Recently Serre has extended the philosophy of this theory to elliptic curves without complex multiplication. More precisely, if $G$ denotes the Galois group of $K$, then $G$ acts naturally on $p^\infty E(K) = \text{Ker}(p_E: E(K) \to E(\bar{K}))$ where $\bar{K}$ is the algebraic closure of $K$. Consequently there is a continuous representation $\rho_p$ of $G$ on $\lim_{\to p} E(K) \cong \hat{\mathbb{Z}}_p \oplus \mathbb{Z}_p$. (The isomorphism is clear if one thinks of $E$ as being defined by a lattice in $\mathbb{C}$). If $G = \rho_p(G) \subset \text{GL}_2(\hat{\mathbb{Z}}_p)$, then $G$ is a closed subgroup of a $p$-adic analytic group and so is an analytic subgroup. Serre has shown [11] that $\mathfrak{g}_p$, the Lie algebra of $G$, is $\text{gl}_2$ if $E$ has no complex multiplications. Consequently $G$ is an open subgroup of the compact group $\text{GL}_2(\mathbb{Z}_p)$. His proof is essentially a case by case examination of the possible subalgebras. A theorem of Šafarevič which rests in turn on a deep theorem of Siegel allows him to eliminate most of the possibilities. The remainder of the McGill notes and some unpublished work of Tate on $p$-divisible groups then eliminate the other awkward case.

The purpose of this note is to introduce a new approach to deformations of abelian varieties and to apply it to the study of $p$-adic representations of $G$ over a local field. This allows us to recover Serre’s results over local fields. In essence, our approach studies elliptic curves over $K$ by first studying them over a finite field where the Frobenius map gives a great deal of information, then lifting the information to characteristic zero by

Research partially supported by the National Science Foundation.
deformation theory and passing to the local field case by Tate’s theorem on Barsotti-Tate groups. In principle there is no reason to restrict our attention to the dimension one case. Tate’s work [12] has considerably clarified this more general situation over finite fields. A version of Proposition 1 which is not restricted to square zero deformations is needed to lift effectively information to characteristic zero, but this is available by using divided power structures. Tate’s theorem on $p$-divisible groups then plays the same role. On the other hand, this requires considerably more of the reader and so I have restricted our attention to the dimension one case.

The prerequisites for understanding this approach are somewhat ambiguous. In general a knowledge of elliptic curves over fields and finite commutative group schemes over fields such as may be found in [7] is required along with a familiarity with the language of schemes and Grothendieck topologies [1, 2]. This and a willingness to accept a couple of theorems on faith should be enough, although some properties of Picard functors which can, I hope, be worked out by the reader are also used. Although the basic notion of a Neron minimal model will be mentioned briefly, the deformation theory aspects of abelian varieties cannot be adequately handled in the language of classical algebraic geometry. I have however restricted myself to deformations of families of elliptic curves for the sake of concreteness. Thus many of the stated results will hold in greater generality.

The results that we obtain are essentially known already, although almost all of the proofs are new. Our approach is rather different from Serre’s in that we deal as much as possible with the group schemes themselves instead of using $p$-adic analysis on their Lie algebras. The deformation theory which is described in the first section may at first sight appear more complicated than the classical deformation theory. But our approach of deforming the functor of points of a scheme is much better suited to the study of arbitrary nilpotent deformations than the more classical approach of deforming the structural equations, since this latter approach is only linear for square zero extensions. My development of this approach to deformation theory was suggested by Grothendieck’s crystalline conjectures [7].

If $X$ is a scheme, $X$ generally indicates the sheaf it defines by its functor of points in whatever topology is being used. Thus $\text{Mor}(S, X)$ is usually denoted $X(S)$.

§1. Preliminaries

Since our approach to the deformation theory of abelian schemes will consist of embedding the abelian scheme in the category of sheaves on an
appropriate Grothendieck topology \([1,2]\) and studying the deformation theory in this larger category, let us begin by defining the sites of interest to us on a given scheme \(S\). The fppf site, \(S_{\text{fppf}}\), is defined as the full subcategory of \((\text{Schemes}/S)\) consisting of those schemes which are flat and locally of finite presentation over \(S\) with the topology generated by the pretopology for which the coverings of \(Y\) are those families \(\{\phi_a: Y_a \to Y\}\) with \(\phi_a\) flat and locally of finite presentation and \(\bigcup \phi_a(Y_a) = Y\). The étale site, \(S_{\text{ét}}\), is defined as the full subcategory of \((\text{Schemes}/S)\) consisting of those schemes which are étale over \(S\) with the topology generated by the pretopology for which the coverings of \(Y\) are those families \(\{\phi_a: Y_a \to Y\}\) with \(\phi_a\) étale and \(\bigcup \phi_a(Y_a) = Y\). Finally we will be interested in the Zariski site, \(S_{\text{Zar}}\), which is the site in which algebraic geometry is usually done. Its category consists of all open immersions into \(S\), and its topology is given by the usual condition that \(\{U_a\}\) is a covering of \(U\) if \(U = \bigcup U_a\). The category of sheaves of abelian groups in any of these sites will be denoted \(\mathcal{T}^*;\). A similar subscript will be used to distinguish the various cohomology and Ext groups. If there is no subscript the fppf topology is to be used. In general, boldface will be used to indicate sheaves on these sites. Note that if \(E\) and \(F\) are commutative flat group schemes which are locally of finite presentation over \(S\), then \(\text{Hom}_{S_{\text{fppf}}}(E, F)\) is by the Yoneda lemma the same as \(\text{Hom}_{S_{\text{pl}}}(E, F)\). Moreover if \(f: T \to S\), then \(f^*(E) \cong E_T\) where we follow the usual convention of denoting \(E \times_S T\) by \(E_T\).

Let \(S\) be a noetherian scheme. An abelian scheme of dimension one over \(S\) is a proper smooth group scheme \(E\) over \(S\) whose fibers are elliptic curves. It is not hard to show that this is the same as giving a proper smooth family of elliptic curves \(E\) over \(S\) together with a section \(0_S: S \to E\) (see the remarks about \(E\) preceding Proposition 1.3). Thus the projective closure in \(P^2_S\) of the cubic \(Y^2 - X(X - 1)(X - \lambda)\) defines an abelian scheme of dimension one over \(S = \text{Spec}(\mathbb{Z}[\lambda, \lambda^{-1}, (\lambda - 1)^{-1}])\). When \(S = \text{Spec} \ A\), \(A\) a discrete valuation ring with quotient field \(K\), there is another more concrete description of abelian schemes in terms of their generic fiber. Suppose \(\text{char } K \neq 2, 3\). Then any elliptic curve \(E\) over \(K\) with a rational point can be written as a nonsingular cubic

\[Y^2 + a_1XY + a_3Y + X^3 + a_2X^2 + a_4X + a_6 = 0\]

with the rational point being the point at infinity. The cubic is nonsingular as long as its discriminant \(\Delta\) is a unit. Such a description is not unique since \(X = u^2X', Y = v^3Y'\) gives a different cubic describing the same curve for units \(u, v \in K\). A Weierstrass minimal model for \(E\) is a cubic with \(a_i \in A\) and
ord $(\Delta)$ minimal. Such a cubic is uniquely determined up to a change of coordinates as above with $u, v$ units in $A$. In particular, $E$ is said to have good reduction at $A$ if $\Delta$ is a unit in $A$ for the Weierstrass minimal model. In this case the cubic defined over $A$ by this equation has an elliptic curve for its closed fiber. If ord $(\Delta) > 0$, then a smooth group scheme over $A$ with generic fiber $E$ can be constructed by removing the singularities of the closed fiber. The resulting group scheme has a closed fiber isomorphic to $G_n$ or $G_m$. This group scheme is also isomorphic to the connected component of the Neron minimal model of $E$. The techniques used in studying the deformation theory of an abelian variety of dimension one with good reduction may also be used to study the deformation theory of this smooth group scheme. This study would, however, lead us astray from our main goal and so will be deferred to another time.

We begin with some elementary facts about abelian schemes. If $E$ is an abelian scheme of dimension one over $S$ and $n$ is an integer, we let $nE: E \to E$ denote multiplication by $n$ and $(nE)_s$ denote the kernel of $nE$. Since $nE$ is proper and $(nE)_s = (E_s)$ is a finite commutative group scheme over $S$ for all $s \in S$, $(nE)$ is finite over $S$. Moreover since $nE$ is an isogeny (= finite, flat, surjective homomorphism of group schemes) on each of the fibers, $(nE)$ is flat [4, IV, 11.3.11] (If $S$ is reduced, this follows more easily from the constancy of the rank of $(nE)$).

If $p$ is a prime, we let $E(p)$ denote the inductive limit scheme $\lim_{\to} nE$. The corresponding fppf sheaf is denoted $E(p)$. This is one of the most important examples of a Barsotti-Tate group [7] (= $p$-divisible group in [13]). For our purposes a Barsotti-Tate group $G$ is an fppf sheaf of abelian groups $G$ where 1) $G$ is a $p$-torsion group on which multiplication by $p$ is surjective, and 2) the kernel of multiplication by $p'$ on $G$ is represented by a finite, flat group scheme $G_p$. Note that $G = \lim_{\to} G_p$. Moreover if $f: T \to S$ and $\lim_{\to} G_p$ is a Barsotti-Tate group over $S$, then $f^*(\lim_{\to} G_p)$ is a Barsotti-Tate group over $T$ since $f^*$ is exact, commutes with inductive limits, and $f^*(G_p) = G_p$.

Now if $S = \text{Spec}(K)$ and $E$ is an abelian variety of dimension one over $K$ where $K$ is a field of characteristic 0, then $pE$ is an étale group scheme over $K$ and so is determined uniquely by giving the action of $G = \text{Gal}(\bar{K}/K)$ on $pE = \mathbb{Z}/p^n\mathbb{Z} \oplus \mathbb{Z}/p^n\mathbb{Z}$. Thus giving $E(p)$ is equivalent to giving a $G$-action on $E(p)(\bar{K}) = \mathbb{Q}_p/\hat{\mathbb{Z}}_p \oplus \mathbb{Q}_p/\hat{\mathbb{Z}}_p$. By Pontrjagin duality this is the same as giving a $G$-action on $\text{Hom}(E(p)(\bar{K}), \mathbb{Q}/\mathbb{Z}) = \lim_{\to} nE(\bar{K}) = \hat{\mathbb{Z}}_p \oplus \hat{\mathbb{Z}}_p$. The resulting $G$-module is denoted by $T_p(E)$, and $V_p(E)$ denotes the $G$-module over $\mathbb{Q}_p$, the $p$-adic rationals, given by $T_p(E) \otimes \hat{\mathbb{Z}}_p$. As indicated above, the purpose of this note is to study the representation of $G$. 

given by $T_p(E)$ when $K$ is a number field and $E$ is an elliptic curve over $K$ with good reduction at primes over $p$.

We begin by fixing a prime number $p$ and proving some elementary results about $\text{Hom}_S(E(p), E(p))$.

**Proposition 1.1.** Let $S$ be a noetherian scheme, $E$ and $F$ abelian schemes of dimension one over $S$. Then

$\text{Hom}_S(E(p), F(p)) \cong \lim_{\leftarrow} \text{Hom}_S\left(\mathbb{Z}_p E, \mathbb{Z}_p F\right)$

is a complete torsion free $\mathbb{Z}_p$ module. If $\text{Hom}_S(E, F)$ is finitely generated, e.g., $S = \text{Spec } K$ with $K$ a field, then

$j: \text{Hom}_S(E, F) \to \text{Hom}_S(E(p), F(p))$

is monic, and the natural monomorphism

$j: \text{Hom}_S(E, F) \otimes \hat{\mathbb{Z}}_p \to \text{Hom}_S(E(p), F(p))$

has a torsion free cokernel.

**Proof.** Since $E(p) = \lim_{\leftarrow} p^n E$ and $F(p) = \lim_{\leftarrow} p^n F$, the isomorphism follows easily. On the other hand

$\text{Hom}_S(E(p), F(p))/(p^n) \text{Hom}_S(E(p), F(p)) \subseteq \text{Hom}_S(p^n E, p^n F)$

and so $\text{Hom}_S(E(p), F(p))$ is a complete module over $\hat{\mathbb{Z}}_p$. Since multiplication by $p$ on $E(p)$ is surjective, this group must be torsion free.

Now suppose $\phi: E \to F$ is a homomorphism containing $p^n E$ in its kernel for any $n$. Since $p^n E_F$ is an isogeny, there is a homomorphism $\phi_{p^n}: E \to F$ with $\phi_{p^n} = \phi$. Thus $\phi = p^n \phi_{p^n}: E \to F$. But $\text{Hom}_S(E, F)$ contains no element which is $p^n$-divisible for any $n$ except 0 and so the map $j$ is monic.

Since $\text{Hom}_S(E, F)$ is a finitely generated abelian group, its $p$-adic completion is $\text{Hom}_S(E, F) \otimes \hat{\mathbb{Z}}_p$ which is embedded into $\text{Hom}_S(E(p), F(p))$. Suppose $\psi = \{\psi_r\} \in \text{Hom}_S(E(p), F(p))$ with $m\psi = \{\phi_r\}$ where $\{\phi_r\}$ is a Cauchy sequence of elements in $\text{Hom}_S(E, F)$; that is, $\phi_r \equiv \phi_{r-1} \mod (p^{r-1} \text{Hom}_S(E, F))$. Since the cokernel of $j$ is a module over $\hat{\mathbb{Z}}_p$, we may assume that $n = p^m$. Then for every $r$, $p^n\psi_r: p^n E \to p^n F$ agrees with the restriction of $\phi_r: E \to F$ to $p^n E$. In particular $p^n E$ is contained in the kernel of $\phi_r$ for every $r$. Just as above, this allows us to conclude that $\phi_r = p^n \phi_r$ for each $r$. Since $\{\phi_r\}$ is a Cauchy sequence, so is $\{\phi_r\}$. But then $\psi - j(\{\phi_r\})$ is an element of order $p^n$ and so must be zero by the first part of the proposition.

Our discussion of the deformation theory of abelian schemes requires the concept of a dual abelian scheme. Let $E$ be an abelian scheme of dimension one over $S$ with structure map $p: E \to S$. Recall that the fppf sheaf
Pic\textsubscript{E/S}: (Schemes /S)\textsuperscript{0} \to (Ab) is defined by Pic\textsubscript{E/S}(T) = \text{Pic}(E_T)/p^\bullet_T (\text{Pic}(T)). L \subseteq \text{Pic}\textsubscript{E/S}(T) is in Pic\textsubscript{0,E/S}(T) if it can be represented by an invertible sheaf on \text{E}_T which is of degree 0 on each fiber \text{E}_t for any geometric point \text{t} \to \text{T}.

Since the degree of an invertible sheaf on \text{E}_T is locally constant, there is an exact sequence of sheaves on \text{S}_{\text{pt}}:

\begin{align}
0 \to \text{Pic}_{E/S}^0 \to \text{Pic}_{E/S} \xrightarrow{\text{deg}} \text{Z}_S \to 0
\end{align}

where \text{Z}_S is the constant sheaf \text{Z} on \text{S}_{\text{pt}}. There is an alternative description of Pic\textsubscript{E/S} which will be useful to us. Let \text{G}_m stand for the sheaf of units on \text{E}_{\text{pt}}. Then \text{R}^1 p_* \text{G}_m is the sheafification of the presheaf \text{T} \to \text{Pic}(E_T). It is easy to see that Pic\textsubscript{E/S} restricted to \text{S}_{\text{pt}} is also \text{R}^1 p_* \text{G}_m, a fact which will be of considerable use to us.

The general theory of Picard schemes shows that Pic\textsubscript{0,E/S} is representable [5], and we denote Pic\textsubscript{0,E/S} by \hat{E}. In our special case, we can use autoduality to identify \hat{E} with \text{E}. A map is constructed in the following manner. Let \Delta(\text{E}) and \text{0}(\text{E}) be the closed subschemes of \text{E} \times \text{S}\text{E} defined by the diagonal map \Delta_{E/S}: \text{E} \to \text{E} \times \text{S}\text{E} and \text{0}_E \times \text{id}: \text{E} \to \text{E} \times \text{S}\text{E}. They are of codimension one and are defined by relative Cartier divisors since this is true on each of the fibers over \text{S} [8]. Let \text{P} be the invertible sheaf on \text{E} \times \text{S}\text{E} defined by \mathcal{O}(\Delta(\text{E})) \otimes \mathcal{O}(\text{0}(\text{E}))^{-1}. This is a family of invertible sheaves of degree zero parametrized by \text{E} through \text{p}_2, projection on the second factor. Let us show that the pair (\text{P}, \text{E}) represents the functor Pic\textsubscript{0,E/S} if \text{S} = \text{Spec} \text{A}, \text{A} a discrete valuation ring. \text{P} \in Pic\textsubscript{0,E/S}(\text{E}) and so defines a map \text{\phi}_p: \text{E} \to Pic\textsubscript{0,E/S}. \text{\phi}_p is an isomorphism over the quotient field \text{K} of \text{A} and the residue field of \text{A} by the autoduality of elliptic curves. (This is an easy application of the Riemann-Roch theorem.) Thus \text{\phi}_p(\text{E}) = Pic^0_{E/S} since the image of \text{E} is closed. Moreover \text{\phi}_p is flat by the local criterion [4, IV, 11.3.11] and so it is an isomorphism. Note that the duality hypothesis follows immediately from the isomorphism \text{E} \cong \hat{E}; that is, the map \text{E} \to \hat{E} defined by the universal bundle on \text{E} \times \hat{E} is an isomorphism.

While the following proposition which describes the deformation theory of homomorphisms of abelian schemes is stated for arbitrary square zero deformations, it will be applied to deformations of the form \text{S}_0 \hookrightarrow \text{S} where \text{S} = \text{Spec}(\text{A}/\text{m}^n), \text{S}_0 = \text{Spec}(\text{A}/\text{m}^{n-1}) and \text{A} is a complete discrete valuation ring. Thus the above remarks apply to an abelian scheme \text{E}_S formed by restricting an abelian scheme over \text{A} to \text{A}/\text{m}^{n-1}.

**Proposition 1.3.** Let \text{i}: \text{S}_0 \hookrightarrow \text{S} = \text{Spec} \text{O} be the closed immersion defined by an ideal \text{I} where \text{O} is a noetherian ring of characteristic \text{p}^n and
Let $E$ and $F$ be abelian schemes of dimension one over $S$. Let $E_0, F_0$ denote $E_{S_0}, F_{S_0}$ respectively. Then there is an exact, commutative diagram

$$
0 \rightarrow \text{Hom}_S(E, F) \rightarrow \text{Hom}_{S_0}(E_0, F_0) \rightarrow \text{Ext}^1_S(E, (R^1 p_*)(p^*I)) \rightarrow 0
$$

In particular, $\ker(j) \subseteq \ker(j_0)$ and the groups $\text{cok}(j), \text{cok}(j_0)$ differ by $p^n$ torsion groups.

**Proof.** If $p : A \rightarrow S$ is an abelian scheme of dimension one over $S$, let $(R^1 p_*(G_m)^0$ be the kernel of the degree map, $\deg : R^1 p_*(G_m) \rightarrow \mathbb{Z}_S$. Then we may assume that $F = (R^1 p_*(G_m)^0$ for an appropriate choice of $A$ by the duality hypothesis $F \cong \hat{F}$. Moreover $i_*(R^1 p_*(G_m, A)^0 = R^1 p_0_*(G_m, A_0)^0$ since $A$ is a flat group scheme locally of finite presentation over $S$, and so it is enough to exhibit the above diagram in terms of sheaves on $\overline{S}_{pl}$.

There is an exact sequence of sheaves on $\overline{A}_{pl}$

$$
0 \rightarrow p^*I \rightarrow G_{m, A} \rightarrow i_A^*G_{m, A_0} \rightarrow 0
$$

where the first map is defined by sending $f \in \Gamma(T, p^*I)$ to $1 + f \in \Gamma(T, G_{m, A})$. This is a unit since $(1 + f)(1 - f) = 1$. The surjectivity follows from noting that for a flat affine scheme $\text{Spec } R$ over $A$, any unit of $R/IR$ comes from a unit of $R$. Since $p_i\mathcal{O}_A = \mathcal{O}_S$ and $p_i i_A^*\mathcal{O}_{A_0} = i_* \mathcal{O}_{S_0}$ where $i_A : A_0 \rightarrow A$, we see that $p_*(G_m, A) \rightarrow p_*(i_A^*G_{m, A_0})$ is onto. Moreover if $f : Y \rightarrow X$ is a closed immersion then $R^1 f_*G_{m, Y} = (0)$. Thus

$$(R^1 p_*)(i_A^*G_{m, A_0}) = R^1(p_0 i_A)_*(G_{m, A_0}) = i_*R^1 p_0_*(G_{m, A_0}),$$

and so we have a sequence

$$
0 \rightarrow R^1 p_*(p^*I) \rightarrow R^1 p_*(G_m, A) \rightarrow i_*R^1 p_0_*(G_{m, A_0}) \rightarrow 0.
$$

Exactness at the first four places follows from the long exact cohomology sequence and the remarks above. Since $p^*I$ is a coherent module on $A_{pl}$, its fppf direct image is determined by its Zariski (usual) direct image $[2]$. Since the fibers of $p$ are one dimensional, $R^2 p_*(p^*I) = 0$, and so the last map is surjective. Since the degree of a line bundle is independent of nilpotent elements in the base, the above sequence defines an exact sequence in $\overline{S}_{pl}$

$$
(1.4) \quad 0 \rightarrow R^1 p_*(p^*I) \rightarrow F \rightarrow i_*F_0 \rightarrow 0.
$$

The rest of the proof is homological algebra in $\overline{S}_{pl}$. Apply the morphism of functors defined from the inclusion of $f_{pl}E$ into $E$. 
\[ \text{Hom}_{S,p}(E, -) \rightarrow \text{Hom}_{S,p}(p^n E, -) \]
to (1.4) to get a diagram (1.5) for each integer \( n \).

\[
\begin{array}{c}
0 \rightarrow \text{Hom}_S(E, R^1 p_*(p^* I)) \rightarrow \text{Hom}_S(E, F) \rightarrow \text{Hom}_S(E, i_* F_0) \\
\downarrow \\
0 \rightarrow \text{Hom}_S(p^n E, R^1 p_*(p^* I)) \rightarrow \text{Hom}_S(p^n E, F) \rightarrow \text{Hom}_S(p^n E, i_* F_0) \\
\downarrow \\
\rightarrow \text{Ext}_S^1(E, R^1 p_*(p^* I)) \\
\downarrow \\
\rightarrow \text{Ext}_S^1(p^n E, R^1 p_*(p^* I)).
\end{array}
\]

Since \( E \) is \( p \)-divisible, \( \text{Hom}_S(E, R^1 p_*(p^* I)) = 0 \). The sequence

\[
\begin{array}{c}
0 \rightarrow \text{Ext}_S^1(E, R^1 p_*(p^* I)) \rightarrow \text{Ext}_S^2(p^n E, R^1 p_*(p^* I)) \\
\rightarrow \text{Ext}_S^2(E, R^1 p_*(p^* I))
\end{array}
\]

defined from \( 0 \rightarrow p^n E \rightarrow E \rightarrow E \rightarrow 0 \) is exact for \( n > N \) since then \( p^n \) annihilates \( R^1 p_*(p^* I) \). But the sequences (1.6) fit together into a projective system coming from the projective system of short exact sequences

\[
\begin{array}{c}
0 \rightarrow p^n E \rightarrow E \rightarrow E \rightarrow 0 \\
\downarrow \\
0 \rightarrow p^{n+1} E \rightarrow E \rightarrow E \rightarrow 0.
\end{array}
\]

Thus the maps from the last group of (1.6) to the last group of (1.6) is multiplication by \( p' \). Consequently

\[ \text{Ext}_S^1(E, R^1 p_*(p^* I)) \cong \lim_{\leftarrow} \text{Ext}_S^1(p^n E, R^1 p_*(p^* I)). \]

Replacing \( E \) by \( E(p) \) (which is still \( p \)-divisible) in the above argument shows that

\[ \text{Ext}_S^1(E(p), R^1 p_*(p^* I)) \cong \lim_{\leftarrow} \text{Ext}_S^1(p^n E, R^1 p_*(p^* I)) \]

and that \( \lim_{\leftarrow} \text{Hom}_S(p^n E, R^1 p_*(p^* I)) = 0 \). Now taking the projective limit of (1.5) gives the exact, commutative diagram (1.7) since the Mittag-Leffler condition is satisfied for \( \text{Hom}_S(p^n E, R^1 p_*(p^* I)) \). Note that \( \text{Hom}_S(E, i_* F_0) \) is naturally isomorphic to \( \text{Hom}_S(E_0, F_0) \) and similarly for \( \text{Hom}_S(p^n E, i_* F_0) \).
Finally $\text{Hom}_S(E(p), F) \rightarrow \text{Hom}_{S_0}(E_0(p), F_0) \rightarrow \text{Ext}^1_S(E, R^1 p_*(p^*I))$.

\[(1.7) \quad \rightarrow \text{Hom}_S(E, F) \rightarrow \text{Hom}_{S_0}(E_0, F_0) \rightarrow \text{Ext}^1_S(E, R^1 p_*(p^*I)).\]

Finally $\text{Hom}_S(E, F) = \text{Hom}_S(E_0, F_0)$ and so $\text{Hom}_S(E(p), F) = \text{Hom}_S(E(p), F(p))$. Similarly $\text{Hom}_{S_0}(E_0(p), F_0) = \text{Hom}_{S_0}(E_0(p), F_0(p))$. Putting this information into (1.7) gives the diagram in the statement of the proposition.

Since $R^1 p_*(p^*I)$ is $p^\infty$ torsion so are the Ext groups in (1.7). Thus a simple diagram chase finishes the proof of the proposition.

§2. Local theory

We can now handle the local case. Let $K$ be a field of characteristic 0 which is complete with respect to a discrete valuation $v$. Let $O_v$ be the valuation ring and suppose it has a finite residue field $k$ containing $q = p^r$ elements and is unramified. Let $m_v$ be the maximal ideal of $O_v$. Let $S_n = \text{Spec}(O_v/m_v^{n+1})$. If $E$ is an abelian scheme over $\hat{S} = \text{Spec} O_v$ let $E_n = E \times S_n$, etc. The next result will let us pass from $S_n$ to $\hat{S}$.

**Proposition 1.8.** Let $E$ and $F$ be abelian schemes of dimension one over $\hat{S} = \text{Spec} O_v$.

1) The natural map $\text{Hom}_{\hat{S}}(E, F) \rightarrow \lim_{\leftarrow} \text{Hom}_{S_n}(E_n, F_n)$ is an isomorphism.

2) The natural map $\text{Hom}_{\hat{S}}(E(p), F(p)) \rightarrow \lim_{\leftarrow} \text{Hom}_{S_n}(E_n(p), F_n(p))$ is an isomorphism.

**Proof.** 1) Since $F \cong \hat{F}$ with universal bundle $P$ on $F \times F$ defined by $\mathcal{O}(\mathcal{L}(E)) \otimes \mathcal{O}(\mathcal{L}(E))^{-1}$, it will be enough to prove that the natural map is an isomorphism when $F = \hat{F}$ and $F_n = \hat{F}_n$. If $\{\phi_n\}$ is a compatible system of maps, $\phi_n : E_n \rightarrow \hat{F}_n$, then $\phi_n$ is determined by the line bundle

$$L_n = (F_n \times \phi_n)^*(P_n) \in \text{Pic}(F_n \times E_n).$$

The compatibility of the $\phi_n$'s shows that $L_n \otimes O_v/m_v^{n+1} \cong L_{n-1}$. But then the sequence of line bundles $\{L_n\}$ determines a formal line bundle on $F \times E$ and Grothendieck's algebraization theorem [4, III, 5.1.4] asserts the existence of a unique line bundle $L$ on $F \times E$ with the property that $L|_{F_n \times E_n} \cong L_n$. Since $L_n|_{F_n \times \{0\}} = \mathcal{O}_{F_n}$, $L|_{F \times \{0\}} = \mathcal{O}_F$. Consequently $L$ determines a map $\phi_L : E \rightarrow \text{Pic}_F$ and $\phi_L(0) = 0$. Since $E$ is connected, $\phi_L(E)$ is contained in the connected component of the identity which by (1.2) is $\text{Pic}_{\text{c}} = \hat{F}$. Since $L|_{F_n \times E_n} \cong \hat{F}_n$, $\phi_L|_{E_n} = \phi_n : E_n \rightarrow \hat{F}_n$. Finally $\phi_L$ is a homomorphism because
each of the diagrams below commute, so the arrows from the upper left to the bottom right define the same invertible sheaves on $F_n \times E_n \times E_n$.

\[
\begin{array}{c}
E_n \times E_n \\
m_{E_n}
\end{array}
\begin{array}{c}
\phi_n \times \phi_n \\
\rightarrow
\end{array}
\begin{array}{c}
F_n \times \hat{F}_n \\
m_{F_n}
\end{array}
\begin{array}{c}
E_n \\
\phi_n
\end{array}
\begin{array}{c}
\rightarrow
\end{array}
\begin{array}{c}
\hat{F}_n
\end{array}
\]

By the uniqueness in the algebraization theorem, the corresponding diagram for $E \times E, E, \hat{E} \times \hat{F}, \hat{F}$ must commute. Similarly $\phi_L$ preserves the inverse map.

In order to finish 1), we must show that the only homomorphism $\phi: E \to \hat{F}$ which is zero on $E_n$ for all $n$ is the zero map. If $\phi_K: E_K \to \hat{F}_K$ is non-zero, then it must be onto since the image is closed, connected, and not a point. But then $\phi(E)$ is a closed subset of $\hat{F}$ containing the generic fiber of $\hat{F}$. Hence $\phi(E) = \hat{F}$. In particular the restriction of $\phi$ to $E_0$, the closed fiber of $E$, is a surjection onto $\hat{F}_0$ and so $\phi_0 \neq 0$.

2) We will show that $\text{Mor}_S(E(p), F(p)) = \lim \text{Mor}_S(\text{pr}_E, E_n, \text{pr}_F)$ is isomorphic to

\[
\lim_n \text{Mor}_S(E_n(p), F_n(p)) = \lim_n \lim_r \text{Mor}_S(\text{pr}_E, E_n, \text{pr}_F)
\]

Now there is an isomorphism $\text{Mor}_S(H, G) \cong \lim \text{Mor}_S(H_n, G_n)$ which holds for any finite, flat group scheme $H, G$ over $\hat{S}$. If $H = \text{Spec}(A(H))$ and $G = \text{Spec}(A(G))$, this isomorphism follows by observing that $A(H)$ and $A(G)$ being finite $O_v$-algebras are complete in the $v$-adic topology and so

$\text{Hom}_{O_v\text{-alg}}(A(G), A(H))$

\[
\cong \lim \text{Hom}_{(O_v/m_v^{n+1})\text{-alg}}((A(G)/m_v^{n+1}A(G)), (A(H)/m_v^{n+1}A(H))).
\]

Applying this isomorphism with $H = \text{pr}_E$ and $G = \text{pr}_F$ and then taking projective limits over $r$ will give us the desired isomorphism between morphisms of Barsotti-Tate groups over $\hat{S}$ and over $S_n$. This shows that the natural map in 2) is monic. The surjectivity follows by noting that a compatible system of homomorphisms $\phi_n: E_n(p) \to F_n(p)$ lifts to a unique morphism $\phi: E(p) \to F(p)$. The uniqueness of the lifting shows, just as in 1), that $\phi$ is actually a homomorphism.
Before proving the main result of this section we need to recall some definitions concerning $E_0$, an abelian variety of dimension one over the residue field $k$ of $O_v$. $E_0$ is said to be supersingular if any of the following equivalent conditions [7] are satisfied:

ss1) $\text{End}_k(E_0)$ is an order in a quaternion algebra over $\mathbb{Q}$ which is split at $p$ and $\infty$ where $\bar{k}$ is the algebraic closure of $k$.

ss2) $\rho_p E_0$ is a local-local group scheme for some (any) $n$.

ss3) $F_E = nE$ for some integer $n$ where $F_E$, the Frobenius map on $E$, is the identity map on the topological space $E$ and raises functions on $E$ to their $p$th power.

If $E_0$ is non supersingular, then $\text{End}_k(E_0)$ is an order in a quadratic extension of $\mathbb{Q}$ and $\rho_p E_0$ decomposes into an étale subgroup scheme and a local subgroup scheme for any $n$ [7]. Finally $E$ is said to have complex multiplications defined over $K$ if $\text{End}_K(E_K) \neq \mathbb{Z}$.

**Theorem 1.9.** Let $E$ be an abelian scheme of dimension one over $S$ with no complex multiplications, where $S = \text{Spec}(\mathcal{A})$, etc., is as above and $G = \text{Gal}(K/k)$.

1) If $E_0$ is non supersingular, then

$$j_K : \text{End}_k(E_0) \otimes \hat{\mathbb{Z}}_p \to \text{End}_G(T_p(E_K))$$

is an isomorphism.

2) If $E_0$ is supersingular, then

$$j_K : \text{End}_k(E_0) \otimes \hat{\mathbb{Z}}_p \to \text{End}_G(T_p(E_K))$$

is either an isomorphism or has a torsion free cokernel of rank one.

**Proof.** We begin by reducing the theorem to the corresponding assertion over $S$. Thus Tate’s theorem on Barsotti-Tate groups [13] shows that $\text{End}_S(E(p))$ is isomorphic to $\text{End}_G(T_p(E_K))$. If we recall that $E \cong \hat{E}$, then $\phi \in \text{Mor}_S(\hat{E}, \hat{E})$ restricts to the zero map over $K$ only if the line bundle $(E \times \phi)^*(P)$ on $E \times_S \hat{E}$ corresponding to $\phi$ is trivial over $E_K \times_k E_K$. The kernel of $\text{Pic}(E \times_S E) \to \text{Pic}(E_K \times_k E_K)$ is generated by divisors which are multiples of the special fiber of $E \times_S E$. Since these are divisors of functions, we conclude that $\text{End}_S(\hat{E}) \to \text{End}_k(\hat{E}_K)$ is monic. Given $\psi \in \text{End}_k(\hat{E}_K)$, it corresponds to a line bundle $(E_K \times_k \psi)^*(P)$ on $E_K \times_k \hat{E}_K$. Represent this line bundle as a sum of divisors and then take the closure of the divisors in $E \times_S \hat{E}$ to produce a line bundle $L$ on $E \times_S \hat{E}$ which restricts to $(E_K \times_k \psi)^*(P)$ on $E_K \times_k \hat{E}_K$. $L$ defines $\psi_L : \hat{E} \to \text{Pic}_{E/\mathcal{S}}$ and $(\psi_L)_K = \psi$. Consequently $\psi_L$ factors thru $\hat{E}$. This map $\hat{E} \to \hat{E}$ is a homomorphism since the appropriate diagrams $\hat{E} \times_S \hat{E} \to \hat{E}$ commute by an argument analogous to that showing
the monotonicity above. Thus $\text{End}_S(E) \cong \text{End}_K(E_k)$. In view of this, the diagram (1.10) below will reduce the theorem to calculations over a finite field when it is shown to be exact.

$$
0 \to \text{End}_S(E) \otimes \hat{\mathbb{Z}}_p \to \text{End}_S(E_0) \otimes \hat{\mathbb{Z}}_p \\
\downarrow j \quad \quad \downarrow j_0 \quad \quad i \downarrow \\
0 \to \text{End}_S(E(p)) \to \text{End}_S(E_0(p))
$$

(1.10)

The commutativity of (1.10) is clear. $j$ and $j_0$ are monic by Proposition 1.1. We see that $\text{End}_S(E_n(p))$ and $\text{End}_S(E_n) \otimes \hat{\mathbb{Z}}_p$ are contained in $\text{End}_S(E_0(p))$ and $\text{End}_S(E_0) \otimes \hat{\mathbb{Z}}_p$ respectively by using induction on $n$ and applying Proposition 1.3 to the square zero deformation $S_{n-1} \to S_n$. Moreover, once we have shown that $j_0$ is an isomorphism, Proposition 1.1 and Proposition 1.3 together with induction show that

$$j_n : \text{End}_S(E_n) \otimes \hat{\mathbb{Z}}_p \to \text{End}_S(E_0(p))$$

is an isomorphism. Consequently Proposition 1.8 shows that

$$\text{End}_S(E) \otimes \hat{\mathbb{Z}}_p \to \lim (\text{End}_S(E_n) \otimes \hat{\mathbb{Z}}_p)$$

must be a monomorphism and it is an isomorphism if and only if $j$ is an isomorphism.

Proposition 1.1 will show that $j_0$ is an isomorphism if the ranks over $\mathbb{Z}$ and $\hat{\mathbb{Z}}_p$ of $\text{End}_S(E_0)$ and $\text{End}_S(E_0(p))$ respectively are the same. Now multiplication by $p$ on $E_0(p)$ is surjective and so we have an exact sequence

$$0 \to \text{End}_S(E_0(p)) \to \text{End}_S(E_0(p)) \to \text{Hom}_S(pE_0, E_0(p)).$$

Since $\text{Hom}_S(pE_0, E_0(p)) = \text{Hom}_S(pE_0, E_0)$, the rank of $\text{End}_S(E_0(p))$ is less than or equal to $\dim_{\mathbb{Z}/p\mathbb{Z}}[\text{End}_S(pE_0)]$. In the non supersingular case, $pE_0 = (pE_0)_{\text{et}} \oplus (pE_0)_{\text{loc}}$, where $(pE_0)_{\text{et}}$ and $(pE_0)_{\text{loc}}$ are étale and local group schemes respectively of rank $p$. Consequently the dimension of $\text{End}_S(pE_0)$ is less than or equal to $p + p$. But the rank of $\text{Hom}_S(E_0, E_0)$ is at least 2 since the Frobenius map is not multiplication by any number. Thus the rank of $\text{End}_S(E_0(p))$ must be 2 and the map $\text{End}_S(E_0) \otimes \hat{\mathbb{Z}}_p \to \text{End}_S(E_0(p))$ is an isomorphism. In the supersingular case, $pE_0$ is a local-local group scheme of rank $p^2$. Consequently $\text{End}_S(E_0(p))$ has rank $\leq 4$. If $\text{End}_S(E_0)$ has all of its complex multiplications defined over $S_0$, then it is of rank 4 and so we can conclude as above. In any case there is a finite extension field $\mathbb{k}$ of $k$ over which all of the complex multiplications are defined. Thus, over Spec $\mathbb{k}$, the map is an isomorphism. But if $G(\mathbb{k}/k)$ is the Galois group of this finite extension, then
\[ \text{End}_k(E_0) \otimes \hat{\mathbb{Z}}_p \] \( G^{(E/k)} = \text{End}_k(E_0) \otimes \hat{\mathbb{Z}}_p = \text{End}_k(E_0) \otimes \hat{\mathbb{Z}}_p \) and similarly for \( \text{End}_s(E_0(p)) \). Hence the map is an isomorphism and the rank of \( \text{End}_k(E_0(p)) \leq 4 \) with equality if and only if all of the complex multiplications of \( E_0 \) are defined over \( k \).

Suppose \( E_0 \) is non supersingular. If the rank of \( \text{End}_s(E(p)) \) is two, then \( F \) lifts to an endomorphism of \( E(p) \). Thus \( F \) lifts to an element of \( \text{End}_s(E_n) \) for each \( n \) and so defines an element in \( \text{End}_s(E) \) by Proposition 1.8. Since it cannot be multiplication by an integer, the rank of \( \text{End}_s(E) \) must be two, and so \( j \) is an isomorphism. On the other hand if the rank of \( \text{End}_s(E(p)) \) is one, \( j \) is clearly an isomorphism.

Suppose \( E_0 \) is supersingular. The theorem will follow from Proposition 1.1 if we show that the rank of \( \text{End}_s(E(p)) \) is either one or two. If the rank of \( \text{End}_s(E(p)) \) is four, then \( \text{End}_s(E(p)) \) equals \( \text{End}_s(E_0(p)) \) and so by Proposition 1.8 any endomorphism of \( E_0 \) lifts to an endomorphism of \( E \). But \( \text{End}_k(E) \) is commutative and so this cannot happen. In order to finish the proof we will show that \( \text{End}_s(E(p)) \otimes \hat{\mathbb{Z}}_p Q_p \) is a simple ring and so \( \text{End}_s(E(p)) \otimes \hat{\mathbb{Z}}_p Q_p \) is its own commutant in \( M_2(Q_p) = \text{End}_s(E_0(p)) \otimes \hat{\mathbb{Z}}_p Q_p \). In particular \( \text{End}_s(E(p)) \) must be \( \hat{\mathbb{Z}}_p \) or an order in a quadratic extension of \( Q_p \).

So suppose \( \phi \in \text{End}_s(E(p)) \otimes \hat{\mathbb{Z}}_p Q_p \) and \( \phi^2 = \phi \) or \( \phi^2 = 0 \) with \( \phi \neq 0, \pm 1 \). Then for some \( r \), \( p^r \phi = \phi \in \text{End}_s(E(p)) \) and either \( \phi^2 = p^r \phi \) or \( \phi^2 = 0 \). If \( \phi(p) = 0 \), then \( \phi = p \phi_1 \) and \( \phi_1 \) satisfies one of these conditions while being nonzero and not \( \pm 1 \). Since \( \text{End}_s(E(p)) \) is a finitely generated \( \hat{\mathbb{Z}}_p \) module, there will be \( \psi \in \text{End}_s(E(p)) \) with \( \psi \neq 0, \pm 1 \) and \( \psi^2 = 0 \) or \( \psi^2 = p^r \psi \) for some \( r \) and \( \psi(p)E \neq 0 \). Clearly \( \psi|_{pE} : pE \to pE \) cannot be an isomorphism and so \( K_1 = \text{Ker} \left( \psi \right) \) is a finite group scheme over \( S \) whose generic fiber has rank \( p \). If \( \text{A}(K_1) \) denotes the Hopf algebra of the group scheme \( K_1 \) over \( O_v \), then \( \text{A}(K_1) = \text{A}(K_1) / \text{tors}(\text{A}(K_1)) \) is also a Hopf algebra where \( \text{tors}(\text{A}(K_1)) \) is the Hopf ideal of \( O_v \)-torsion elements in \( \text{A}(K_1) \). Since it is a torsion free \( O_v \) module it is a free \( O_v \)-module. Let \( \overline{K}_1 = \text{Spec} \left( \text{A}(K_1) \right) \). Then \( \overline{K}_1 \) is a finite, flat commutative group scheme over \( O_v \) of rank \( p \) and there is a closed immersion \( K_1 \hookrightarrow \overline{K}_1 \). Reducing everything mod \( m_v \), we find that \( \overline{K}_1 \) is a finite flat commutative group scheme over \( S_0 \) which must be local-local since \( pE_0 \) is local-local. Since its rank is \( p \) it is simple. But the only simple finite flat commutative group scheme of local-local type is \( \alpha_p \), the kernel of the Frobenius on the additive group. Interestingly enough, there are no liftings of \( \alpha_p \) to characteristic zero unramified discrete valuation rings [10] and so \( \overline{K}_1 \) cannot exist. This contradiction shows that \( \text{End}_s(E(p)) \) is simple.
Corollary 1.11. If $E$ has supersingular reduction then $T_p(E)$ is an irreducible $G$-module.

Proof. Suppose $T$ is a $G$-submodule of $T_p(E)$. Then it determines a Barsotti-Tate group $T' = \text{Hom}(T, \mathbb{Q}_p) \otimes \mathbb{Z}_p)$ over $K$. By Tate's theorem [14], there is a Barsotti-Tate group $\overline{E}$ over $S$ and an inclusion $\overline{E} \to E(p)$ with $\overline{E}_K \approx T'$ and the inclusion restricting to the inclusion of $T'$ in $E_K(p)$.

Moreover, $\overline{E}$ is represented by $\overline{E}_1$ which must be of rank $p$ since $\overline{E} \neq E(p)$.

But then the argument at the end of the theorem shows that $\overline{E}_1$ is a lifting of $\alpha_p$ which is impossible.

Remark. Let $G$ be the image of $G$ in $\text{Aut}(V_p(E_K)) = GL_2(\mathbb{Q}_p)$. Serre [12] has shown that a closed subgroup of a $p$-adic analytic group is analytic. Hence $G$ is a $p$-adic analytic subgroup. The above procedures allow us to identify $\mathfrak{g}$, the Lie algebra of this group, with a subalgebra of $\mathfrak{sl}_2$ and so up to finite index, the group itself with a subgroup of $GL_2(\mathbb{Z}_p)$. If $E$ has formal complex multiplications, that is, if $\text{End}_{O_v}(E(p)) \neq \mathbb{Z}_p$ for some discrete valuation ring $O_v$ which is finite over $O$, then $\mathfrak{g}$ is a Cartan subalgebra of $\mathfrak{gl}_2$. If $E$ has no formal complex multiplications and has supersingular reduction, then $\mathfrak{g} = \mathfrak{sl}_2$. If $E$ has no formal complex multiplications and has non supersingular reduction, then $\mathfrak{g}$ is a Borel subalgebra. The first statement follows since $G$ is, possibly after a base extension, commutative and $V_p(E_K)$ is semi-simple. The second assertion follows since $V_p(E_K)$ is a simple $\mathfrak{g}$-module with $\text{End}_G(V_p(E_K)) = \mathbb{Q}_p$. Thus $\mathfrak{g}$ is either $\mathfrak{sl}_2$ or $\mathfrak{gl}_2$. The $\mathfrak{sl}_2$ case is eliminated since $\Lambda^2 V_p(E_K)$ is $G$-isomorphic to $(\lim_{\nu} \mu_p^\nu) \otimes \mathbb{Z}_p \otimes \mathbb{Q}_p$ where $\mu_p$ is the group of $p$th roots of unity in $K$. The last assertion follows from the observation that the étale group schemes $(\mu_p E_0)_{el}$ lift uniquely to étale group schemes $(\mu_p E)_{el}$ over $S$ [14]. Thus there is a short exact sequence of Barsotti-Tate groups

$$0 \to (E(p))_{\text{loc}} \to E(p) \to (E(p))_{\text{et}} \to 0$$

which defines a short exact sequence of $G$-modules via Tate’s theorem

$$0 \to T_p(E)_{\text{loc}} \to T_p(E) \to T_p(E)_{\text{et}} \to 0.$$


