Chapter V. The Deformation Theory and Applications

§1. Notation (1.1) Let S be a scheme with p locally nilpotent on it, I a quasi-coherent ideal of $\mathcal{O}_S$ endowed with locally nilpotent divided powers. Let $S_o = \mathrm{Var}(I)$ so that $S_o \hookrightarrow S$ is an object of the crystalline site of S_o. Denote by $\mathrm{B.T.}'(S_o)$ the full sub-category of $\mathrm{B.T.}(S_o)$ consisting of those G_o's which can locally (for Zariski) be lifted to a G in $\mathrm{B.T.}(S)$.

Remark (1.2) The definition of $\mathrm{B.T.}'(S_o)$ adopted above differs from that of [IV (2.1)]. The reason for this is that we shall in this chapter usually not be concerned with the crystals per se but rather only with their values on particular objects of the crystalline site (i.e., $S_o \hookrightarrow S$). By [IV (2.2)] it is clear that with the new definition of $\mathrm{B.T.}'(S_o)$ the values of what would be the crystals $\mathbb{E}(G_o)$, $\overline{\mathbb{E}}(G_o)$, $D(G_o)$ are all defined on $S_o \hookrightarrow S$. Again it is appropriate to refer to the comments made in the introduction, ...

Notation (1.3) For G_o in $\mathrm{B.T.}'(S_o)$ the symbols $\mathbb{E}(G_o)_S$, $\overline{\mathbb{E}}(G_o)_S$, $D(G_o)_S$ refer to the values of the appropriate crystals on $S_o \hookrightarrow S$ as explained in (1.2). Thus locally on S, $\mathbb{E}(G_o)_S$ is the universal extension $E(G)$ of any lifting of G_o to S and similarly for $\overline{\mathbb{E}}(G_o)_S$, $D(G_o)_S$.

Definition (1.4) A filtration $\mathrm{Fil}^1 \subseteq D(G_o)_S$ is said to be admissible if Fil^1 is a locally-free vector sub-group with locally-free quotient, which reduces to $\underline{V}(G_o) \hookrightarrow \underline{\mathrm{Lie}}\,(E(G_o))$ on S_o.

(1.5) We define an obvious category whose objects are pairs (G_o, Fil^1) with G_o in $\mathrm{B.T.}'(S_o)$, Fil^1 an admissible filtration on $D(G_o)_S$. Morphisms are defined as pairs (u_o, ξ) where $u_o : G_o \longrightarrow H_o$ and ξ is a morphism of filtered objects, i.e., a commutative diagram

$$\begin{array}{ccc} \mathrm{Fil}^1 & \hookrightarrow & D(G_o)_S \\ \downarrow{\scriptstyle \xi} & & \downarrow{\scriptstyle D(u_o)_S} \\ \mathrm{Fil}^1 & \hookrightarrow & D(H_o)_S \end{array}$$

which reduces on S_o to

$$\begin{array}{ccc} \underline{V}(G_o) & \hookrightarrow & \underline{\mathrm{Lie}}\,(E(G_o)) \\ \downarrow{\scriptstyle \underline{V}(u_o)} & & \downarrow{\scriptstyle \underline{\mathrm{Lie}}\,(E(u_o))} \\ \underline{V}(H_o) & \hookrightarrow & \underline{\mathrm{Lie}}\,(E(H_o)) \end{array}$$

Having introduced all the terminology and notation, the following theorem can be stated.

Theorem (1.6) The functor $G \longmapsto (G_o, \underline{V}(G) \hookrightarrow \underline{\mathrm{Lie}}\,(E(G)) = D(G_o)_S)$ establishes an equivalence of categories:

$$\mathrm{B.T.}(S) \xrightarrow{\sim} \text{category of pairs } (G_o, \mathrm{Fil}^1).$$

Prior to proving the theorem some preliminary remarks are necessary.

Remark (1.7) 1) Let G_o be in $\mathrm{B.T.}'(S_o)$. On S there is defined a (Zariski) sheaf of sets $\mathcal{L}$ in the following way: For an affine open $U \subseteq S$ $\Gamma(U, \mathcal{L})$ = set of linear equivalence classes of prolongations of $\underline{V}(G_o)|U_o \hookrightarrow E(G_o)|U_o$ to a vector subgroup $V' \hookrightarrow \mathbb{E}(G_o)_S|U$ [III 2.7.2].

It is immediate that this definition gives us a sheaf on the affine open sets and hence can be extended to give a sheaf on S.

2) By the construction of $\mathbb{E}(G_o)_S$ it is clear that $\mathscr{L}$ has a canonical section $\Theta \in \Gamma(S, \mathscr{L})$ which is determined on any sufficiently small affine open set U by the equivalence class of $\underline{V}(G)$ where G is any lifting of $G_o|U_o$ to U. In fact from [IV 2.2] if G_1 and G_2 are two liftings of $G_o|U_o$ there is a commutative diagram:

$$\begin{array}{ccc} \underline{V}(G_1) & \hookrightarrow & E(G_1) \\ {\scriptstyle w}\downarrow & & \downarrow{\scriptstyle v} \\ \underline{V}(G_2) & \xrightarrow{i} & E(G_2) \end{array}$$

with $i \circ w - v|\underline{V}(G_1)$ an exponential. This says exactly that $i \circ w$ and $v|\underline{V}(G_1)$ are linearly equivalent.

3) If G is a global lifting of G_o, then $E(G) \xrightarrow{\sim} \mathbb{E}(G_o)_S$ (canonically) and hence $\underline{V}(G)$ gives us an element in Θ (i.e., a distinguished vector subgroup in the linear equivalence class of prolongations of $\underline{V}(G_o)$).

4) Recall that by [III 2.7.7] to give a $V \subseteq \mathbb{E}(G_o)_S$ which belongs to Θ is precisely equivalent to the giving of an admissible filtration $\mathrm{Fil}^1 \hookrightarrow D(G_o)_S$. In particular to know $\underline{V}(G) \hookrightarrow \mathbb{E}(G_o)_S$ where G is as in 3), is the same as knowing $\underline{V}(G) \hookrightarrow D(G_o)_S$. But from knowing $\underline{V}(G) \hookrightarrow \mathbb{E}(G_o)_S$, G can be reconstructed via $G \xrightarrow{\sim} \mathbb{E}(G_o)_S / \underline{V}(G)$.

(1.8) Proof of (1.6): We prove successively that the functor is:

1) faithful

2) full

3) essentially surjective.

1) Let G and H be two B.T. groups on S and $u, v: G \longrightarrow H$, be two homomorphisms. By taking their difference we are led to show that if $u_o: G_o \longrightarrow H_o$ is the zero map and if $\underline{\mathrm{Lie}}\,(E(u)): \underline{\mathrm{Lie}}\,(E(G)) \longrightarrow \underline{\mathrm{Lie}}\,(E(H))$ is the zero map, then u is the zero map. This is a local question and hence S can be assumed to be affine. Since $\underline{V}(u)$ is zero, as follows from the commutative diagram

$$\begin{array}{ccc} \underline{V}(G) & \hookrightarrow & \underline{\mathrm{Lie}}\,(E(G)) \\ \downarrow & & \downarrow \\ \underline{V}(H) & \hookrightarrow & \underline{\mathrm{Lie}}\,(E(H)) \end{array}$$

it follows that both $E(u): E(G) \longrightarrow E(H)$ and $0: E(G) \longrightarrow E(H)$ can be used to fill in the dotted arrow to give a commutative diagram:

$$\begin{array}{ccc} \underline{V}(G) & \hookrightarrow & E(G) \\ \downarrow & & \vdots \\ \underline{V}(H) & \hookrightarrow & E(H) \end{array}$$

Thus by [IV 2.2] $E(u) = 0$ and hence $u = 0$.

2) Let $u_o: G_o \longrightarrow H_o$ and $\beta: \underline{V}(G) \longrightarrow \underline{V}(H)$ be given such that $\beta_o = \underline{V}(u_o)$ and the following diagram commutes:

$$\begin{array}{ccc} \underline{V}(G) & \hookrightarrow & \underline{\mathrm{Lie}}\,(E(G)) \\ \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle D(u_o)_S} \\ \underline{V}(H) & \hookrightarrow & \underline{\mathrm{Lie}}\,(E(H)) \end{array}$$

We must find a $u: G \longrightarrow H$ lifting u_o with $\beta = \underline{V}(u)$. Because of the faithfulness proved above it suffices to consider the case in which S is affine. Let us apply [IV 2.2] so as to obtain $E_S(u_o): E(G) \longrightarrow E(H)$. Then $E_S(u_o)|\underline{V}(G) - i \circ \beta$ (i being the inclusion $\underline{V}(H) \hookrightarrow E(H)$) is an exponential. Applying $\underline{\mathrm{Lie}}$ to this homomorphism gives zero since $\underline{\mathrm{Lie}}\,(E_S(u_o)) = D(u_o)_S$. This means $E_S(u_o)|\underline{V}(G) = i \circ \beta$ and hence passing to the quotient we obtain a map u which lifts u_o.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & V(G) & \longrightarrow & E(G) & \longrightarrow & G & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle E_S(u_o)} & & \downarrow{\scriptstyle u} & & \\ 0 & \longrightarrow & V(H) & \longrightarrow & E(H) & \longrightarrow & H & \longrightarrow & 0 \end{array}$$

Since $E(u) = E_S(u_o)$, β must be $\underline{V}(u)$ and thus the functor is full.

3) Let $(G_o, \mathrm{Fil}^1 \hookrightarrow D(G_o)_S)$ be given. The problem is to construct from this data a B.T. group G which gives rise to it when our functor is applied. By the fourth remark of (1.7) the giving of $\mathrm{Fil}^1 \hookrightarrow D(G_o)_S$ is the same as giving $V \in \mathfrak{B}$, $V \hookrightarrow \mathbb{E}(G_o)_S$ lifting $\underline{V}(G_o) \hookrightarrow E(G_o)$. Assume for the moment that $\mathbb{E}(G_o)_S/V = G$ is a Barsotti-Tate group. Constructing its universal extension, there is a map

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \underline{V}(G) & \longrightarrow & E(G) & \longrightarrow & G & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & V & \longrightarrow & \mathbb{E}(G_o)_S & \longrightarrow & G & \longrightarrow & 0 \end{array}$$

Since $G = \mathbb{E}(G_o)_S/V$ restricts on S_o to $E(G_o)/\underline{V}(G_o) = G_o$, it is clear (because both extensions restrict to the universal extension for G_o) that $\underline{V}(G) \longrightarrow V$ restricts to an isomorphism. By restricting to an affine open set of S and using the nilpotence of I and the flatness of V it is clear that $\underline{V}(G) \longrightarrow V$ is an isomorphism. (This is essentially Nakayama.) Thus the above mapping of extensions is an isomorphism and by taking $\underline{\mathrm{Lie}}$ of the left-hand square we find $(G_o, \mathrm{Fil}^1 \hookrightarrow D(G_o)_S)$ is isomorphic to $(G_o, V(G) \hookrightarrow \underline{\mathrm{Lie}}\,(E(G)))$.

Hence we have reduced ourselves to proving $G = \mathbb{E}(G_o)_S/V$ is a Barsotti-Tate group. This is a local question on S and hence S can be assumed to be affine with $p^N \cdot 1_S = 0$, and furthermore it may be assumed that G_o can be lifted to S.

Under these hypotheses $\mathbb{E}(G_o)_S$ is a direct limit of groups $E(n)$ which are flat of finite presentation over S. In fact if G' lifts G_o so $E(G') \xrightarrow{\sim} \mathbb{E}(G_o)_S$, take $E(n) = E(G') \underset{G'}{\times} G'(n)$ to obtain groups which satisfy the statement. Because V is quasi-compact and $\mathbb{E}(G_o)_S = \varinjlim E(n)$, $V \hookrightarrow E(n)$ for $n \gg 0$, and thus $G = \varinjlim E(n)/V$ (the direct limit being taken over n sufficiently large). By construction $E(n)/V|S_o = G_o(n)$ and hence is representable. From [G.A. III §2, 7.1] it follows that $E(n)/V$ is representable. This quotient is affine since modulo a

nilpotent ideal it is and is furthermore flat and of finite presentation [S.G.A.3 VI b 9.2 xi, xiii]. Let $G\langle n\rangle = E(n)/V$ so that $G = \varinjlim G\langle n\rangle$ and $G\langle n\rangle|S_o = G_o(n)$. Let $S = \mathrm{Spec}\,(A)$, $G\langle n\rangle = \mathrm{Spec}\,(B_n)$. Since B_n/IB_n is a finite A/I module, the nilpotence of I implies that B_n is a finite A-module. By [E.G.A. IV 1.4.7] $G\langle n\rangle$ is a finite locally-free S group.

To show G is a Barsotti-Tate group, it must be shown that G is of p-torsion, is p-divisible and that the $G(n)$ are finite and locally-free. To see G is of p-torsion observe that by [III 2.2.6] $I\cdot B_n^{\vee} \cap \underline{\mathrm{Lie}}\,(B_n) \xrightarrow{\sim} \mathrm{Ker}\,[\Gamma(S, G\langle n\rangle) \longrightarrow \Gamma(S_o, G\langle n\rangle)]$ and that the analogous statement is true when S is replaced by a T which is flat over S. Since $\Gamma(S_o, G\langle n\rangle) = \Gamma(S_o, G_o(n))$ is killed by p^n and the left side $IB_n^{\vee} \cap \underline{\mathrm{Lie}}\,(B_n)$ is killed by p^N, $\Gamma(S, G\langle n\rangle)$ is killed by p^{N+n}. Because $G\langle n\rangle$ is flat over S, this implies p^{N+n} kills $G\langle n\rangle$. Hence G is of p-torsion.

Since multiplication by p on $\mathbb{E}(G_o)_S$ maps $E(n+1)$ to $E(n)$, multiplication by p on G induces a map $G\langle n+1\rangle \longrightarrow G\langle n\rangle$ which reduces to $G_o(n+1) \xrightarrow{p} G_o(n)$. This last map is an epimorphism and thus by [E.G.A. IV 11.3.11] the map $G\langle n+1\rangle \longrightarrow G\langle n\rangle$ is faithfully flat and hence an epimorphism. Clearly this implies that $G = \varinjlim G\langle n\rangle$ is p-divisible.

Let us observe that with the $E(n)$ chosen as above that the kernel of p^n on $\mathbb{E}(G_o)_S$ is contained in $E(n)$ and hence $V \longrightarrow \mathbb{E}(G_o)_S$ factors through $E(N)$. Since $G(n) = \mathrm{Ker}\ p^n$ on $\mathbb{E}(G_o)_S/V$ it is obvious that $G(n)$ is contained in the image of $\mathrm{Ker}\left(p^{n+N}\cdot \mathrm{id}_{\mathbb{E}(G_o)_S}\right)$ and hence

$G(n) \subseteq G\langle n+N\rangle$. Consider the following cartesian square:

$$\begin{array}{ccc} G\langle n+N\rangle & \xrightarrow{p^n} & G\langle N\rangle \\ \uparrow & & \uparrow \\ G(n) & \longrightarrow & S \end{array}$$

Since $p^n: G\langle n+N\rangle \longrightarrow G\langle N\rangle$ is an epimorphism, it follows that $G(n)$ is flat of finite presentation over S. $G(n)$ is in fact finite over S since modulo the nilpotent ideal I it becomes equal to $G_o(n)$ which is certainly finite. Thus just as above in the case of $G\langle n\rangle$, $G(n)$ is finite and locally-free. This completes the proof that G is a Barsotti-Tate group and hence the proof of the theorem as well.

(1.9) The notation being that of (1.0), let us indicate how the results of this section are to be modified so as to apply to abelian schemes. By [IV 2.8.1] the crystals $\mathbb{E}(A_o)$, $\overline{\mathbb{E}}(A_o)$, $D(A_o)$ are defined for all abelian schemes A_o on S_o. The notation $\mathbb{E}(A_o)_S$, $\overline{\mathbb{E}}(A_o)_S$, $D(A_o)_S$ will indicate the values of these crystals on the object $S_o \hookrightarrow S$ of the crystalline site of S_o. The definition of an admissible filtration, (1.4), carries over without change. The category of pairs (A_o, Fil^1) is defined in the same way as in (1.5). Remark (1.7) also is repeated without change in this context. Finally we have:

Theorem (1.10) The functor $A \longmapsto (A_o, \underline{V}(A) \hookrightarrow \underline{\mathrm{Lie}}\,(E(A)))$ is an equivalence of categories between the category of abelian schemes on S

and the category of pairs (A_o, Fil^1) with A_o an (arbitrary) abelian scheme on S_o and Fil^1 an admissible filtration on $D(A_o)_S$.

Proof: That the functor is faithful and full is proved exactly as in (1.8). To prove it is essentially surjective, we reason in the same way as in the proof of the corresponding statement of (1.8). Thus we are led to show that if $V \hookrightarrow \mathbb{E}(A_o)_S$ is a vector subgroup lifting $\underline{V}(A_o) \hookrightarrow E(A_o)$, then $A = \mathbb{E}(A_o)_S / V$ is an abelian scheme on S.

Locally on S, A is representable by [G.A.III §2, 7.1] since A reduces to the abelian scheme A_o on S_o. Because A is a sheaf, it follows that A is representable. By [S.G.A. 3 VI B 9.2 xii, xiii] $A \longrightarrow S$ is smooth and of finite presentation. $V \hookrightarrow \mathbb{E}(A_o)_S$ is a closed immersion because A_o being separated over S_o implies that $\underline{V}(A_o) \hookrightarrow E(A_o)$ is a closed immersion. Thus A is separated over S [S.G.A. 3 VI B 9.2 (x)]. Since A is separated and of finite type over S, it follows immediately that A is proper over S because A_o is proper over S_o and this certainly implies that $A \longrightarrow S$ is universally closed. Because the fibers of $A \longrightarrow S$ are the same as those of $A_o \longrightarrow S_o$, it is clear that A is an abelian S-scheme.

§2. (2.0) Let S_o be a scheme with p locally nilpotent on it. For any abelian scheme A_o on S_o, let $\bar{A}_o$ denote its associated Barsotti-Tate group [I (3.4)]. Because of the way in which $\bar{A}_o$ is defined it is obvious that [IV 2.8.1] implies that $\bar{A}_o$ can always be locally lifted so that $\bar{A}_o$

belongs to $\mathrm{B.T.}'(S_o)$ in the notation of [IV 2.1]. The following theorem will be of critical importance in proving the Serre-Tate theorem on lifting abelian schemes.

Theorem (2.1) There is a canonical homomorphism of crystals in groups $\mathbb{E}(\bar{A}_o) \longrightarrow \mathbb{E}(A_o)$ which induces an isomorphism of crystals $D(\bar{A}_o) \xrightarrow{\sim} D(A_o)$. This homomorphism is functorial in A_o and is compatible with all base changes.

Proof: Let $U_o \hookrightarrow U$ denote an object of the crystalline site. We are to define a homomorphism $\mathbb{E}(\bar{A}_o)_U \longrightarrow \mathbb{E}(A_o)_U$ which induces an isomorphism when "Lie" is applied to it (or more precisely to the associated map of formal Lie groups). Both the source and the target are f.p.p.f. sheaves on U. Hence it suffices to define the homomorphism locally on U (for the Zariski topology) provided we can show that these local definitions patch together. Hence we first turn to the problem of giving the local definition.

Local definition: S_o and S can be assumed affine, with S_o defined by an ideal I having nilpotent divided powers and such that p^N kills S. Let A and B be two liftings of A_o so that $\bar{A}$ and $\bar{B}$ (the associated B.T. groups) are two liftings of $\bar{A}_o$. Recall the universal extension of A by $\underline{V}(A)$ is obtained via $\alpha: A(n) \longrightarrow \underline{V}(A)$ from the extension:

$$(*) \qquad 0 \longrightarrow A(n) \longrightarrow A \xrightarrow{p^n} A \longrightarrow 0 \qquad (n \geq N)$$

Similarly the universal extension of $\bar{A}$ by $\underline{V}(\bar{A}) = \underline{V}(A)$ is obtained via α

from the extension

$$(**) \qquad 0 \longrightarrow A(n) \longrightarrow \bar{A} \xrightarrow{p^n} \bar{A} \longrightarrow 0$$

Thus we conclude the universal extension of $\bar{A}$ by $\underline{V}(A)$ is obtained from that of A by $\underline{V}(A)$ by pulling back along $\bar{A} \hookrightarrow A$. This means there is the following commutative diagram in which the right-hand square is cartesian:

$$(2.1.1) \qquad \begin{array}{ccccccccc} 0 & \longrightarrow & \underline{V}(A) & \longrightarrow & E(\bar{A}) & \longrightarrow & \bar{A} & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \varphi_A} & & \downarrow & & \\ 0 & \longrightarrow & \underline{V}(A) & \longrightarrow & E(A) & \longrightarrow & A & \longrightarrow & 0 \end{array}$$

Of course there is a completely analogous diagram for the situation arising from B. By [IV 2.2] and the analogous statement for abelian schemes, there are canonical isomorphisms

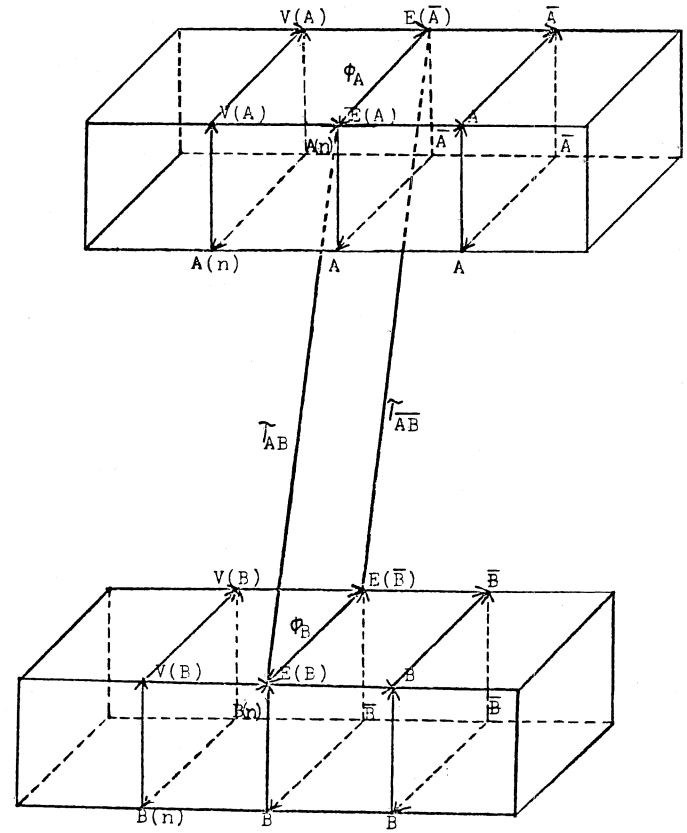
$$(2.1.2) \qquad \tau_{\bar{A}\bar{B}} : E(\bar{A}) \xrightarrow{\sim} E(\bar{B})$$

$$(2.1.3) \qquad \tau_{AB} : E(A) \xrightarrow{\sim} E(B)$$

We want to show that the following square is commutative:

$$(2.1.4) \qquad \begin{array}{ccc} E(\bar{A}) & \xrightarrow{\tau_{\bar{A}\bar{B}}} & E(\bar{B}) \\ \downarrow{\scriptstyle \varphi_A} & & \downarrow{\scriptstyle \varphi_B} \\ E(A) & \xrightarrow{\tau_{AB}} & E(B) \end{array}$$

Since $E(\bar{A})$ is the amalgamated sum of $\bar{A}$ and $\underline{V}(A)$, to show



(2.1.5)

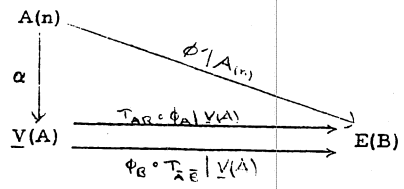
$\tau_{AB} \circ \varphi_A = \varphi_B \circ \tau_{\bar{A}\bar{B}}$ it suffices to show that both mappings have the same restriction to $\bar{A}$ and to $\underline{V}(A)$.

First let us deal with the restrictions to $\bar{A}$. It is immediately checked (see accompanying diagram) that $\tau_{AB} \circ \varphi_A \big| \bar{A}$ and $\varphi_B \circ \tau_{\bar{A}\bar{B}} \big| \bar{A}$ both reduce on S_o to the natural map $\bar{A}_o \hookrightarrow A_o \longrightarrow E(A_o)$. This means that (denoting by i the inclusion $i: S_o \hookrightarrow S$)

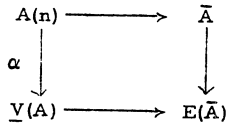
$\left(\tau_{AB} \circ \varphi_A - \varphi_B \circ \tau_{\bar{A}\bar{B}}\right) \Big| \bar{A}: \bar{A} \longrightarrow$ Ker where Ker denotes the kernel of the mapping $E(B) \longrightarrow i_* i^*(E(B))$. But as has been seen in the proof of [IV 2.2] this kernel (or at least its restriction to flat arguments) is killed by p^N. Again just as in the proof of [IV 2.2] this implies $\mathrm{Hom}(\bar{A}, \mathrm{Ker}) = 0$ as $\bar{A}$ is p-divisible. Hence $\tau_{AB} \circ \varphi_A$ and $\varphi_B \circ \tau_{\bar{A}\bar{B}}$ have the same restriction to $\bar{A}$. Let this common restriction be denoted by φ'.

Let us examine the restrictions of $\tau_{AB} \circ \varphi_A$ and $\varphi_B \circ \tau_{\bar{A}\bar{B}}$ to $\underline{V}(A)$. Consider the following diagram:

(2.1.6)



Since



is commutative it is immediate that both horizontal maps make the diagram commutative. Furthermore, both

horizontal maps have the same restriction to S_o: namely $\underline{V}(A_o) \hookrightarrow E(A_o)$. Let $g: \underline{V}(A) \longrightarrow \underline{V}(B)$ be any linear lifting of $\underline{V}(A_o) \xrightarrow{\text{id.}} \underline{V}(A_o)$ (since S is affine and $\underline{V}(A)$ is projective such a lifting exists). By the way in which τ_{AB} was constructed it is clear that $\tau_{AB} \circ \varphi_A \big| \underline{V}(A) = \tau_{AB} \big| \underline{V}(A)$ is the composite of $\underline{V}(A) \xrightarrow{g} \underline{V}(B)$ with $\underline{V}(B) \hookrightarrow E(B)$, plus an exponential. On the other hand $\varphi_B \circ \tau_{\bar{A}\bar{B}} \big| \underline{V}(A) = \varphi_B \circ (\underline{V}(A) \xrightarrow{g} \underline{V}(B) \hookrightarrow E(\bar{B})$ + an exponential). An exponential from $\underline{V}(A)$ to either $E(B)$ or $E(\bar{B})$ factors through their common formal Lie group. (The fact that they have a common formal Lie group follows immediately from [IV 1.2.1], the analogous statement for abelian schemes, and the obvious fact that $\bar{B}$ and B have the same formal Lie group.) It is thus clear that $\varphi_B \circ$ (an exponential) is an exponential and thus $\tau_{AB} \circ \varphi_A \big| \underline{V}(A)$ differs from $\varphi_B \circ \tau_{\bar{A}\bar{B}} \big| \underline{V}(A)$ by an exponential. Therefore applying [IV 2.6.3] it follows that $\tau_{AB} \circ \varphi_A \big| \underline{V}(A) = \varphi_B \circ \tau_{\bar{A}\bar{B}} \big| \underline{V}(A)$.

This gives us the local definition of our mapping. The passage from the above local definition to a global one is now immediate. For, in effect, we've shown that the morphisms we have defined locally are independent (up to canonical isomorphism) of all choices. Since the morphism $\varphi_A: E(\bar{A}) \longrightarrow E(A)$ when restricted to an open subset U of S gives $\varphi_{A|U}: E(\overline{A|U}) \longrightarrow E(A|U)$, it is obvious that because the sources and targets patch together the morphisms will also. This gives us our definition of $\mathbb{E}(\bar{A}_o)_{S_o} \hookrightarrow S \longrightarrow \mathbb{E}(A_o)_{S_o} \hookrightarrow S$. Because we are dealing with crystals it is again immediate that these morphisms are compatible

and hence give us the desired morphism of crystals $\mathbb{E}(\bar{A}_o) \longrightarrow \mathbb{E}(A_o)$.

It is now immediate that the induced homomorphism $D(\bar{A}_o) \longrightarrow D(A_o)$ is an isomorphism. In fact the question is local and hence the statement follows from the observation that the middle vertical arrow in the following diagram is an isomorphism (since the two ends are):

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \underline{V}(A) & \longrightarrow & \underline{Lie}\,(E(\bar{A})) & \longrightarrow & \underline{Lie}\,(\bar{A}) & \longrightarrow & 0 \\ & & \| & & \downarrow\wr & & \downarrow\wr & & \\ 0 & \longrightarrow & \underline{V}(A) & \longrightarrow & \underline{Lie}\,(E(A)) & \longrightarrow & \underline{Lie}\,(A) & \longrightarrow & 0 \end{array}$$

See [IV 1.2.2] where it was observed that the above sequences are exact.

Also, the fact that the above morphism of crystals is compatible with base change is obvious from the manner in which the inverse image of crystals is constructed [III 3.8] and the explicit local definition of the morphism (using [IV 2.4.4]).

Finally to show the functoriality of the morphism $\mathbb{E}(\bar{A}_o) \longrightarrow \mathbb{E}(A_o)$, it is clearly sufficient to show that when S and S_o are affine (p^N kills S, ...) and liftings A of A_o, B of B_o are given, then for any homomorphism $u_o : A_o \longrightarrow B_o$, the following diagram commutes:

(2.1.7)
$$\begin{array}{ccc} E(\bar{A}) & \xrightarrow{E_S(\bar{u}_o)} & E(\bar{B}) \\ {\scriptstyle \varphi_A}\downarrow & & \downarrow{\scriptstyle \varphi_B} \\ E(A) & \xrightarrow{E_S(u_o)} & E(B) \end{array}$$

(Here $E_S(\bar{u}_o)$ and $E_S(u_o)$ are the unique morphisms whose existence is

guaranteed by [IV 2.2]. This is the notation which was used in [IV 2.4.1]).

To prove the commutativity of (2.1.7) we reason as above where the special case involving τ_{AB} and $\tau_{\bar{A}\bar{B}}$ was proven. Namely if in (2.1.5) τ_{AB} and $\tau_{\bar{A}\bar{B}}$ are replaced by $E_S(u_o)$ and $E_S(\bar{u}_o)$, it is clear that $(E_S(u_o) \circ \varphi_A)|\bar{A}$ restricts on S_o to $\bar{A}_o \longrightarrow A_o \xrightarrow{u_o} B_o \longrightarrow E(B_o)$ (using the analogue of the commutative diagram [IV 2.7.2] for abelian schemes). On the other hand $\varphi_B \circ E_S(\bar{u}_o)|\bar{A}$ restricts on S_o to $\bar{A}_o \xrightarrow{\bar{u}_o} \bar{B}_o \longrightarrow E(\bar{B}_o) \longrightarrow E(B_o)$. Since these composites are obviously equal, the reasoning applied above (in the case with τ_{AB} and $\tau_{\bar{A}\bar{B}}$) show $E_S(u_o) \circ \varphi_A|\bar{A} = \varphi_B \circ E_S(\bar{u}_o)|\bar{A}$.

To conclude the proof that $E_S(u_o) \circ \varphi_A = \varphi_B \circ E_S(\bar{u}_o)$ it suffices to show both maps have the same restriction to $\underline{V}(A)$.

But both restrictions to $\underline{V}(A)$ when pulled back to S_o become $\underline{V}(A_o) \xrightarrow{\underline{V}(u_o)} \underline{V}(B_o) \hookrightarrow E(B_o)$. The rest of the reasoning used in the special case $\tau_{AB} = E_S(u_o)$, $\tau_{\bar{A}\bar{B}} = E_S(\bar{u}_o)$ goes through word for word (changing g to be a linear lifting of $\underline{V}(u_o)$ of course). This completes the proof of the theorem.

(2.2) We shall prove the theorem of Serre-Tate on lifting abelian schemes. Let us first recall its statement. Let S be a scheme with p locally nilpotent on it and let I be a locally nilpotent quasi-coherent ideal of $\mathcal{O}_S$. Set $S_o = \mathrm{Var}(I)$. Consider the category of pairs $(A_o, \bar{A})$ con-

sisting of an abelian scheme A_o on S_o and a Barsotti-Tate group $\bar{A}$ on S which lifts $\bar{A}_o$, the Barsotti-Tate group associated to A_o. Morphisms between $(A_o, \bar{A})$ and $(B_o, \bar{B})$ are defined to be pairs $(u_o, \bar{u})$ where $u_o: A_o \longrightarrow B_o$ is a homomorphism and $\bar{u}: \bar{A} \longrightarrow \bar{B}$ is a homomorphism lifting $\bar{u}_o$.

Theorem (Serre-Tate) (2.3): The functor $A \longmapsto (A \times_S S_o, \bar{A})$ is an equivalence of categories between the category of abelian schemes on S and the above defined category of pairs.

We proceed to prove the theorem via a series of reduction steps.

Lemma (2.3.1) It suffices to prove the theorem locally on S. More precisely if we can find a basis for the open sets of S such that the theorem is true for each set in the basis, then the theorem is true.

Proof: Let $\{U_i\}$ be such a basis. We prove successively that the functor is faithful, full, and essentially surjective.

1) faithful: Let $u, v: A \longrightarrow B$ be homomorphisms of abelian schemes such that $u_o = v_o: A_o \longrightarrow B_o$ and $\bar{u} = \bar{v}: \bar{A} \longrightarrow \bar{B}$ ("o" denotes reduction to S_o and "$\bar{\ }$" denotes passage to the associated B.T. group). Restricting to each U_i, it is clear that $u|U_i = v|U_i$ since the theorem is assumed true for U_i and since reducing to S_o and taking the associated B.T. group commutes with localization. This obviously implies $u = v$.

2) full: Let $u_o: A_o \longrightarrow B_o$, $\bar{u}: \bar{A} \longrightarrow \bar{B}$ be given where A and B are abelian schemes on S. Assume of course that $(\bar{u})_o = \bar{u}_o$. For each U_i, by hypothesis there is a unique $u_i: A|U_i \longrightarrow B|U_i$ which gives rise

to $u_o|U_i$ and $\bar{u}|U_i$. By this uniqueness $u_i|U_i \cap U_j$ and $u_j|U_i \cap U_j$ must agree on all open sets U_k in our base which are contained in $U_i \cap U_j$. Thus u_i and u_j agree on $U_i \cap U_j$ and therefore patch together to give a morphism $u: A \longrightarrow B$. Obviously $u|S_o = u_o$ and u is a homomorphism (since the fact that it is a homomorphism is expressed by the commutativity of a certain diagram and this diagram does indeed commute because on sufficiently small open sets it does). Knowing that u is a homomorphism, it induces a mapping $\bar{A} \longrightarrow \bar{B}$. But since $u|U_i = u_i$ and $\bar{u}_i = \bar{u}|U_i: \bar{A}|U_i \longrightarrow \bar{B}|U_i$ we see the homomorphism that u induces from $\bar{A} \longrightarrow \bar{B}$ is indeed $\bar{u}$.

3) essential surjectivity: Let A_o be an abelian scheme on S_o and A' a B.T. group on S with $(A')_o = \bar{A}_o$. For each U_i in our base choose an abelian scheme A_i on U_i and an isomorphism $\varphi_i: (A_{i_o}, \bar{A}_i) \xrightarrow{\sim} (A_o|U_i, A'|U_i)$. We want to construct an isomorphism between $A_j|U_i \cap U_j$ and $A_i|U_i \cap U_j$. For each $U_k \subseteq U_i \cap U_j$ in our base $(\varphi_i^{-1}|U_k) \circ (\varphi_j|U_k)$ is an isomorphism between $(A_{j_o}|U_k, \overline{A_j|U_k})$ and $(A_{i_o}|U_k, \overline{A_i|U_k})$. Thus it comes from a unique isomorphism $A_j|U_k \xrightarrow{\sim} A_i|U_k$. Because these isomorphisms are unique they patch together to give an isomorphism $\xi_{ij}: A_j|U_i \cap U_j \xrightarrow{\sim} A_i|U_i \cap U_j$. To show that $\xi_{ik} = \xi_{ij} \circ \xi_{jk}$ we simply observe that for any $U_\ell \subseteq U_i \cap U_j \cap U_k$ in our base, the restriction of the functor to U_ℓ transforms both sides into $(\varphi_i^{-1}|U_\ell) \circ (\varphi_k|U_\ell)$. Thus since the functor is by hypothesis faithful on U_ℓ, the cocycle condition is satisfied. Hence the A_i can be glued together to obtain an A. Since by

construction there are isomorphisms $(A|U_i)_o \xrightarrow{\sim} A_o|U_i$ which patch together, it is clear that $A \underset{S}{\times} S_o \xrightarrow{\sim} A_o$. Since A is obviously locally of finite type over S and the morphism $A \longrightarrow S$ is quasi-compact (as $A_o \longrightarrow S_o$ is), A is of finite type over S. Furthermore $A \longrightarrow S$ is separated since $A_o \longrightarrow S_o$ is and the morphism $A \longrightarrow S$ is universally closed since $A_o \longrightarrow S_o$ is. Thus A is proper over S. A is an S-group scheme because the transition morphisms used to define A respected the algebraic structure on the various A_i. Since A is obviously smooth with geometrically connected fibers, A is an abelian scheme. We have already observed that $A \underset{S}{\times} S_o \xrightarrow{\sim} A_o$. Also by construction there are local isomorphisms $\bar{A}|U_i \xrightarrow{\sim} A'|U_i$ which patch together. Thus it is clear that A is mapped by our functor into an object which is isomorphic to (A_o, A').

Lemma (2.3.2) Let $S_o \subseteq S_1 \subseteq \cdots \subseteq S_r = S$ be a sequence of (closed) subschemes of S corresponding to ideals $I \supseteq I_o \supseteq I_1 \supseteq \cdots \supseteq I_r = (0)$. Assume the theorem is true for each pair (S_i, S_{i+1}). Then the theorem is true.

Proof: We prove this by an obvious induction on r. For $r = 0$ it is trivial. Thus assume the theorem is true for the pairs (S_o, S_{r-1}) and (S_{r-1}, S_r). Again we show successively that the functor is faithful, full, and essentially surjective.

1) faithful: Let $u, v: A \longrightarrow B$ be such that $u_o = v_o$ and $\bar{u} = \bar{v}$. Since $\bar{u}|S_{r-1} = \bar{v}|S_{r-1}$, it follows that $u|S_{r-1} = v|S_{r-1}: A|S_{r-1} \longrightarrow B|S_{r-1}$ since

the theorem is true for (S_o, S_{r-1}). But since it is also true for (S_{r-1}, S_r) we must have $u = v$.

2) full: Let $u_o: A_o \longrightarrow B_o$, $\bar{u}: \bar{A} \longrightarrow \bar{B}$ where A and B are abelian schemes on S_r. Then there is a $v: A|S_{r-1} \longrightarrow B|S_{r-1}$ such that $v_o = u_o$ and $\bar{v} = \bar{u}|S_{r-1}$. Now we can apply the fullness to the pair $(v, \bar{u}: (A|S_{r-1}, \bar{A}) \longrightarrow (B|S_{r-1}, \bar{B})$ to conclude there is a $u: A \longrightarrow B$ inducing $\bar{u}: \bar{A} \longrightarrow \bar{B}$ and with $u|S_{r-1} = v$. But then $u|S_o = v|S_o = u_o$.

3) essentially surjective: Let A_o be an abelian scheme on S_o and A' a B.T. group on S_r such that $A'|S_o = \bar{A}_o$. Since the theorem is true for (S_o, S_{r-1}) there is an abelian scheme A_{r-1} with $A_{r-1}|S_o = A_o$, $\bar{A}_{r-1} = A'|S_{r-1}$. Applying the theorem to (S_{r-1}, S_r) there is an A with $\bar{A} = A'$ and $A|S_{r-1} = A_{r-1}$ and hence $A|S_o = A_{r-1}|S_o = A_o$.

(2.3.3) By (2.3.1) it suffices to prove the theorem when S is affine, say $S = \mathrm{Spec}\,(A)$. By [II 4.1] and (2.3.2) we can assume $S_o = \mathrm{Spec}\,(A_o)$ where $A_o = A/I$, $pI = I^2 = (0)$.

Lemma (2.3.4) Let A be a ring and I be an ideal in it satisfying $pI = I^2 = (0)$. Giving divided powers on I is equivalent to giving a p-linear mapping $\pi: I \longrightarrow I$ (I being viewed as an A/pA-module).

Proof: Given divided powers (γ_n) on I, certainly $\gamma_p = \pi$ is such a mapping. Conversely given π define divided powers on I explicitly by

$$\gamma_n(x) = \frac{x^{a_o} (\pi(x))^{a_1} \cdots (\pi^r(x))^{a_r}}{a_o! \quad \cdots \quad a_r!}$$

when the p-digit expansion of n is $n = a_o + a_1 p + \ldots + a_r p^r$. One checks directly that the (γ_n) defined in this

way satisfy the axioms (it being quite trivial as $I^2 = (0)$). Clearly the only non-zero divided powers are the γ_{pi} .

(2.3.5) It is obvious that divided powers defined on the ideal I by the procedure of (2.3.4) are nilpotent exactly when π is nilpotent. In particular by choosing $\pi = 0$ we obtain nilpotent divided powers on I. Thus we conclude our proof of (2.3) by proving:

Theorem (2.3.6) Let S be a scheme with p locally nilpotent on it, I an ideal with nilpotent divided powers, $S_o = \mathrm{Var}(I)$. The functor $A \longmapsto (A_o, \bar{A})$ is an equivalence of categories between the category of abelian schemes on S and the category of pairs consisting of an abelian scheme on S_o and a lifting of its B.T. group to S.

Proof: Again let us show successively that the functor is faithful, full, and essentially surjective.

1) faithful: Let $u, v: A \longrightarrow B$ be given. Assume $u_o = v_o : A_o \longrightarrow B_o$ and $\bar{u} = \bar{v}: \bar{A} \longrightarrow \bar{B}$. Then $\bar{u}$ and $\bar{v}$ induce the same mapping $(\underline{V}(A) \hookrightarrow D(\bar{A}_o)_S) \longrightarrow (\underline{V}(B) \hookrightarrow D(\bar{B}_o)_S)$, namely $D(\bar{u}_o)_S$. Thus u and v induce the same mapping $(\underline{V}(A) \hookrightarrow D(A_o)_S) \longrightarrow (\underline{V}(B) \hookrightarrow D(B_o)_S)$ by (2.1). Hence by the assertion of faithfulness in (1.10) $u = v$.

2) full: Let $u_o : A_o \longrightarrow B_o$ and $u' : \bar{A} \longrightarrow \bar{B}$ be given with $u'_o = \bar{u}_o$. The giving of u' lifting $\bar{u}_o$ gives us a map of admissible filtrations $(\underline{V}(A) \hookrightarrow D(\bar{A}_o)_S) \longrightarrow (\underline{V}(B) \hookrightarrow D(\bar{B}_o)_S)$ and hence by (2.1) a map of admissible filtrations $(\underline{V}(A) \hookrightarrow D(A_o)_S) \longrightarrow (V(B) \hookrightarrow D(B_o)_S)$. By the fullness assertion of (1.10) there is a $u: A \longrightarrow B$ reducing to u_o

and giving rise to the same map on the admissible filtrations. But then $\bar{u}$ and u' give the same map on filtrations and $(\bar{u})_o = (\bar{u}_o) = u'_o$. Thus the faithfulness assertion in (1.6) implies that $\bar{u} = u'$. Hence our functor is full.

3) essentially surjective: Let A_o be an abelian scheme on S_o, A' a B.T. group on S with $A'_o = \bar{A}_o$. The giving of A' is equivalent to giving an admissible filtration on $D(\bar{A}_o)_S = D(A_o)_S$ (by (2.1)). Thus by the essential surjectivity assertion of (1.10) there is an abelian scheme A on S reducing to A_o and giving the desired filtration on $D(A_o)_S$. But $\bar{A}$ and A' reduce to the same B.T. group and give rise to the same filtration on $D(\bar{A}_o)_S$. Hence by (1.6) we conclude that there is an isomorphism between $\bar{A}$ and A' such that $(A \underset{S}{\times} S_o, \bar{A})$ is isomorphic to (A_o, A'). Thus the functor is essentially surjective.

§3. (3.0) As an application of what has preceded we give here the Serre-Tate construction of the canonical lifting of an ordinary abelian variety over a perfect field k of characteristic p.

Definition (3.1) A g-dimensional abelian variety A_o over k is said to be ordinary if $A_o(1)$ has separable rank equal to p^g.

Lemma (3.2) Let k be a perfect field of characteristic p, W(k) its ring of Witt vectors. The functor $A' \longmapsto (A'_o, \bar{A}')$ is an equivalence of categories between the category of formal abelian schemes on W(k) and the catagory of pairs consisting of an abelian variety A_o on k and a

Barsotti-Tate group $\bar{A}$ on $W(k)$ lifting $\bar{A}_o$ (the B.T. group associated to A_o).

Proof: By [E.G.A. I 10.12.3, E.G.A. III 3.4.1] there is an equivalence of categories:

Formal abelian schemes/$W(k) \xrightarrow{\sim}$ Lim (Abelian schemes/$W_n(k)$).

By [II 4.16] there is an equivalence of categories:

B.T. $(W(k)) \xrightarrow{\sim}$ Lim B.T. $(W_n(k))$.

The equivalence is now an immediate consequence of (2.3: to the compatible family (A_n) of abelian schemes is associated $(A_o, (\bar{A}_n))$ which in turn is identified with a pair consisting of an abelian variety A_o and a B.T. group on $W(k)$.

Theorem (3.3) Let A_o be an ordinary abelian variety on k. There is a projective abelian scheme A on $W(k)$ lifting A_o such that the map

$$\underset{W(k)\text{-gr.}}{\text{End}}(A) \longrightarrow \underset{k\text{-gr.}}{\text{End}}(A_o)$$

is bijective. We call A, which is constructed explicitly below (up to canonical isomorphism), the canonical lifting of A_o.

Proof: Since k is perfect and A_o is ordinary, it follows from [22, page 147] that $\bar{A}_o$, the Barsotti-Tate group associated to A_o, is equal to a product $\bar{A}_o^{\text{ét}} \times \bar{A}_o^{\text{tor.}}$ of an étale and a toroidal B.T. group (both of height g). By [E.G.A. IV 18.3.2] there is a "unique" lifting of $\bar{A}_o^{\text{ét}}$ to each $W_n(k)$. Applying Cartier duality to $\bar{A}_o^{\text{tor.}}$, it is clear that this group can also be lifted uniquely to each $W_n(k)$. Let us call these liftings A_n' and A_n'' respectively. Then $A_n' \times A_n''$ lifts $\bar{A}_o$ (for any choice of n). By (3.2) there is associated to $(A_o, (A_n' \times A_n'')_{n\geq 0})$ a formal

abelian scheme A'. It is immediate from [II 3.3.21] and the above reference to E.G.A., that the map $\text{End}(A_n' \times A_n'') \longrightarrow \text{End}(\bar{A}_o)$ is bijective for all n. Thus the map $\text{End}(A') \longrightarrow \text{End}(A_o)$ is bijective.

It remains to show that A' can be algebraicized. First let us observe that by [26, XII 4.1(i)] $A'|W_n(k)$ is quasi-projective and hence projective [E.G.A. II 5.5.3(ii)]. Thus by [21, pp. 117-118] the dual abelian scheme $(A'|W_n(k))^*$ exists. Using either [23, 1.8] or [24, 19.2] we have $\overline{(A'|W_n(k))}^* \xrightarrow{\sim} \overline{(A'|W_n(k))^*}$.

Now choose an ample L_o on A_o, so as to obtain in the usual way a homomorphism $\lambda_o : A_o \longrightarrow (A_o)^*$ [21, pg. 120]. $\bar{\lambda}_o$ can be lifted to each $A_n' \times A_n''$ by simply looking at the unique lifting of $A_n' \longrightarrow A_n'^*$ (obvious notation) and similarly for the toroidal parts. By (2.3) this gives us for each n a mapping $\lambda_n : A'|W_n(k) \longrightarrow (A'|W_n(k))^*$ and it is obvious that $\lambda_{n+1}|W_n(k) = \lambda_n$. By [25, 2.3.2] this means there is a compatible system of invertible sheaves L_n on $(A'|W_n(k))$ such that λ_n is associated to L_n. By [E.G.A. III 5.4.5] A' comes from a projective scheme A over $W(k)$. [E.G.A. III 5.4.1] simultaneously implies that A is a group scheme and that the map $\text{End}(A) \longrightarrow \text{End}(A_o)$ is bijective (since we already know $\text{End}(A') \longrightarrow \text{End}(A_o)$ is bijective). By [E.G.A. IV 12.2.4 (viii)] A has geometrically integral fibers. Finally by [4, Chap. 3 §5, Theorem 1, Prop. 2] A is flat and hence since the generic fiber is smooth [G.A. II §6, 1.1] A is smooth [E.G.A. IV 17.5.1].

Corollary (3.4) Let A_o, B_o be ordinary abelian varieties over k and A, B their respective canonical liftings. The map $\mathrm{Hom}(A,B) \longrightarrow \mathrm{Hom}(A_o, B_o)$ is bijective.

Proof: Injectivity follows immediately from the rigidity lemma [21, 6.2]. If $f_o : A_o \longrightarrow B_o$ is a homomorphism, it induces $\bar{f}_o : \bar{A}_o \longrightarrow \bar{B}_o$ which can be lifted to $A'_n \times A''_n \longrightarrow B'_n \times B''_n$ (notation as above) by defining the lifting separately on the étale and toroidal parts. This gives a homomorphism between the formal abelian schemes $f' : A' \longrightarrow B'$ lifting f_o. By [E.G.A. III 5.4.1] f' comes from a homomorphism $f : A \longrightarrow B$.

APPENDIX

Our purpose here is to give some additional results on the canonical lifting of on ordinary abelian variety and to give consequences of the theorem of Serre-Tate in the case of ordinary elliptic curves. The first section gives a characterization of the canonical lifting. The second section is a technical interlude necessary for the applications to ordinary elliptic curves given in the third section.

Lemme (1.0). Let A_o be an ordinary abelian variety on a field k of characteristic p. Then, the Verschiebung, $V : A_o^{(p)} \longrightarrow A_o$ is étale.

Proof. It may be assumed that k is algebraically closed [EGA_{IV} 17.7.3 (ii)]. As A_o is ordinary there is a non-canonical isomorphism $A_o^{(p)}(1) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^g \times (\mu_p)^g$, where $g = \dim(A_o)$. Since V kills $\mathbb{Z}/p\mathbb{Z}$ and is the identity ou μ_p, the kernel of V is the étale part of $A_o^{(p)}(1)$. From the exactness of $0 \longrightarrow \mathrm{Ker}(V) \longrightarrow A_o^{(p)} \xrightarrow{V} A_o \longrightarrow 0$, it follows by descent [EGA 17.7.3 (ii)] that V is étale.

(1.1) Let k be a perfect field of characteristic p, $W(k)$ the ring of Witt vectors of k, A_o an ordinary abelian variety on k and A an abelian scheme on $W(k)$ which lifts A_o.

Proposition (1.2). A is a canonical lifting if (and only if) there is an integer i and a homomorphism $W : A^{(p^i)} \longrightarrow A$ (where $A^{(p^i)}$ is the inverse image of A under the i^{th} power of the canonical Frobenius on $W(k)$) which lifts the i^{th} iterate of Verschiebung, $V^i_{A_o}$.

Proof. Let us begin by showing W is étale. By [EGA 17.7.3 (ii)] it suffices to consider the case when k is algebraically closed. Fix a prime $\ell \neq p$ and let us temporarily denote by $A(\ell^u)$ (resp. $A_o(\ell^u)$) the kernel of multiplication by ℓ^u on A (resp. A_o). The sequence $0 \longrightarrow \mathrm{Ker}(V^i_{A_o}) \longrightarrow V^{-i}_{A_o}(A_o(\ell^u)) \longrightarrow A_o(\ell^u) \longrightarrow 0$ is exact because $V^i_{A_o}$ is an epimorphism. By (1.0) the sequence can be interpreted as an ordinary extension of a p-group by an ℓ-group, which necessarily splits. Then the map $V^i_{A_o} : A_o^{(p^i)}(\ell^u) \longrightarrow A_o(\ell^u)$ is an isomorphism. Hence the map $W : A_o^{(p^i)}(\ell^u) \longrightarrow A^{(p^i)}(\ell^u)$ is an isomorphism. In particular W induces an isomorphism between the ℓ-divisible groups of the generic fibres of $A^{(p^i)}$ and A. Since the points of A of order a power of ℓ with values in some algebraic closure of the fraction field of $W(k)$ are dense and since W is proper [EGA_{II} 5.4.3 (i)], it follows that on the generic fibers W is surjective. Thus by the lemma of generic flatness [21, 6.1.2] it follows that W induces a flat morphism on the generic fibers. Because the kernel of W is proper and has zero-dimensional fibres, it is finite [EGA_{IV} 8.11.1]. Thus the kernel is finite, and locally-free. From (1.0) and [EGA_{IV} 17.6.2 c'] it follows that Ker W is étale, which implies that W is étale.

We can of course repeat the above reasoning with W replaced by $W^{(p-i)} : A \longrightarrow A^{(p^{-i})}$, $W^{(p-2i)} \circ W^{(p^{-i})} : A \longrightarrow A^{(p-2i)}$, ... Thus each of the corresponding kernels is an étale subgroup of A. Call the n^{th} such subgroup $A<n>$. Then $p^{in} : A<n> \longrightarrow A<n>$ reduces to zero and hence as $A<n>$ is étale we have $A<n> \subseteq A(in)$. Let $\widetilde{A} = \varinjlim A<n>$. We wish to show it is a Barsotti-Tate group. Certainly it is of p-torsion. To show $\widetilde{A}$ is p-divisible, it suffices to show the map $p^i : A<n+1> \longrightarrow A<n>$ is an epimorphism (notice that this has a sense because $(V^i_{A_o})^{(p^{-in})} \circ \ldots \circ (V^i_{A_o})^{(p^{-i})} \circ p^i = 0$). Because $A<n+1>$ is étale, the

map $F^i_{A_o} : A_o<n+1> \longrightarrow A_o<n+1>^{(p^i)}$ can be lifted to a homomorphism F; and the lifting is in fact an isomorphism since it lifts one. Again using the fact that $A<n+1>$ is étale the map $A<n+1> \xrightarrow{F} A<n+1>^{(p^i)} \xrightarrow{W} A<n+1>$ which lifts p^i, is equal to p^i. Thus it suffices to show $W : A<n+1>^{(p^i)} \longrightarrow A<n>$ is an epimorphism. But this is immediate since $W : A^{(p^i)} \longrightarrow A$ is an epimorphism (because it is faithfully flat) and $W^{-1}(A<n>) \subseteq A<n+1>^{(p^i)}$.

From [I 1.1, 1.5] it follows that to show $\widetilde{A}$ is a Barsotti-Tate group is suffices to show $\widetilde{A}(i)$ is finite, locally-free. Let us show $\widetilde{A}(i) = A<1>$. Since $\widetilde{A}(i) = \varinjlim A<n>(i)$ it suffices to show the inclusion $A<1> \hookrightarrow A<n>(i)$ is an isomorphism for all n. Because $A<n>$ is étale, $p^i : A<n> \longrightarrow A<n>$ is étale and thus $A<n>(i)$ is étale and in particular finite, locally-free. The inclusion $A<1> \hookrightarrow A<n>(i)$ corresponds to a homomorphism of free (of finite rank) W-algebras which reduces to an isomorphism modulo p and hence is an isomorphism.

Consider now the inclusion $\widetilde{A} \hookrightarrow A(\infty)$. Over k, there is a map $A_o(\infty) \longrightarrow \widetilde{A}_o = A_o(\infty)^{\text{ét}}$ which when composed with the inclusion is the identity on $\widetilde{A}_o$ (since $A_o(\infty) = A_o(\infty)^{\text{t.m.}} \times A_o(\infty)^{\text{ét}}$). Because $\widetilde{A}$ is ind-étale this splitting can be lifted, which shows that A is a canonical lifting of A_o.

Corollary (1.2). *A is a canonical lifting if and only if there is a homomorphism $F : A \longrightarrow A^{(p)}$ lifting Frobenius.*

Proof. There is such an F if and only if there is a W lifting Verschiebung on A^*_o (because Cartier duality interchanges F and V), hence if and only if A^* is a canonical lifting. Since by Cartier duality $A^*(\infty) = (A(\infty))^*$, it

follows that $A(\infty)$ is a product of an étale and a toroidal part and hence that A is a canonical lifting.

Corollary (1.3). If k is finite, A is a canonical lifting if and only if $\mathrm{End}(A,A) \longrightarrow \mathrm{End}(A_o,A_o)$ is bijective.

Proof. If k has p^i elements, then the i^{th} iterate of Verschiebung is an endomorphism of A_o.

(2.0). Let S_o be a sheme with p locally nilpotent on it and $S_o \hookrightarrow S$ an immersion defined by a locally nilpotent ideal. Let G'_o be a toroidal B.T. group on S_o, G''_o an ind-étale B.T. group on S_o and fix liftings G' and G" to B.T. groups on S'. We wish to consider liftings of $G'_o \times G''_o$ to Barsotti-Tate groups on S_o.

Proposition (2.1). There is an equivalence of categories between the category of extensions of G" by G' provided with a trivialization of the induced extension of G''_o by G'_o and the category of lifting of $G'_o \times G''_o$.

Proof. Let G be a lifting. Because G" is ind-étale there is a unique homomorphism $G \longrightarrow G''$ reducing to the projection $G'_o \times G''_o \longrightarrow G''_o$. By the criterion for checking flatness fiber by fiber [EGA_{IV} 11.3.11], this map is an epimorphism. Let K denote its kernel so that we have an exact sequence

$$0 \longrightarrow K \longrightarrow G \longrightarrow G'' \longrightarrow 0 \quad .$$

Obviously K is of p-torsion. Because the maps $G(n) \longrightarrow G''(n)$ are actually epimorphisms (since they lift epimorphisms), K is p-divisible. K(1) is flat,

finite [EGA_{II} 6.1.5 (iii)] and of finite presentation [EGA_{IV} 1.6.2 (v)] over S, and thus it is finite locally-free [EGA_{IV} 1.4.7]. Th s shows that K is a B.T. group. The given isomorphism $K \underset{S}{\times} S_o \xrightarrow{\sim} G'_o$ is uniquely liftable to an isomorphism $K \xrightarrow{\sim} G'$ as is seen by using Cartier duality and the fact that G'_o is toroidal. Via this isomorphism we make G an extension of G" by G'.

This construction defines a functor from the category of liftings to the category of trivialized extensions. It is obviously an equivalence of categories which is quasi-inverse to the functor "forget the structure of extension".

Remark (2.2). An easy passage to the limit gives the corresponding assertion when R is an adic ring whose topology is defined by an ideal I such that I/I^2 is of finite type over R/I [cf. II 4.15, 4.16]. We note the following consequence.

Corollary (2.3). Let R be a complete noetherian local ring with perfect residue field k of characterictic p. Let G'_o (resp. G''_o) be a toroidal (resp. ind-étale) B.T. group on k and G' (resp. G") a lifting to R. Then the set of isomorphism classes of lifting of $G'_o \times G''_o$ is in bijective correspondence with $\mathrm{Ext}^1(G'',G')$.

Proof. This follows immediately from the proposition and the fact that since k is perfect, there is exactly one way to trivialize an extension of G''_o by G'_o.

(2.4) The calculation of $\mathrm{Ext}^1(\mathbb{Q}_p/\mathbb{Z}_p, \mu)$ made below in (2.5) will be utilized in section 3 to give the results on ordinary elliptic curves alluded to above.

(2.4.1) Let R be an artin local ring with perfect residue field, k, of characteristic p and maximal ideal $\underline{m}$. Consider the inductive system of sheaves on R : $\mathbb{Z} \xrightarrow{p} \mathbb{Z} \xrightarrow{p} \mathbb{Z} \longrightarrow \ldots$ which is indexed by the natural numbers, $\mathbb{N}$. Writing $\mathbb{Q}_p/\mathbb{Z}_p = \varinjlim_{n \geq 0} \mathbb{Z}/p^n\mathbb{Z}$ we see that there is an exact sequence of sheaves on R :

(2.4.2) $$0 \longrightarrow \mathbb{Z} \longrightarrow \varinjlim \mathbb{Z} \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0 \quad .$$

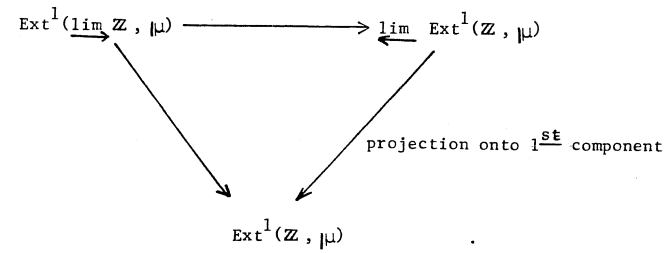
Looking at the relevant portion of the long exact sequence arising from applying the functor $\mathrm{Hom}(-, \mu)$ we obtain the sequence :

(2.4.3) $$\varprojlim \mathrm{Hom}(\mathbb{Z}, \mu) \longrightarrow \mathrm{Hom}(\mathbb{Z}, \mu) \xrightarrow{\delta_R} \mathrm{Ext}^1(\mathbb{Q}_p/\mathbb{Z}_p, \mu) \longrightarrow \mathrm{Ext}^1(\varinjlim \mathbb{Z}, \mu)$$

Proposition (2.5). As R varies over artin local rings with residue field k, the homomorphism δ_R of (2.4.3) defines a functorial isomorphism : $1 + \underline{m} = \mu(R) \xrightarrow{\sim} \mathrm{Ext}^1_R(\mathbb{Q}_p/\mathbb{Z}_p)_Q, \mu)$; the subscript "R" denoting Ext of sheaves on Spec(R).

Proof. $\mathrm{Hom}(\mathbb{Z}, \mu) = \mu(R) = 1+\underline{m}$ and because for n sufficiently large $(1+\underline{m})^{p^n} = \{1\}$, it follows that the inverse limit, $\varprojlim \mathrm{Hom}(\mathbb{Z}, \mu)$, is zero. Thus δ_R is injective. To show it is surjective it suffices to show the next mapping in (2.4.3) is zero or equivalently that the map $\mathrm{Ext}^1(\varinjlim \mathbb{Z}, \mu) \longrightarrow \mathrm{Ext}^1(\mathbb{Z}, \mu)$ is injective. This map factors as shown in the diagram :

(2.5.1)



We shall show that each of the maps occuring in the factorization is injective.

Lemma (2.5.2). The map $\mathrm{Ext}^1(\varinjlim \mathbb{Z}, \mu) \longrightarrow \varprojlim \mathrm{Ext}^1(\mathbb{Z}, \mu)$ is injective.

Proof. Let C' be the category of abelian sheaves on Spec(R), C the category of projective systems of abelian groups indexed by $\mathbb{N}$ (i.e. the category of abelian presheaves on $\mathbb{N}$, which thus has enough injectives), C'' the category of abelian groups. The functor $F \longmapsto \mathrm{Hom}(\varinjlim \mathbb{Z}, F)$ from C' to C'' can be factored as follows : $C' \xrightarrow{F \longmapsto (\mathrm{Hom}(\mathbb{Z}, F))_{i \in \mathbb{N}}} C \xrightarrow{\Gamma} C''$. We want to write down the associated spectral sequence of a composite functor : $E_2^{p,q} = R^p\Gamma((\mathrm{Ext}^q(\mathbb{Z}, \mu))_{i \in \mathbb{N}}) \Longrightarrow \mathrm{Ext}(\varinjlim \mathbb{Z}, \mu)$. This will be permissible once it is shown :

(2.5.2.1) For I an injective object in C', the projective system $(\mathrm{Hom}(\mathbb{Z}, I))_{i \in \mathbb{N}}$ is Γ-acyclic.

But quite generally if $0 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 0$ is an exact sequence in C with the transition morphisms of G' surjective, then $0 \longrightarrow \Gamma(G') \longrightarrow \Gamma(G) \longrightarrow \Gamma(G'') \longrightarrow 0$ is exact. On the other hand given an

exact sequence $0 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 0$, then G having surjective transition morphisms implies G'' does also. Since injective objects in G have surjective transition morphisms the last two remarks imply : if G' in C has surjective transition morphisms, then G' is Γ-acyclic. Thus the definition of an injective object together with the fact that $\mathbb{Z} \xrightarrow{p} \mathbb{Z}$ is a monomorphism implies (2.5.2.1) and allows us to form the spectral sequence. The corresponding sequence of terms of low degree is

(2.5.2.2) $\quad 0 \longrightarrow R^1\Gamma((1+\underline{m})_{i\in\mathbb{N}}) \longrightarrow \mathrm{Ext}^1(\varinjlim \mathbb{Z}, \mu) \longrightarrow \varprojlim \mathrm{Ext}^1(\mathbb{Z}, \mu)$.

Since for n sufficiently large, $(1+\underline{m})^{p^n} = \{1\}$, the inverse system $(1+\underline{m})_{i\in\mathbb{N}}$ satisfies the Mittag-Leffler condition. Hence by [EGA_0 13.2.2] $R^1\Gamma((1+\underline{m})_{i\in\mathbb{N}}) = (0)$ and by (2.5.2.2) we conclude.

(2.5.3). The injectivity of the map $\varprojlim \mathrm{Ext}^1(\mathbb{Z}, \mu) \longrightarrow \mathrm{Ext}^1(\mathbb{Z}, \mu)$ follows from the more precise:

Lemma (2.5.4). $H^1(\mathrm{Spec}(R), \mu) = (0)$.

Proof: By an obvious modification of [SGA_4 VII 3.1] if follows from [SGA_4 VI 6 1.2 (3)] that $H^1(\mathrm{Spec}(R), \mu) = \varinjlim H^1(\mathrm{Spec}(R), \mu(n))$ and hence is of p-torsion. Thus to prove the lemma it suffices to know $H^1(\mathrm{Spec}(R), \mu)$ has no p-torsion. To see this choose n sufficiently large so that $(1+\underline{m})^{p^n} = \{1\}$. Consider the morphism of exact sequences :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mu(n) & \longrightarrow & \mu & \xrightarrow{p^n} & \mu & \longrightarrow & 0 \\
 & & \| & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mu(n) & \longrightarrow & \mathbb{G}_m & \xrightarrow{p^n} & \mathbb{G}_m & \longrightarrow & 0
\end{array} .$$

Because k is perfect the map $1+\underline{m}/(1+\underline{m})^{p^n} = 1+\underline{m} \longrightarrow R^*/(R^*)^{p^n}$ is bijective. Thus writing the relevant position of the cohomology sequences we find:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & 1+\underline{m} & \longrightarrow & H^1(\mathrm{Spec}(R), \mu(n)) & \longrightarrow & {}_{p^n}H^1(\mathrm{Spec}(R), \mu) & \longrightarrow & 0 \\
 & & \wr\downarrow & & \| & & \downarrow & & \\
0 & \longrightarrow & R^*/(R^*)^{p^n} & \longrightarrow & H^1(\mathrm{Spec}\ R, \mu(n) & \longrightarrow & {}_{p^n}H^1(\mathrm{Spec}\ R, \mathbb{G}_m) & \longrightarrow & 0
\end{array} .$$

This shows the p^n-torsion in $H^1(\mathrm{Spec}(R), \mu)$ is isomorphic to that in $H^1(\mathrm{Spec}(R), \mathbb{G}_m)$. Since R is a local ring it follows from [G.A III § 4,6.10] that $H^1(\mathrm{Spec}(R), \mathbb{G}_m) = (0)$.

(2.5.5). Let us now explicate the mapping which is the inverse of δ_R . Thus let the extension (ϵ) $\quad 0 \longrightarrow \mu \longrightarrow E \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0$ arise from pushing out the extension (2.5.1) along a homomorphism $\phi : \mathbb{Z} \longrightarrow \mu$ so that we have a commutative diagram :

(2.5.6)
$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \varinjlim \mathbb{Z} & \longrightarrow & \mathbb{Q}_p/\mathbb{Z}_p & \longrightarrow & 0 \\ & & \downarrow \phi & & \downarrow & & \| & & \\ 0 & \longrightarrow & \mu & \longrightarrow & E & \longrightarrow & \mathbb{Q}_p/\mathbb{Z}_p & \longrightarrow & 0 \end{array} .$$

Restricting (ϵ) to $\mathbb{Z}/p^n\mathbb{Z}$ is the same as pushing out
$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0$ along ϕ .
We have the exact sequence,

(2.6) $$\mathrm{Hom}(\mathbb{Z}, \mu) \xrightarrow{p^n} \mathrm{Hom}(\mathbb{Z}, \mu) \xrightarrow{\delta_R} \mathrm{Ext}^1(\mathbb{Z}/p^n, \mu) \longrightarrow \mathrm{Ext}^1(\mathbb{Z}, \mu) .$$

By (2.5.4) this gives us the isomorphism : $\mathrm{Hom}(\mathbb{Z}, \mu)\Big/p^n\mathrm{Hom}(\mathbb{Z}, \mu) \xrightarrow{\sim} \mathrm{Ext}^1(\mathbb{Z}/p^n\mathbb{Z}, \mu)$

The inverse is furnished is follows : lift the section $1 \in \Gamma(\mathrm{Spec}(R)), \mathbb{Z}/p^n\mathbb{Z})$ to an arbitrary section in $E \times_{\mathbb{Q}_p/\mathbb{Z}_p} \mathbb{Z}/p^n\mathbb{Z}$, multiply it by p^n to obtain a section of μ which is unique up to p^n th powers.

Passing to the inverse limit we obtain a map

$$\mathrm{Ext}^1(\mathbb{Q}_p/\mathbb{Z}_p, \mu) \longrightarrow \varprojlim \mathrm{Ext}^1(\mathbb{Z}/p^n\mathbb{Z}, \mu) \xrightarrow{\sim} 1+\underline{m}$$

which is the inverse of the map δ_R of proposition (2.5). Incidentally this shows the map $\mathrm{Ext}^1(\mathbb{Q}_p/\mathbb{Z}_p, \mu) \longrightarrow \varprojlim \mathrm{Ext}^1(\mathbb{Z}/p^n\mathbb{Z}, \mu)$ is an isomorphism.

(2.7) If R is a complete noetherian local ring (whose maximal ideal is denoted by $\underline{m}$) with perfect residue class field of characteristic p, then passing to the limit as n increases and utilizing [II 4.15, 4.16] we find from (2.5) :

$$1+\underline{m} = \varprojlim(1+\underline{m}/\underline{m}^n) \xrightarrow{\sim} \varprojlim \mathrm{Ext}_{R/\underline{m}^n}(\mathbb{Q}_p/\mathbb{Z}_p, \mu) = \mathrm{Ext}_R(\mathbb{Q}_p/\mathbb{Z}_p, \mu) .$$

(3.0) In order to apply the above results to giving a "down-to-earth" spelling out of the theorem of Serre-Tate in the case of elliptic curves, let us fix an algebraically closed field, k, of characteristic p, and an ordinary elliptic curve E_o over k. Let us choose an isomorphism $r_o : \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\sim} E_o(\infty)^{\text{ét}}$. Because E_o is canonically isomorphic to its dual, the choice of r_o furnishes us an isomorphism between μ and the toroidal part of $E_o(\infty)$. The product of these two isomorphisms gives us an isomorphism $\mathbb{Q}_p/\mathbb{Z}_p \times \mu \longrightarrow E_o(\infty)$. If E_1 is another ordinary elliptic curve let us choose an isomorphism $r_1 : \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow E_1(\infty)^{\text{ét}}$. A homomorphism $\rho_o : E_o \longrightarrow E_1$ induces a homomorphism $E_o(\infty) \longrightarrow E_1(\infty)$ and thus via the identifications made using r_o and r_1 a homomorphism $\mathbb{Q}_p/\mathbb{Z}_p \times \mu \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \times \mu$. Because $\mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, \mu) = \mathrm{Hom}(\mu, \mathbb{Q}_p/\mathbb{Z}_p) = 0$ and $\mathrm{End}(\mathbb{Q}_p/\mathbb{Z}_p) = \mathrm{End}(\mu) = \mathbb{Z}_p$, ρ_o furnishes us with a pair (z_o, z_1) of p-adic integers such that ρ_o induces multiplication by z_o on $\mathbb{Q}_p/\mathbb{Z}_p$ and multiplication by z_1 on μ.

(3.1) Let R be a complete noetherian local ring of residue field k and E a lifting of E_o to R. Then $E(\infty)$ is a lifting of $E_o(\infty)$ and hence determines an extension (once we've chosen r_o as above)

$$0 \longrightarrow \mu \longrightarrow E(\infty) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0$$

by (2.3). This extension determines via (2.5),(2.6),(2.7) an element in $1+\underline{m}$, which we denote by $q(E, r_o)$.

Proposition (3.2.) *Given an ordinary elliptic cure E_o over k, fix $r_o : \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\sim} E_o(\infty)^{\text{ét}}$. Then, the map $E \longmapsto q(E, r_o)$ establishes a bijective correspondence between the set of isomorphism classes of lifting of E_o and the elements in $1 + \underline{m}$.*

Proof. The map $E \longmapsto E(\infty)$ is a bijection between formal liftings of E_o and liftings of $E_o(\infty)$ by the theorem of Serre-Tate [V 2.3, II 4.15]. Hence the proposition follows immediately from (2.3), (2.5), (2.6), (2.7) and the fact that formal liftings of curves are automatically uniquely algebraisable [EGA_{III} 5.4.1, 5.4.5, SGA_1 III 7.1].

Proposition (3.3). Let (E_o,r_o), (E_1,r_1) be two ordinary elliptic curves provided with isomorphisms $r_i : \mathbb{Q}/\mathbb{Z}_p \xrightarrow{\sim} E_i(\infty)^{ét}$. Let $\rho_o : E_o \longrightarrow E_1$ be a homomorphism (thus determining (z_o,z_1) as in (3.0)). Let E (resp. E') correspond via proposition (3.2) to elements q (resp. q') in $1+\underline{m}$. Then ρ_o can be lifted to a homomorphism $\rho : E \longrightarrow E'$ if and only if $q^{z_1} = q'^{z_o}$, and in this case the lifting is unique.

Proof. To lift ρ_o is equivalent to lifting $\rho_o(\infty) : E_o(\infty) \longrightarrow E_1(\infty)$ to a homomorphism $\rho(\infty)\ E(\infty) \longrightarrow E'(\infty)$ [V 2.3, II 4.15]. Assume that such a lifting $\rho(\infty)$ exists. $E(\infty)$ and $E'(\infty)$ are both extensions of $\mathbb{Q}_p/\mathbb{Z}_p$ by μ. Consider the diagram :

(3.3.1)
$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mu & \longrightarrow & E(\infty) & \longrightarrow & \mathbb{Q}_p/\mathbb{Z}_p & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle z_1} & & \downarrow{\scriptstyle \rho(\infty)} & & \downarrow{\scriptstyle z_o} & & \\ 0 & \longrightarrow & \mu & \longrightarrow & E'(\infty) & \longrightarrow & \mathbb{Q}_p/\mathbb{Z}_p & \longrightarrow & 0 \end{array} .$$

By definition of z_1, $\rho(\infty)$, z_o (3.3.1) commutes when restricted to k. Using [II 4.15, 4.16] together with an obvious modification of [II 3.3.2.1] obtained by employing [II 3.3.17], it follows that (3.3.1) commutes. This says that the upper row when "pushed out" via $z_1 : \mu \longrightarrow \mu$ is isomorphic to the lower row when "pulled back" via $z_1 : \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$. Because of the isomorphism $1+\underline{m} \xrightarrow{\sim} \mathrm{Ext}^1(\mathbb{Q}_p/\mathbb{Z}_p,\mu)$ "pushing out" corresponds to raising q to the power z_1. From this isomorphism and the bi-functoriality

of Ext, it follows that "pulling back" corresponds to raising q' to the power z_o. Thus the existence of a lifting implies $q'^{z_o} = q^{z_1}$. Conversely if this equality holds the push out of one extension is isomorphic to the pull back of the other and hence there exists a map $\rho(\infty) : E(\infty) \longrightarrow E'(\infty)$ rendering (3.3.1) commutative. Reducing this diagram we obtain a commutative diagram over k. Because there are no homomorphism from $\mathbb{Q}_p/\mathbb{Z}_p$ to μ this tells us that the reduction of $\rho(\infty)$ is $\rho_o(\infty)$. The uniqueness of the homomorphism follows immediately from [EGA_{III} 5.4.1] and [V 2.3, II 4.15, 4.16].