Chapter IV. The Crystals Associated to Barsotti-Tate Groups

§1. (1.0) In this chapter we shall associate to Barsotti-Tate groups G on a scheme S (where p is locally nilpotent) certain crystals. For applications in the next chapter it is necessary to know that via (essentially) the same method, crystals can also be associated to abelian schemes on S. The constructions in the case of an abelian scheme go through by repeating word for word the reasoning in the case of a Barsotti-Tate group. For this reason only the case of a Barsotti-Tate group is explicitly discussed, but from time to time certain minor differences in the two situations are explicitly noted.

(1.1) This paragraph is devoted to showing that when p is locally nilpotent on the base scheme S, a Barsotti-Tate group G admits a universal extension by a vector group. The first proposition below makes no hypothesis on the base, but afterwards it shall always be assumed that p is locally nilpotent on S.

(1.2) Let S be a scheme and G a finite locally-free S-group. Recall that associated to a quasi-coherent $\mathcal{O}_S$-module M is a group W(M) (in the notation of [S.G.A. 3.I 4.6]) whose sections over an S-scheme T are given by

$$\Gamma(T, W(M)) = \Gamma(T, \mathcal{O}_T \otimes_{\mathcal{O}_S} M).$$

Because no confusion will result, the W(M) notation is below shortened to M.

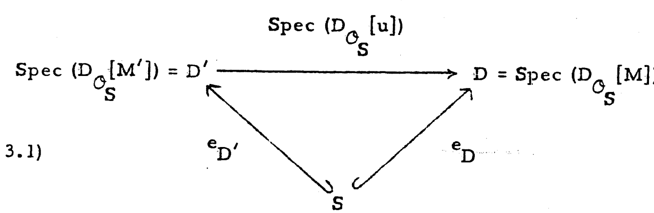
Proposition (1.3) The functor (on quasi-coherent modules) $M \longmapsto \mathrm{Hom}_{S\text{-gr.}}(G, M)$ is represented by $\underline{\omega}_{G^*}$, G^* being the Cartier dual of G.

Proof: Fix a module M and let $D_{\mathcal{O}_S}[M] = \mathcal{O}_S \oplus M$, viewed as an algebra via $M^2 = (0)$ and $D = \mathrm{Spec}(D_{\mathcal{O}_S}[M])$. The S scheme D coincides with S as topological space and has an obvious section $e_D: S \hookrightarrow D$ corresponding to the augmentation $D_{\mathcal{O}_S}[M] \longrightarrow \mathcal{O}_S$. Hence D-groups can be pulled back to S along this section and it makes sense to speak of

$$\mathrm{Ker}\,[\mathrm{Hom}_{D\text{-gr.}}(G_D, \mathbb{G}_{m_D}) \longrightarrow \mathrm{Hom}_{S\text{-gr.}}(G, \mathbb{G}_{m_S})].$$

Because G is fixed, this kernel depends only on M (as D depends only on M) and hence can be written as $\mathcal{A}(M)$. Note that $M \longmapsto \mathcal{A}(M)$ is a covariant functor, for given a linear $u: M \longrightarrow M'$ there is a commutative diagram:

(1.3.1)



Assume momentarily that there is a functorial isomorphism: $\mathrm{Hom}_{S\text{-gr.}}(G, M) \xrightarrow{\sim} \mathcal{A}(M)$. Let us show how the proposition follows. By definition (or by [S.G.A. 3 VII A 3.3]) $\mathcal{A}(M) = \mathrm{Ker}[G^*(D) \longrightarrow G^*(S)]$. But by [S.G.A. 3 III 0.9] this group is given by $\mathrm{Hom}(\underline{\omega}_{G^*}, M)$. It is clear from the explicit construction of the isomorphism between the two groups [E.G.A. IV 16.5.14] that it is functorial in M and thus the functor is indeed represented by $\underline{\omega}_{G^*}$.

Thus we must establish the isomorphism

(1.3.2) $\quad \mathrm{Hom}\,(G, M) \xrightarrow{\sim} \mathfrak{A}\,(M).$

M being fixed, let $\pi_T: T \longrightarrow D$ be a D-scheme. There is to be associated to a $\varphi: G \longrightarrow M$ a $\varphi': G_D \longrightarrow \mathbb{G}_{m_D}$. Such a φ' is given by a family $\varphi'(T): G_D(T) \longrightarrow \mathbb{G}_{m_D}(T)$. But $G_D(T) = G(T)$ when T is viewed as an S-scheme via $T \xrightarrow{\pi_T} D \longrightarrow S$. Thus $\varphi'(T): G(T) \longrightarrow \Gamma(T, \mathcal{O}_T^*)$. To define $\varphi'(T)$ proceed as follows: Corresponding to the fact that T is a D-scheme there is a ring homomorphism $\rho_T: \pi_T^{-1}(\mathcal{O}_S \oplus M) = \pi_T^{-1}(\mathcal{O}_S) \oplus \pi_T^{-1}(M) \longrightarrow \mathcal{O}_T$. Under this homomorphism the image of $\pi_T^{-1}(M)$ has square zero. On the other hand associated to φ there is a $\varphi(T): G(T) \longrightarrow \Gamma(T, \mathcal{O}_T \otimes_{\pi_T^{-1}(\mathcal{O}_S)} \pi_T^{-1}(M))$. Hence for $x \in G(T)$, $1 + \rho_T \circ \varphi(T)(x)$ has an obvious meaning. It is a unit and the map $x \longmapsto 1 + \rho_T \circ \varphi(T)(x)$ is a group homomorphism $G(T) \to \Gamma(T, \mathcal{O}_T^*)$. By definition this is $\varphi'(T)$. It is now obvious because φ is a homomorphism of functors, that for variable T, the family $\varphi'(T)$ defines a morphism $G_D \longrightarrow \mathbb{G}_{m_D}$. Furthermore, it is clear since $(\varphi_1 + \varphi_2)'(T) = \varphi_1'(T) + \varphi_2'(T)$ that $\varphi \longmapsto \varphi'$ is a homomorphism. Since the restriction morphism $\mathrm{Hom}\,(G_D, \mathbb{G}_{m_D}) \longrightarrow \mathrm{Hom}_S(G, \mathbb{G}_{m_D})$ is "obtained" by viewing a given S-scheme T as a D-scheme via $T \longrightarrow S \xrightarrow{e_D} D$ it is immediate

that the map $\rho_T: \pi_T^{-1}(\mathcal{O}_S) \oplus \pi_T^{-1}(M) \longrightarrow \mathcal{O}_T$ must map $\pi_T^{-1}(M)$ to zero and hence φ' actually belongs to $\mathfrak{A}\,(M) = \mathrm{Ker}[\mathrm{Hom}_{D\text{-gr.}}(G_D, \mathbb{G}_{m_D}) \longrightarrow \mathrm{Hom}_{S\text{-gr.}}(G, \mathbb{G}_m)]$.

If $u: M \longrightarrow M'$, then there is the map $D' \longrightarrow D$ corresponding to $D_{\mathcal{O}_S}[M] \longrightarrow D_{\mathcal{O}_S}[M']$. Let $\varphi: G \longrightarrow M$ and T' be a D'-scheme via $\pi'_{T'}$. Denote by $\varphi': G_D \longrightarrow \mathbb{G}_{m_D}$ the map associated to φ above. It must be shown that $\varphi' \mid D': G_{D'} \longrightarrow \mathbb{G}_{m_{D'}}$ is the same as $(u \circ \varphi)'$ (i.e., the map associated to $G \xrightarrow{\varphi} M \xrightarrow{u} M'$). But $(\varphi' \mid D')(T') \overset{\text{def}}{=\!=} \varphi'(T' \xrightarrow{\pi'_{T'}} D' \longrightarrow D) =$ the map $x \longmapsto 1 + \rho_{T'} \circ \varphi(T')(x)$ where $\rho_{T'}: \pi_{T'}^{-1}(\mathcal{O}_S) \oplus \pi_{T'}^{-1}(M) \longrightarrow \mathcal{O}_{T'}$. But obviously this is the composite

$$\pi_{T'}^{-1}(\mathcal{O}_S) \oplus \pi_{T'}^{-1}(M) \longrightarrow \pi'_{T'}(\mathcal{O}_S) \oplus \pi'^{-1}_{T'}(M') \longrightarrow \mathcal{O}_{T'}$$

(since $\pi_{T'} = \pi'_{T'}$, D and D' having the same underlying topological space). From this it is clear that the map $\mathrm{Hom}_{S\text{-gr.}}(G, M) \longrightarrow \mathfrak{A}\,(M)$ is functorial.

It remains to show that this map is bijective. Let us first observe that the map is compatible with any base change $S' \longrightarrow S$. To see this take T' to be a $D' = D \times_S S' = \mathrm{Spec}\,[\mathcal{O}_{S'} \oplus (M \otimes_{\mathcal{O}_S} \mathcal{O}_{S'})]$ scheme and note that for $x \in G(T')$ and $\varphi: G \longrightarrow M$, $(\varphi \mid S')'(x) = 1 + \rho_{T'} \circ (\varphi \mid S')(T')(x) = 1 + \rho_{T'} \circ \varphi(T')(x) = (\varphi' \mid D')(x)$.

Thus to prove the injectivity it suffices to show $\varphi'(D) = 0$ implies

$\varphi(S) = 0$. But $\varphi'(D) = 0$ says that for $x \in G(D)$ $1 + \rho_D \circ \varphi(D)(x) = 1$, i.e., $\rho_D \circ \varphi(D)(x) = 0$. Here $\varphi(D): G(D) \longrightarrow \Gamma(D, D_{\mathcal{O}_S}[M] \otimes_{\mathcal{O}_S} M)$ and ρ_D is the identity map $D_{\mathcal{O}_S}[M] \xrightarrow{\text{id.}} D_{\mathcal{O}_S}[M]$. Now over an affine open set U of S, $\varphi(D)(x)$ will be given by $\sum (a_i \oplus m_i) \otimes m_i'$ and hence the hypothesis that $\varphi'(D) = 0$ says that $\sum a_i m_i' = 0$. Notice that over this affine open U $\varphi(S)(e_D^*(x)) = \sum a_i m_i' = 0$. This means $\varphi(S)$ must vanish on the image of $G(D)$ in $G(S)$. But from the fact that e_D is a section of the structural map $D \longrightarrow S$ it follows that $G(D) \longrightarrow G(S)$ is onto. Thus the map $\mathrm{Hom}(G, M) \longrightarrow \mathfrak{A}(M)$ is injective.

To show surjectivity let $\tilde{\varphi} \in \mathfrak{A}(M)$ be given. For any S' over S $\tilde{\varphi}$ defines a homomorphism $\tilde{\varphi}(D_{S'}): G(D_{S'}) \longrightarrow \mathbb{G}_m(D_{S'})$. Consider the inclusion $G(S') \hookrightarrow G(D_{S'})$. For $x \in G(S')$, $\tilde{\varphi}(D_{S'})(x)$ is "killed" under the augmentation $D_{\mathcal{O}_{S'}}[\mathcal{O}_{S'} \otimes_{\mathcal{O}_S} M] \longrightarrow \mathcal{O}_{S'}$. Hence $\tilde{\varphi}(D_{S'})(x)$ is of the form $1 + y$ where $y \in \Gamma(S', \mathcal{O}_{S'} \otimes_{\mathcal{O}_S} M)$. If $\varphi: G \longrightarrow M$ is defined via $\varphi(S')(x) = y$ (in the above notation), it is clear that since $\tilde{\varphi}$ is a homomorphism of functors φ is also. To show the φ' associated to φ under the map $\mathrm{Hom}(G, M) \longrightarrow \mathfrak{A}(M)$ is the same as $\tilde{\varphi}$, let $T \xrightarrow{\pi_T} D$ be a D-scheme and let $x \in G(T)$. $\varphi'(T)(x) = 1 + \rho_T \circ \varphi(T)(x)$. Here $\varphi(T)(x)$ = image of x under $G(T) \hookrightarrow G(D_T) \xrightarrow{\tilde{\varphi}(D_T)} \mathbb{G}_M(D_T)$ minus $1 = \tilde{\varphi}(T)(x) - 1$ because there is a commutative diagram

$$\begin{array}{ccc} G(D_T) & \xrightarrow{\tilde{\varphi}(D_T)} & \mathbb{G}_m(D_T) \\ \uparrow & & \uparrow \\ G(T) & \xrightarrow{\tilde{\varphi}(T)} & \mathbb{G}_m(T) \end{array}$$

But in this case it is immediate that $\rho_T(\varphi(T))(x) = \varphi(T)(x)$. Hence $\varphi'(T)(x) = 1 + \varphi(T)(x) = 1 + \tilde{\varphi}(T)(x) - 1 = \tilde{\varphi}(T)(x)$.

Remark (1.4) By the proposition there is defined a homomorphism $\alpha: G \longrightarrow \underline{\omega}_{G^*}$ with the property that given $\beta: G \longrightarrow M$, there is a unique linear $u: \underline{\omega}_{G^*} \longrightarrow M$ such that $\beta = u \circ \alpha$.

Remark (1.5) If $\underline{\omega}_{G^*}$ is locally-free it is easy to make α "explicit": Let $G = \mathrm{Spec}(B)$, $G^* = \mathrm{Spec}(B^\vee)$, $I \subseteq B^\vee$, the augmentation ideal corresponding to the unit section of G^*, $\eta: B^\vee \longrightarrow \mathcal{O}_S$ the augmentation. Define $\varphi: B^\vee \longrightarrow D_{\mathcal{O}_S}[I/I^2]$ via $\varphi(b) = \eta(b) +$ residue class of $(b - \eta(b))$ in I/I^2. Since $\alpha: G \longrightarrow \underline{\omega}_{G^*}$, it corresponds to an algebra homomorphism $\mathrm{Sym}[\check{\underline{\omega}}_{G^*}] \longrightarrow B$, that is to a linear map $\check{\underline{\omega}}_{G^*} \longrightarrow B$ or by transposition a linear map $B^\vee \longrightarrow \underline{\omega}_{G^*}$. This last linear map is given by $b \longmapsto \varphi(b) - \eta(b)$.

Remark (1.6) It is easy to check that the above constructed isomorphism $\mathrm{Hom}_{S\text{-gr.}}(G, M) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}_S}(\underline{\omega}_{G^*}, M)$ is functorial in G. Thus for $u: G \longrightarrow H$, a homomorphism of finite locally-free groups, the diagram:

$$\begin{array}{ccc} G & \xrightarrow{u} & H \\ {\scriptstyle \alpha_G}\downarrow & & \downarrow{\scriptstyle \alpha_H} \\ \underline{\omega}_{G^*} & \longrightarrow & \underline{\omega}_{H^*} \end{array}$$

commutes. (The lower horizontal arrow is induced by the Cartier dual of u).

In fact since the isomorphism $\text{Hom}(G, M) \xrightarrow{\sim} \text{Hom}(\underline{\omega}_{G^*}, M)$ is composed from three isomorphisms:

1) $\text{Hom}(G, M) \xrightarrow{\sim} \mathfrak{a}(M)$

2) $\mathfrak{a}(M) \xrightarrow{\sim} \text{Ker}\,[G^*(D) \longrightarrow G^*(S)]$

3) $\text{Ker}\,[G^*(D) \longrightarrow G^*(S)] \xrightarrow{\sim} \text{Hom}(\underline{\omega}_{G^*}, M)$

it suffices to show that each is functorial in G.

1) For T a D-scheme and $\varphi: H \longrightarrow M$,

$$\varphi'(u(T)(x)) = 1 + \rho_T \circ \varphi(T)\, u(T)(x) = (\varphi \circ u)'(x) \quad \text{for any } x \text{ in } G(T).$$

2) This follows immediately from the proof that

$$\underline{\text{Hom}}(G, \mathbb{G}_m) \xrightarrow{\sim} G^* \quad [\text{S.G.A. 3 VII A 3.3}]$$

3) Let $G^* = \text{Spec}(C)$, $H^* = \text{Spec}(B)$, C and B two finite locally-free $\mathcal{O}_S$-algebras. The Cartier dual of $u: G \longrightarrow H$ corresponds to a bi-algebra homomorphism $f: C \longrightarrow B$. The identification of $\text{Hom}(\underline{\omega}_{H^*}, M)$ with the kernel of $H^*(D) \longrightarrow H^*(S)$ is made via thinking of $\tau: \underline{\omega}_{H^*} \longrightarrow M$ as an $\mathcal{O}_S$-linear derivation $B \longrightarrow M$ (with M viewed as B module via $\eta_B: B \longrightarrow \mathcal{O}_S$) and then associating to τ the homomorphism $B \longrightarrow D_{\mathcal{O}_S}[M]$

given by $b \longmapsto \eta_B(b) + \tau(b)$ for b a local section of B. Composing this with f we find the homomorphism $C \longrightarrow D_{\mathcal{O}_S}(M)$ with $c \longmapsto \eta_C(c) + \tau(f(c))$. This makes obvious the functoriality in question.

(1.7) Let S be a scheme on which p^N is zero. For G a Barsotti-Tate group on S and M a quasi-coherent module, $\text{Hom}_{S\text{-gr.}}(G, M) = (0)$ because G is p-divisible and p^N times any homomorphism $f: G \longrightarrow M$ is zero, i.e., there is a commutative diagram:

$$\begin{array}{ccc} G & \xrightarrow{f} & M \\ {\scriptstyle p^N}\downarrow & & \downarrow{\scriptstyle p^N} \\ G & \xrightarrow{f} & M \end{array}$$

Therefore an extension of G by M admits no trivial automorphism and an extension is uniquely determined by its class in $\text{Ext}^1(G, M)$.

<u>Definition</u> (1.8) An extension (E) $0 \longrightarrow \underline{V}(G) \longrightarrow E(G) \longrightarrow G \longrightarrow 0$ of G by a vector group $\underline{V}(G)$ (i.e., a quasi-coherent module) is said to be universal if given any extension $0 \longrightarrow M \longrightarrow * \longrightarrow G \longrightarrow 0$ of G by another vector group there is a unique linear map $\underline{V}(G) \xrightarrow{\varphi} M$ such that $\varphi_*((E))$ is the given extension.

<u>Remark</u> (1.9) Because of the rigidity of the category of extensions EXT (G, M), it follows that there is no ambiguity in the way in which $\varphi_*((E))$ "is" the given extension and that a universal extension is determined up to unique isomorphism (rather than just its extension class).

Proposition (1.10) The hypotheses being those of (1.7), there is a universal extension of G by a vector group.

Proof: Consider the exact sequence

(1.10.1) $0 \longrightarrow G(N) \longrightarrow G \xrightarrow{p^N} G \longrightarrow 0.$

"Applying" Hom (_, M) we find a long exact sequence:

$0 \longrightarrow \mathrm{Hom}(G, M) \longrightarrow \mathrm{Hom}(G, M) \longrightarrow \mathrm{Hom}(G(N), M) \xrightarrow{\delta} \mathrm{Ext}^1(G, M) \longrightarrow \mathrm{Ext}^1(G, M).$

Since Ext is a bi-functor, the map $\mathrm{Ext}^1(G,M) \longrightarrow \mathrm{Ext}^1(G, M)$ comes from multiplication by p^N on M. Hence it is zero. This means there is an isomorphism induced by the coboundary map δ, $\delta\colon \mathrm{Hom}(G(N), M) \xrightarrow{\sim} \mathrm{Ext}^1(G, M)$. This isomorphism is certainly functorial in M. But by (1.3) the functor which occurs on the left-hand side above is represented by $\underline{\omega}_{G(N)^*}$. Therefore by definition of the connecting homomorphism δ, it follows that the extension induced from (1.10.1) by α:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G(N) & \longrightarrow & G & \xrightarrow{p^N} & G & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow & & \| & & \\ 0 & \longrightarrow & \underline{\omega}_{G(N)^*} & \longrightarrow & \underline{\omega}_{G(N)^*} \amalg^{G(N)} G & \longrightarrow & G & \longrightarrow & 0 \end{array}$$

is universal.

Remark (1.11) The integer N could have been replaced with any $n \geq N$ and the extension obtained would certainly be universal. In fact the unique

isomorphism between two such extensions comes from the commutative diagram (1.6)

$$\begin{array}{ccc} G(N+i) & \xrightarrow{p^i} & G(N) \\ \alpha \downarrow & & \downarrow \alpha \\ \underline{\omega}_{G(N+i)^*} & \xrightarrow{\sim} & \underline{\omega}_{G(N)^*} \end{array}$$

The fact that $\underline{\omega}_{G(N+i)^*} \longrightarrow \underline{\omega}_{G(N)^*}$ is an isomorphism is [II 3.3.20].

Definition (1.12) For n sufficiently large we write $\underline{\omega}_{G(n)^*} = \underline{V}(G)$ and the universal extension constructed above is written $0 \longrightarrow \underline{V}(G) \longrightarrow E(G) \longrightarrow G \longrightarrow 0$. Thus E(G) is an f.p.p.f. sheaf of groups on S, determined up to unique isomorphism.

Lemma (1.13) The universal extension $0 \longrightarrow \underline{V}(G) \longrightarrow E(G) \longrightarrow G \longrightarrow 0$ commutes with an arbitrary base change $S' \longrightarrow S$.

Proof: From its construction via the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G(N) & \longrightarrow & G & \xrightarrow{p^N} & G & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow & & \| & & \\ 0 & \longrightarrow & \underline{V}(G) & \longrightarrow & E(G) & \longrightarrow & G & \longrightarrow & 0 \end{array},$$

what must be shown is that $\alpha\colon G(N) \longrightarrow \underline{\omega}_{G(N)^*}$ commutes with base change. Since Cartier duality is compatible with base change and since $\underline{\omega}_{G(N)^*}$ is [II 3.3.20] locally-free, this follows from the explicit description of α given in (1.5).

Corollary (1.14): Assume p is locally nilpotent on S and let G be a Barsotti-Tate group on S. There is a universal extension $0 \to \underline{V}(G) \to E(G) \to G \to 0$ of G by a vector group with $\underline{V}(G) = \underline{\omega}_{G^*}$.

Proof: Cover S by affine open sets U_i and consider for each i the universal extension of $G|U_i$ by $\underline{V}(G|U_i) = \underline{\omega}_{G^*}|U_i$. By the lemma, the two extensions obtained on $U_i \cap U_j$ are canonically isomorphic. This guarantees the co-cycle condition for $U_i \cap U_j \cap U_k$ and tells us that the $E(G|U_i)$ can be glued together to give us a sheaf of groups $E(G)$ on S. We obviously obtain an exact sequence $0 \to \underline{\omega}_{G^*} \to E(G) \to G \to 0$ which gives us the desired universal extension.

Proposition (1.15) Let p be locally nilpotent on S and G, H two Barsotti-Tate groups on S with $u: G \to H$ a homomorphism. There is a unique homomorphism $E(u): E(G) \to E(H)$ such that we obtain a morphism of extensions:

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

(where $\underline{V}(u)$ is the map induced on the invariant differentials by the Cartier dual of u).

Proof: Because of the uniqueness assertion it suffices to prove the proposition locally on S and hence it can be assumed that p^N kills S. Consider the following two diagrams:

(I)
$$\begin{array}{ccccccccc} 0 & \longrightarrow & \underline{\omega}_{G(N)^*} & \longrightarrow & E(G) & \longrightarrow & G & \longrightarrow & 0\\ & & \Big\downarrow{\scriptstyle \underline{V}(u)} & & \Big\downarrow & & \Big\Vert & & \\ 0 & \longrightarrow & \underline{\omega}_{H(N)^*} & \longrightarrow & \underline{\omega}_{H(N)^*} \coprod_{\underline{\omega}_{G(N)^*}} E(G) & \longrightarrow & G & \longrightarrow & 0\end{array}$$

(II)
$$\begin{array}{ccccccccc} 0 & \longrightarrow & \underline{\omega}_{H(N)^*} & \longrightarrow & E(H) \times_H G & \longrightarrow & G & \longrightarrow & 0\\ & & \Big\Vert & & \Big\downarrow & & \Big\downarrow{\scriptstyle u} & & \\ 0 & \longrightarrow & \underline{\omega}_{H(N)^*} & \longrightarrow & E(H) & \longrightarrow & H & \longrightarrow & 0\end{array}$$

Since the uniqueness assertion is a consequence of $\mathrm{Hom}\,(G, \underline{\omega}_{H(N)^*}) = (0)$, it suffices to know that the lower row of (I) is isomorphic to the upper row of (II).

From the functoriality of the connecting homomorphism we have a commutative diagram:

$$\begin{array}{ccc} \mathrm{Hom}\,(H(N), \underline{\omega}_{H(N)^*}) & \xrightarrow{\sim} & \mathrm{Ext}^1(H, \underline{\omega}_{H(N)^*})\\ \Big\downarrow & & \Big\downarrow \\ \mathrm{Hom}\,(G(N), \underline{\omega}_{H(N)^*}) & \xrightarrow{\sim} & \mathrm{Ext}^1(G, \underline{\omega}_{H(N)^*})\end{array}$$

By the functoriality of (1.6), there is also a commutative diagram:

$$\begin{array}{ccc}
\mathrm{Hom}\,(\underline{\omega}_{H(N)^*}, \underline{\omega}_{H(N)^*}) & \xrightarrow{\sim} & \mathrm{Hom}\,(H(N), \underline{\omega}_{H(N)^*}) \\
\downarrow & & \downarrow \\
\mathrm{Hom}\,(\underline{\omega}_{G(N)^*}, \underline{\omega}_{H(N)^*}) & \xrightarrow{\sim} & \mathrm{Hom}\,(G(N), \underline{\omega}_{H(N)^*})
\end{array}$$

Combining these two diagrams it is immediate that the lower row of (I) and the upper row of (II) correspond to the two ways of taking $\mathrm{id}_{\underline{\omega}_{H(N)^*}}$ into $\mathrm{Ext}^1(G, \underline{\omega}_{H(N)^*})$. Thus the two rows are isomorphic as claimed.

(1.16) We wish to show that $\overline{E(G)}$ is a formal Lie group on S. This is a local question and hence S can be assumed to be affine.

Lemma (1.17) $\mathrm{Inf}^k(E(G))$ is representable and of finite presentation.

Proof: Let p^N kill S so that $\mathrm{Inf}^k(G) \subseteq G(n+N-1)$ if $k < p^n$ [II (3.3.17)]. Consider the extension

(1.17.1) $0 \longrightarrow \underline{V}(G) \longrightarrow E(G) \underset{G}{\times} G(n+N-1) \longrightarrow G(n+N-1) \longrightarrow 0$

Since $\mathrm{Inf}^k(E(G))$ maps to $\mathrm{Inf}^k(G)$, it follows that $\mathrm{Inf}^k(E(G)) = \mathrm{Inf}^k(E(G) \underset{G}{\times} G(n+N-1))$. Because $\underline{V}(G)$ and $G(n+N-1)$ are schemes it follows that $E(G) \underset{G}{\times} G(n+N-1)$ is a scheme of finite presentation since it is a torseur on $G(n+N-1)$ under $\underline{V}(G)_{G(n+N-1)}$ [G.A. III §4 1.9]. Thus $\mathrm{Inf}^k(E(G))$ is representable by a scheme of finite presentation.

Lemma (1.18) (Assuming S is affine) $E(G)$ is formally smooth.

Proof: Let $T \hookrightarrow T'$ be a nilpotent immersion with T' an (absolutely) affine S-scheme. Let $\varphi: T \longrightarrow E(G)$ be given:

$$\begin{array}{ccc}
E(G) & & \\
\uparrow \varphi & \nwarrow \varphi' & \\
T & \hookrightarrow & T'
\end{array}$$

Since T is affine and $E(G) = \varinjlim (E(G) \underset{G}{\times} G(n))$, $\varphi \in E(G) \underset{G}{\times} G(n)\,(T)$ for some n.

Consider the exact sequence:

$$0 \longrightarrow \underline{V}(G) \longrightarrow E(G) \xrightarrow{\pi} G \longrightarrow 0$$

$\pi_T(\varphi) \in G(n)\,(T)$ and hence by the formal smoothness of G [II (3.3.13)] it can be assumed (by augmenting n if necessary) that $\pi_T(\varphi): T \longrightarrow G(n)$ can be lifted to T'.

Since S is affine and $\underline{V}(G)$ is a quasi-coherent module all torseurs under $\underline{V}(G)_{G(n)}$ are trivial [G.A. I §1, 2.7; S.G.A. 4 VII 4.4]. This implies that the morphism $E(G) \underset{G}{\times} G(n) \longrightarrow G(n)$ admits a section. Thus the morphism $T' \longrightarrow G(n)$ gives rise to $\psi: T' \longrightarrow E(G) \underset{G}{\times} G(n)$. $\psi|T$ and φ certainly have the same image in $G(n)\,(T)$. Hence $\varphi - \psi|T$ belongs to $\underline{V}(G)(T)$. Since $\underline{V}(G)$ is smooth, $\varphi - \psi|T$ can be lifted to $\eta: T' \longrightarrow \underline{V}(G)$. Thus $\eta + \psi: T' \longrightarrow E(G) \underset{G}{\times} G(n)$ and $\eta + \psi|T = \varphi$. This proves $E(G)$ is formally smooth.

Proposition (1.19) $\overline{E(G)}$ is a formal Lie group.

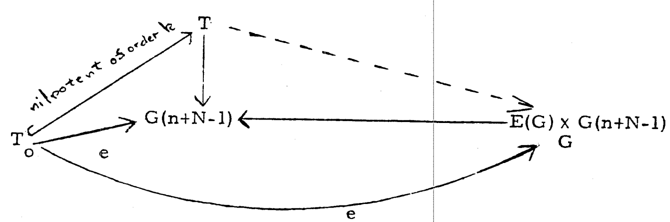
Proof: Since $\overline{E(G)}$ is by (1.18) formally smooth (locally at least) it follows immediately from [II 3.1.1] and (1.17) that $\overline{E(G)}$ is a formal Lie group. In particular $\overline{E(G)}$ is formally smooth.

Definition (1.20) $\underline{\mathrm{Lie}}\,(E(G)) = \underline{\mathrm{Lie}}\,(\overline{E(G)}) =$ (if p^N kills S) $\mathrm{Lie}\,(E(G) \underset{G}{\times} G(N))$.

It is a locally free (of finite rank) sheaf of $\mathcal{O}_S$-modules.

Proposition (1.21) The sequence $0 \longrightarrow \overline{\underline{V}(G)} \longrightarrow \overline{E(G)} \longrightarrow \overline{G} \longrightarrow 0$ is exact.

Proof: The only non-trivial fact is that $\overline{E(G)} \longrightarrow \overline{G}$ is an epimorphism. Because this is a statement about sheaves it suffices to prove it locally. Hence it can be assumed that S is affine and killed by p^N. It must be shown that the map $\mathrm{Inf}^k(E(G)) \longrightarrow \mathrm{Inf}^k(G)$ is an epimorphism (for all k). As was noted in the proof of (1.18), $E(G) \times_G G(n+N-1)$ is as $G(n+N-1)$-scheme isomorphic to $\underline{V}(G)_{G(n+N-1)}$, and therefore is smooth over $G(n+N-1)$. Consider the following diagram, with T affine:



By the smoothness noted above, the dotted arrow can be filled in so as to obtain a commutative diagram. Clearly this implies that

$$\mathrm{Inf}^k(E(G)) \longrightarrow \mathrm{Inf}^k(G) \text{ is an epimorphism.}$$

Proposition (1.22) The sequence $0 \longrightarrow \underline{V}(G) \longrightarrow \underline{\mathrm{Lie}}\,(E(G)) \longrightarrow \underline{\mathrm{Lie}}\,(G) \longrightarrow 0$ is exact.

Proof: Once again the assertion is local so it can be assumed that S is affine and p^N kills S. Then the map $E(G) \times_G G(N) \longrightarrow G(N)$ admits a section (see the proof of 1.18) and hence it is an epimorphism of

presheaves. This certainly implies that $\underline{\mathrm{Lie}}\,(E(G)) \longrightarrow \underline{\mathrm{Lie}}\,(G)$ is an epimorphism (as both are finite and locally free: see [S.G.A.3 II 4.11]). The exactness of the rest of the sequence is obvious.

Remark (1.23) We indicate how the results of this paragraph are to be modified (usually simplified) so as to apply to abelian schemes. By [I (3.4)] the morphism $p: A \longrightarrow A$ is an epimorphism of the abelian scheme A and hence (1.7) - (1.12) are carried over with only the change of replacing everywhere the words "Barsotti-Tate group" with the words "abelian scheme" (i.e., with no change). In (1.14) the symbol $\underline{\omega}_{G^*}$ is to be replaced by $\underline{\omega}_{A(\infty)^*}$ where $A(\infty) \overset{\text{def.}}{=} \varinjlim A(n)$. (1.15) goes through with no change. (1.16) - (1.19) can be simplified since from the exact sequence $0 \longrightarrow \underline{V}(A) \longrightarrow E(A) \longrightarrow A \longrightarrow 0$ (where $\underline{V}(A)$ is locally given as $\underline{\omega}_{A(N)^*}$), it follows that $E(A)$ is a smooth S-scheme and $E(A) \longrightarrow A$ is a smooth morphism: [G.A. III §4 1.9, E.G.A. IV 17.7.3(ii)]. This immediately implies $\overline{E(A)}$ is a formal Lie group. (1.20) remains unchanged and the proof of (1.21) can be simplified by repeating the reasoning of [II (4.11)] utilizing the fact that $E(A) \longrightarrow A$ is smooth to make the simplification. The proof of (1.22) can be simplified using smoothness just as before.

§2. (2.0) The purpose of this paragraph is to associate to certain Barsotti-Tate groups on a scheme S_o (where p is locally nilpotent) various crystals. The word "certain" is undoubtedly unnecessary as was already noted in the introduction. To such a B.T. group G, there will be associated:

1) a crystal in (f.p.p.f) groups: $\mathbb{E}(G)$

2) a crystal in formal Lie groups: $\overline{\mathbb{E}}(G)$

3) a crystal in finite locally-free modules: $\mathbb{D}(G)$

(i.e., a locally-free sheaf on the crystalline site).

The constructions will be such that $\overline{\mathbb{E}}(G)$ is (as the notation suggests) obtained from $\mathbb{E}(G)$ by "completing along the unit section," while $\mathbb{D}(G)$ will be obtained from $\mathbb{E}(G)$ by applying <u>Lie</u>. Hence it is clear that $\mathbb{E}(G)$ is the basic crystal to construct. Again, as the notation is intended to suggest, $\mathbb{E}(G)$ will be obtained by "crystallizing" E(G).

<u>Notation</u> (2.1) $\dot{S}_o$ will denote a scheme with p locally nilpotent on it. $B.T.'(S_o)$ will denote the full sub-category of $B.T.(S_o)$ consisting of those G_o with the following property: There is an open cover of S_o (depending on G_o) formed of affine open sets $U_o \subseteq S_o$ such that for any nilpotent immersion $U_o \hookrightarrow U$ there is a B.T. group G on U with $G|U_o = G_o|U_o$.

<u>Remark</u> (2.1.1) Since amalgamated sums of affine schemes exist, a morphism $f: T_o \longrightarrow S_o$ induces $f^*: B.T.'(S_o) \longrightarrow B.T.'(T_o)$. Also the condition of (2.1) implies that any affine open subset of an element of the cover satisfies the same hypothesis. The B.T. groups in $B.T.'(S_o)$ are "locally infinitesimally liftable."

We can now formulate the main theorem which allows the construction of the crystal $\mathbb{E}(G)$.

<u>Theorem</u> (2.2) Let S = Spec (A), $p^N \cdot 1_S = 0$, S_o = <u>Var (I)</u> where I is an ideal of A with nilpotent divided powers. Let G and H be two B.T. groups on S and assume $u_o: G_o \longrightarrow H_o$ is a homomorphism between their restrictions to S_o. u_o defines a morphism $v_o = E(u_o): E(G_o) \longrightarrow E(H_o)$ of extensions:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \underline{V}(G_o) & \longrightarrow & E(G_o) & \longrightarrow & G_o & \longrightarrow & 0 \\ & & \downarrow \underline{V}(u_o) & & \downarrow v_o & & \downarrow u_o & & \\ 0 & \longrightarrow & \underline{V}(H_o) & \longrightarrow & E(H_o) & \longrightarrow & H_o & \longrightarrow & 0 \end{array}$$

There is a unique morphism of groups $v: E(G) \longrightarrow E(H)$ (not necessarily respecting the structure of extensions) with the following properties:

1) v is a lifting of v_o

2) Given $w: \underline{V}(G) \longrightarrow \underline{V}(H)$, a lifting of $\underline{V}(u_o)$, denote by i the inclusion $\underline{V}(H) \longrightarrow E(H)$, so that $d = i \circ w - v|\underline{V}(G): \underline{V}(G) \longrightarrow E(H)$ induces zero on S_o. Then, d is an <u>exponential</u> (an assertion which makes sense by [III 2.4]).

<u>Remark</u> (2.3) The morphism v is independent of w. For if $w' = w + h$ was a second lifting of $\underline{V}(u_o)$, h would map $\underline{V}(G)$ to $\overline{\underline{V}(H)}$ and would obviously be an exponential. But defining d′ (corresponding to w′) as above, $d' = d + ih$. Since $i \circ h$ is clearly identified with $\bar{i} \circ h$, $\bar{i}: \overline{\underline{V}(H)} \longrightarrow \overline{E(H)}$, it is obvious that (denoting by B the hyperalgebra of the formal Lie group $\overline{E(H)}$) $\bar{i} \circ h(x) = \bar{i}\,(\Sigma\, (h(x))^{(n)}) = \Sigma\, (\bar{i} \circ h(x))^{(n)}$ (identifying $\bar{i}: \overline{\underline{V}(H)} \longrightarrow \overline{E(H)}$ with the corresponding $\Gamma(\underline{V}(H)) \longrightarrow B$) and thus that $i \circ h$ is

an exponential. Hence d' is an exponential if and only if d is one.

(2.4) Prior to proving the theorem let us give the corollaries which allow the construction of $\mathbb{E}(G)$.

Corollary (2.4.1) Let K be a third B.T. group on S and $u'_o : H_o \longrightarrow K_o$ a homomorphism. Denote the v whose existence is guaranteed by the theorem, by $E_S(u_o)$. Then $E_S(u'_o \circ u_o) = E_S(u'_o) \circ E_S(u_o)$.

Proof: Let $v' = E_S(u'_o)$. Since $v' \circ v$ is a lifting of $E(u'_o \circ u_o)$, it must be shown that $v' \circ v$, satisfies the condition concerning the exponential. Let $w: \underline{V}(G) \longrightarrow \underline{V}(H)$ and $w': \underline{V}(H) \longrightarrow \underline{V}(K)$ be liftings of $\underline{V}(u_o)$ and $\underline{V}(u'_o)$. Note such liftings exist by [4(bis) Algèbre Chap. II §5, prop. 7(ii)]. Let $i': \underline{V}(K) \longrightarrow E(K)$ be the inclusion and set $d'' = i' \circ (w' \circ w) - (v' \circ v) | \underline{V}(G)$. It must be shown that d'' is an exponential. Consider the following diagram:

$$\begin{array}{ccccc}
0 & \longrightarrow & \underline{V}(G) & \longrightarrow & E(G) \\
 & & \downarrow w & & \downarrow v \\
0 & \longrightarrow & \underline{V}(H) & \xrightarrow{i} & E(H) \\
 & & \downarrow w' & & \downarrow v' \\
0 & \longrightarrow & \underline{V}(K) & \xrightarrow{i'} & E(K)
\end{array}$$

By hypothesis $i' \circ w' = v' \circ i + \exp(\theta')$, where $\theta': \underline{V}(H) \longrightarrow I \cdot \underline{\mathrm{Lie}}(E(K))$. Thus $i' \circ (w' \circ w) = v' \circ (i \circ w) + \exp(\theta') \circ w$. But $i \circ w = v | \underline{V}(G) + \exp(\theta)$, $\theta: \underline{V}(G) \longrightarrow I \cdot \underline{\mathrm{Lie}}(E(H))$. Hence $i' \circ (w' \circ w) = v' \circ v | \underline{V}(G) + v' \circ \exp(\theta) + \exp(\theta' \circ w)$. Just as in remark (2.3) it is clear that $v' \circ \exp(\theta) + \exp(\theta' \circ w)$

is an exponential. This proves the corollary.

Corollary (2.4.2) If $G = H$ and $u_o = id_{G_o}$, then $E_S(u_o) = id_G$.

Proof: This is immediate from the uniqueness assertion.

Corollary (2.4.3) Let G, H, u_o be as above and assume u_o is an isomorphism. $E_S(u_o)$ is an isomorphism.

Proof: This is a formal consequence of (2.4.1) and (2.4.2).

Corollary (2.4.4) Suppose there is a commutative diagram:

$$\begin{array}{ccc}
S_o & \hookrightarrow & S \\
\uparrow & & \uparrow \\
S'_o & \hookrightarrow & S'
\end{array}$$

where $S_o \hookrightarrow S$ and $S'_o \hookrightarrow S'$ are nilpotent immersions of the type hypothesized in the statement of the theorem. Let $S'_o = \mathrm{Var}(J)$, $S_o = \mathrm{Var}(I)$ and assume $S' \longrightarrow S$ is a divided power morphism. Let G and H be two B.T. groups on S and $u_o : G_o \longrightarrow H_o$ be given. Under these circumstances the construction of the theorem is compatible with the base change $S' \longrightarrow S$: $E_{S'}(u_{o_{S'_o}}) = (E_S(u_o))_{S'} = v_{S'}$.

Proof: Since $v_{S'}$ lifts $u_{o_{S'_o}}$, it must be shown that the exponential condition is verified by $v_{S'}$. (We are of course using (1.13) to know the corollary makes sense.)

In the notation of the theorem let $w: \underline{V}(G) \longrightarrow \underline{V}(H)$ lift $\underline{V}(u_o)$.

$w_{S'}$ lifts $\underline{V}(u_{o_{S'_o}})$ and it must be shown that $d' = i_{S'} \circ w_{S'} - v_{S'} | \underline{V}(G_{S'})$ is an exponential. By its definition d' is $d_{S'}$ where d is as in the statement of the theorem. If $d = \exp(\theta)$ where $\theta : \underline{V}(G) \longrightarrow I \cdot \underline{\mathrm{Lie}}(E(H))$, then $d_{S'}$ is (obviously) $\exp(\theta_{S'})$ where $\theta_{S'} : \underline{V}(G_{S'}) \longrightarrow J \cdot \underline{\mathrm{Lie}}(E(H_{S'}))$ is deduced from θ via extension of scalars.

(2.5) Let us show how the corollaries permit the construction of the crystals. Let S_o be an arbitrary scheme (with p locally nilpotent on it) and let G_o be in B.T.′ (S_o). By the reasoning recalled in [III (3.8)]: namely that f.p.p.f. groups form a stack with respect to the Zariski topology, it suffices to give the value of the crystal $\mathbb{E}(G_o)$ on objects $U_o \hookrightarrow U$ of the crystalline site of S_o with the property that $G_o | U_o$ can be lifted to U, and U_o is affine.

It is precisely the content of (2.4.1) and (2.4.3) that up to canonical isomorphism the group $E(G)$ is independent of the lifting of $G_o | U_o$ which has been chosen.

If $V_o \hookrightarrow V$ was a second object of the crystalline site and there was given a morphism

$$\begin{array}{ccc} U_o & \hookrightarrow & U \\ \uparrow f & & \uparrow \bar{f} \\ V_o & \hookrightarrow & V \end{array}$$

then for a lifting G_U of $G_o | U_o$ to U and a lifting G_V of $G_o | V_o$ to V the same corollaries give a canonical isomorphism $\bar{f}^*(E(G_U)) \xrightarrow{\sim} E(G_V)$.

It is now clear that the value of the crystal $\mathbb{E}(G_o)$ on an object

$U_o \hookrightarrow U$ (as above) is simply $E(G)$ for <u>some</u> choice of lifting of $G_o | U_o$ to U (i.e., chosen via the Hilbert ϵ-function).

In the same way it is clear that for $u_o : G_o \longrightarrow H_o$ a homomorphism between two B.T.′ groups, there is a morphism $\mathbb{E}(u_o)$ between the associated crystals which is defined on a "sufficiently small" open set $U_o \hookrightarrow U$ via $E_U(u_o)$ in the notation introduced above.

Let $f : T_o \longrightarrow S_o$ be an arbitrary morphism. The crystal $f^*(\mathbb{E}(G_o))$ is determined by its values on "sufficiently small" open sets in the crystalline site of T_o. Choose "sufficiently small" to mean that the object $V_o \hookrightarrow V$ has two properties:

1) $f(V_o) \subseteq U_o$ and $G_o | U_o$ can be lifted to infinitesimal neighborhoods.
2) V_o is affine.

Then using the amalgamated sum construction, as in [III (3.8)], we build the diagram

$$\begin{array}{ccc} U_o & \hookrightarrow & U = U_o \coprod_{V_o} V \\ \uparrow f & & \uparrow \bar{f} \\ V_o & \hookrightarrow & V \end{array}$$

It is immediate that, for a lifting G of $G_o | U_o$ to U,

$$\bar{f}^*(E(G)) = E(G_V) = \mathbb{E}(f^*(G_o))_{V_o \hookrightarrow V} .$$

Thus $\qquad f^*(\mathbb{E}(G_o)) = \mathbb{E}(f^*(G_o))$.

Of course the last equalities have to be taken with a grain of salt and a more precise statement would be that the following diagram is commutative up to a unique natural equivalence:

$$\begin{array}{ccc} B.T.'(S_o) & \xrightarrow{\mathbb{E}} & (\text{Crystals in f.p.p.f. groups on } S_o) \\ f^* \downarrow & & \downarrow f^* \\ B.T.'(T_o) & \xrightarrow{\mathbb{E}} & (\text{Crystals in f.p.p.f. groups on } T_o) \end{array} \quad (2.5.1)$$

It is obvious that $\mathbb{E}$ is an additive functor and therefore that the functors $\overline{\mathbb{E}}$ and $\mathbb{D}$ defined below are additive.

$\overline{\mathbb{E}}$ is defined via

(2.5.2) $$\overline{\mathbb{E}}(G_o)_{U_o \hookrightarrow U} = \overline{\left(\mathbb{E}(G_o)_{U_o \hookrightarrow U}\right)}$$

for any object $U_o \hookrightarrow U$ of the crystalline site of S_o.

$\mathbb{D}$ is defined via:

(2.5.3) $$\mathbb{D}(G_o)_{U_o \hookrightarrow U} = \underline{\text{Lie}}\left(\overline{\mathbb{E}}(G_o)_{U_o \hookrightarrow U}\right)$$

for any object $U_o \hookrightarrow U$ of the crystalline site.

(2.5.4) To summarize: if $S_o \hookrightarrow S$ is a nilpotent divided power immersion and G_o can be lifted to a B.T. group G on S, then (up to canonical isomorphism)

1) $\mathbb{E}(G_o)_{S_o \hookrightarrow S} = E(G)$

2) $\overline{\mathbb{E}}(G_o)_{S_o \hookrightarrow S} = \overline{E(G)}$

3) $\mathbb{D}(G_o)_{S_o \hookrightarrow S} = \underline{\text{Lie}}\,(E(G))$.

(2.6) We now turn to the proof of the theorem (2.2). Several preliminary lemmas are necessary. It is Lemma (2.6.3) which plays the crucial role.

Lemma (2.6.1) Under the hypotheses of (2.2) made on S, let G be a Barsotti-Tate group on S. For $n \geq N$, the group $L = E(G) \times_G G(n)$ satisfies the hypotheses of (III 2.6.4) and hence the exponential mapping exp: $\text{Hom}\,(M, I\cdot\underline{\text{Lie}}\,(L)) \hookrightarrow \text{Ker}\,[\text{Hom}\,(M, L) \longrightarrow \text{Hom}\,(M_o, L_o)]$ is defined for any locally-free module M.

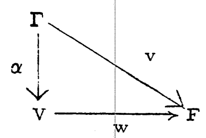
Proof: The first sentence of the proof of (1.2 2) tells us that $E(G) \times_G G(n) \longrightarrow G(n)$ admits a section. Since $E(G) \times_G G(n)$ is a group and the section is a morphism of S-schemes, by translation by an appropriate element of the kernel $\underline{V}(G)\,(S)$ it can be assumed that the section preserves the unit section. Consider the isomorphism of $G(n)$-schemes $E(G) \times_G G(n) \xrightarrow{\sim} \underline{V}(G) \times_S G(n)$ determined by this section. It is obvious that it takes unit section to unit section and hence is an isomorphism of pointed S-schemes.

(2.6.2) Let S, S_o be as in the statement of the theorem. Let Γ be a finite locally-free group on S such that $\underline{\omega}_{\Gamma^*} = V$ is locally-free. Denote by α the canonical map $\Gamma \longrightarrow V$ of (1.4). Let F be a group on S which is one of the three types given as examples in [III (2.7)]. In particular this means the exponential map $\text{Hom}\,(V, I\cdot\underline{\text{Lie}}\,(F)) \overset{\exp}{\hookrightarrow} \text{Ker}[\text{Hom}(V,F) \longrightarrow \text{Hom}\,(V_o, F_o)]$ is defined. Assume further that $\underline{\omega}_F$ is finite and locally free . (This is only an assumption for F of the third type [c.f. III (2.7)] and here it has an obvious meaning.)

Lemma (2.6.3) Let $w_o : V_o \longrightarrow F_o$ be a homomorphism and let Θ be a linear class of liftings [III (2.7.2)] $w: V \longrightarrow F$. Let $v: \Gamma \longrightarrow F$

satisfy $v_o = w_o \circ \alpha_o$. There is a unique w' in Θ such that $w' \circ \alpha = v$.

In other words: given a diagram



which becomes commutative when pulled back to S_o, there is a unique $w': V \longrightarrow F$ such that

1) $v = w' \circ \alpha$

2) $w'_o = w_o$

3) $w' - w$ is an exponential.

(2.6.4) We first make two simple reductions.

<u>1st reduction</u>: Set $w' = w + h$ and $v' = v - w \circ \alpha$.

Then the conditions 1) - 3) to be satisfied become:

1) $v' = h \circ \alpha$

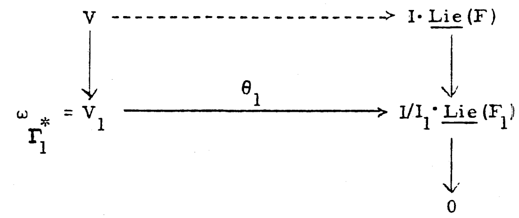
2) $h_o = 0$

3) h is an exponential.

This reduces us to considering the case $w = 0$, $v_o = 0$.

<u>2nd reduction</u>: Take a finite filtration of S: $S = S_r \supseteq S_{r-1} \supseteq \cdots \supseteq S_o$ such that each S_i is defined by an ideal I_i stable under the divided powers induced by I. Assume that the lemma is true step by step. We claim then, that the lemma is true. To verify this it obviously suffices to consider a filtration $S \supseteq S_1 \supseteq S_o$ and to verify the claim in this case.

Let the subscript "1" denote the objects obtained by making the base change $S_1 \hookrightarrow S$. By hypothesis there is a unique $\theta_1 : \omega_{\Gamma_1^*} \longrightarrow I/I_1 \cdot \underline{\mathrm{Lie}}(F_1)$ such that $\exp(\theta_1) \circ \alpha_1 = v_1$. Consider the diagram



Since V is projective (being finite and locally-free) there is a $\theta_2 : V \longrightarrow I \cdot \underline{\mathrm{Lie}}(F)$ which will make the diagram commutative.

The functoriality of the exponential implies that $\exp(\theta_2): V \longrightarrow F$ will reduce to $\exp(\theta_1)$.

Let us apply the hypothesis that the lemma is true to the pair (S, S_1) and the map $\exp(\theta_2)$. Thus there is a unique $\theta_3 : V \longrightarrow I_1 \cdot \underline{\mathrm{Lie}}(F)$ such that $\exp(\theta_2 + \theta_3) \circ \alpha = v$. This gives us the existence of a solution. To show uniqueness let $\theta' : V \longrightarrow I \cdot \underline{\mathrm{Lie}}(F)$ be any solution. Then $\exp(\theta')$ restricted to S_1 is clearly a solution of the problem for the pair (S_1, S_o). By the uniqueness of such a solution $\theta'_1 = \theta_1$ and hence $(\theta' - \theta_2)_1 = 0$. This implies that $\exp(\theta')$ and $\exp(\theta_2)$ are linearly equivalent and hence, by the uniqueness assumption made for the pair (S, S_1), implies $\theta' = \theta_2 + \theta_3$.

<u>Application</u>: The ideals defined in [II (4.1)] are clearly stable under the divided powers of I. Hence it suffices to prove the lemma under the additional hypothesis that $p \cdot I = I^2 = (0)$.

(2.6.5) Let us observe that without loss of generality F can be assumed to be a group scheme. The reason for this is: By hypothesis F is either a group scheme or a filtering direct limit of (sub) group schemes. The map $v: \Gamma \longrightarrow F$ will factor through one of the representable sub-groups since Γ is quasi-compact. Furthermore if F is not representable, our hypothesis on F tells us that the exponential is defined for each of the representable sub-groups in question.

Finally let us observe that F can be assumed to be $\mathcal{C}\mathrm{spec}\,(B)$ for some bi-algebra B. This is obvious for the groups in the second and third examples of [III (2.7)]. If F is a smooth group; then, since the exponential really depends only on the formal Lie group $\bar{F}$, this is clearly permissible [c.f. III (2.4)].

(2.6.6) Proof of (2.6.3):

Let $i: S_o \hookrightarrow S$ be the inclusion and consider the canonical homomorphism $F \longrightarrow i_*(F_o)$. Let K be its kernel. By [S.G.A. 3 III (0.9)]

(2.6.6.1) $$K(T) = \mathrm{Hom}_{\mathcal{O}_{S_o}}\left(\underline{\omega}_{F_o} \otimes_{\mathcal{O}_{S_o}} \mathcal{O}_{T_o},\ I \cdot \mathcal{O}_T\right)$$

for any S-scheme T. For typographical reasons, the "W( )" notation of [S.G.A. 3 I 4.6] will not be used below and the same symbol will be used for a quasi-coherent $\mathcal{O}_S$-module and the corresponding $\underline{\underline{\mathcal{O}}}_S$-module, ...

By [S.G.A. 3 III (0.6)] the restriction of K to the full sub-category of Sch. /S consisting of flat S-schemes is $i_*\left(\underline{\mathrm{Hom}}_{\mathcal{O}_{S_o}}(\underline{\omega}_{F_o}, I)\right)$. Since $v: \Gamma \longrightarrow F$ reduces to zero over S_o, v is a homomorphism $\Gamma \longrightarrow K$.

A homomorphism $\Gamma \longrightarrow K$ is an element $v \in K(\Gamma)$ such that $\mu_\Gamma^*(v) = \mu_K((v \times v))$ in $K(\Gamma \times \Gamma)$ (here $\mu_\Gamma: \Gamma \times \Gamma \longrightarrow \Gamma$ is the group law on Γ and $\mu_K: K \times K \longrightarrow K$ is the group law on K). But because Γ and $\Gamma \times \Gamma$ are flat over S, this implies that a homomorphism $\Gamma \longrightarrow K$ "is" a homomorphism $\Gamma \longrightarrow i_*\left(\underline{\mathrm{Hom}}_{\mathcal{O}_{S_o}}(\underline{\omega}_{F_o}, I)\right)$. Finally by adjointness we see v "is" a homomorphism:

(2.6.6.2) $$v: \Gamma_o \longrightarrow \underline{\mathrm{Hom}}_{\mathcal{O}_{S_o}}(\underline{\omega}_{F_o}, I).$$

We are trying to find a homomorphism $w: V \longrightarrow F$ which is an exponential. To give w is thus equivalent to giving a linear homomorphism $u: V \longrightarrow \underline{\mathrm{Lie}}(F) \otimes_{\mathcal{O}_S} I$.

Since $I^2 = 0$, $\underline{\mathrm{Lie}}(F) \otimes_{\mathcal{O}_S} I = \underline{\mathrm{Lie}}(F) \otimes_{\mathcal{O}_S} \left(\mathcal{O}_{S_o} \otimes_{\mathcal{O}_S} I\right) = \underline{\mathrm{Lie}}(F_o) \otimes_{\mathcal{O}_{S_o}} I = \underline{\mathrm{Hom}}_{\mathcal{O}_{S_o}}(\underline{\omega}_{F_o}, I)$ because $\underline{\omega}_{F_o}$ is locally-free. Thus the giving of w is equivalent by adjointness to the giving of an $\mathcal{O}_{S_o}$-linear homomorphism:

$$u: V_o \longrightarrow \underline{\mathrm{Hom}}_{\mathcal{O}_{S_o}}(\underline{\omega}_{F_o}, I)$$

Since $w: V \longrightarrow F$ is to be an exponential it can be interpreted (just as v was above) as a map $w: V_o \longrightarrow \underline{\mathrm{Hom}}\,(\underline{\omega}_{F_o}, I)$.

From the way in which this identification is made it is immediate that the translation of the requirement $w \circ \alpha = v$ is $w \circ \alpha_o = v$ where w is interpreted as a homomorphism $V_o \longrightarrow \underline{\mathrm{Hom}}\,(\underline{\omega}_{F_o}, I)$ and v is interpreted as a homomorphism $\Gamma_o \longrightarrow \underline{\mathrm{Hom}}\,(\underline{\omega}_{F_o}, I)$.

Let us write $F = \text{Cospec}(B)$ where B is (a not necessarily flat) bi-algebra. In each of the three cases being treated $I \cdot B \cap \underline{\text{Prim}}(B) = I \cdot \underline{\text{Prim}}(B)$. For the case of a formal Lie group this is obvious. For the remaining two cases it follows from [III (2.3.6), (2.3.7)] since the statement is certainly true for $B = \Gamma^{\wedge}[M]$, M locally free.

We now want to make explicit how to interpret $\exp(u): V \longrightarrow F$ as a homomorphism $V_o \longrightarrow \underline{\text{Lie}}(F_o) \otimes I = I \cdot \underline{\text{Lie}}(F)$. First identifying V with $\text{Cospec}(\Gamma^{\wedge}(V))$ we know $\exp(u)(x) = \sum_{n \geq 0} (u(x))^{(n)}$ for any $x \in V$. (If B is not flat then $(u(x))^{(n)}$ is defined via the procedure of [III (2.6.7)]. The extension of the definition of $\exp(u)$ to points of V with values in an S-scheme T is obvious.)

Let us observe that the element $\sum_{n \geq 1} (u(x))^{(n)}$ of B is primitive. This follows from

$$\Delta\Big(1 + \sum_{n\geq 1} u(x)^{(n)}\Big) = \Big(1 + \sum_{n \geq 1} u(x)^{(n)}\Big) \otimes \Big(1 + \sum_{n\geq 1} u(x)^{(n)}\Big)$$

$$= 1 \otimes 1 + \Big(\sum_{n\geq 1} u(x)^{(n)} \otimes 1 + 1 \otimes \sum_{n \geq 1} u(x)^{(n)}\Big)$$

$$+ \Big(\sum_{n \geq 1} u(x)^{(n)}\Big) \otimes \Big(\sum_{n\geq 1} u(x)^{(n)}\Big)$$

and the fact that the last term is zero since each "factor" in the tensor product is in $I \cdot B$ and $I^2 = (0)$.

Thus $\sum_{n\geq 1} u(x)^{(n)}$ is primitive and obviously belongs to $I \cdot B$ and hence from the above remarks it belongs to $\underline{\text{Lie}}(F) \otimes I$.

Hence $\exp(u)$ viewed as a map $V_o \longrightarrow \underline{\text{Lie}}(F) \otimes I$ is given via $x \longmapsto \sum_{n \geq 1} u(x)^{(n)}$.

Now having interpreted what $\exp(u)$ means we must utilize our hypothesis that $p \cdot I = (0)$ in order to show that a unique $u: V_o \longrightarrow \underline{\text{Lie}}(F_o) \otimes I$ can be found so as to satisfy the conditions of the lemma.

Because $\underline{\omega}_F$ is locally free and $p \cdot I = (0)$ the giving of a linear $u: V_o \longrightarrow \underline{\text{Lie}}(F_o) \otimes I$ is equivalent to giving a linear map

$$V_o / p V_o \longrightarrow \underline{\text{Prim}}(B/(p+I) \cdot B) \otimes_{A/(p+I)} I = \underline{\text{Prim}}(B_o) \otimes I.$$

On $\underline{\text{Prim}}(B/(p+I) \cdot B)$ there is a p^{th}-power mapping π_B since this is a Lie-algebra in characteristic p.

If γ denotes the divided powers on I, then

$$\gamma_p(x+y) = \gamma_p(x) + \gamma_p(y) + \sum \gamma_i(x)\, \gamma_{p-i}(y) = \gamma_p(x) + \gamma_p(y) \quad \text{since } I^2 = (0).$$

Because $\gamma_p(\lambda x) = \lambda^p \gamma_p(x)$ it is immediate that γ_p is a p-linear mapping of I to itself.

Hence $\pi = \pi_B \otimes \gamma_p$ is an additive mapping of $\underline{\text{Lie}}(F_o) \otimes I$ to itself. It is immediate that this map extends to any scheme T_o over S_o and hence π defines a homomorphism of the group $\underline{\text{Lie}}(F_o) \otimes I$ to itself. Since $\gamma_{p^{\ell}} = (\gamma_p)^{\ell}$ [5 Exposé 3, §3, Theorem 3] the hypothesis that the divided powers are nilpotent implies π is nilpotent. Hence $\sum_{n \geq 0} \pi^n$ is an automorphism of the S_o-group $\underline{\text{Lie}}(F_o) \otimes I$.

Let $u: V_o \longrightarrow \underline{\text{Lie}}(F_o) \otimes I$ be any linear map. Let $x \in V_o$ and write $u(x) = \sum b_j \otimes i_j$. Then

$$(\sum_{n\geq 0} \pi^n) \circ u(x) = \sum_j (\sum_{n\geq 0} \pi^n (b_j \otimes i_j))$$

$$= \sum_j (\sum_{n\geq 0} b_j^{p^n} \otimes i_j^{(p^n)})$$

$$= \sum_{n\geq 0} (\sum_j b_j^{p^n} \otimes i_j^{(p^n)})$$

$$= \sum_{n\geq 0} (\sum_j (b_j \otimes i_j)^{(p^n)})$$

$$= \sum_{n\geq 0} (\sum b_j \otimes i_j)^{(p^n)} \quad \text{as } I^2 = 0$$

$$= \sum_{n\geq 0} (u(x))^{(p^n)} .$$

But unless n is a power of p, $u(x)^{(n)}$ is in $I^2 \cdot B = 0$ because of the explicit formulas in [5 Exposé 3 §3 Theorem 3].

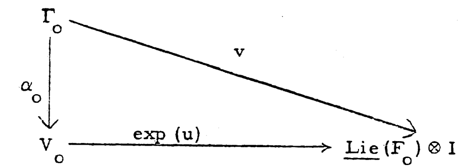
Thus $\sum_{n\geq 0} u(x)^{(p^n)} = \sum_{n\geq 1} u(x)^{(n)} = \exp(u)(x)$.

Thus we can state:

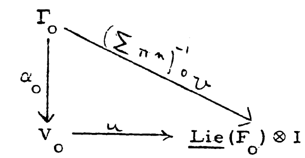
(2.6.6.3) $\quad (\sum \pi^n) \circ u = \exp(u)$.

In the above computation $\underline{\text{Lie}}(F) \otimes I$, $\underline{\text{Lie}}(F_o) \otimes I$, $I \cdot \underline{\text{Lie}}(F)$ have been systematically identified.

To complete the proof let us observe that because $\sum \pi^n$ is an isomorphism, the problem of finding a $u: V_o \longrightarrow \underline{\text{Lie}}(F_o) \otimes I$ such that the following diagram commutes:



is equivalent to the problem of finding a u which makes the following diagram commute:

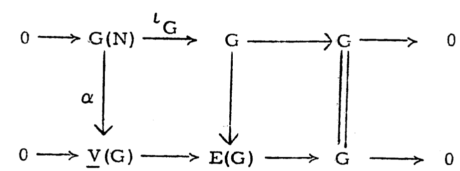


But by the universal property of α_o, there is a unique u making the diagram commute. This completes the proof of the lemma.

(2.7) Proof of Theorem (2.2):

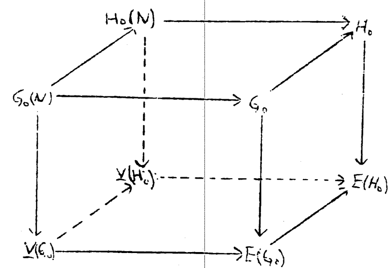
Consider the following diagram from which the universal extension $E(G)$ is obtained (and consider the corresponding diagram for H).

(2.7.1)



Let $v_o' = E(u_o)|G_o$ and $v_o'' = E(u_o)|\underline{V}(G_o) = i_o \circ \underline{V}(u_o)$.

(2.7.2)



Observe that (2.7.2) (above) is commutative. This is obvious except (possibly) for the face

$$\begin{array}{ccc} G_o & \xrightarrow{u_o} & H_o \\ \downarrow & & \downarrow \\ E(G_o) & \xrightarrow{E(u_o)} & E(H_o) \end{array}$$

But by a trivial diagram chase both ways of going around the diagram when composed with $G_o(N) \longrightarrow G_o$ give the same morphism, $G_o(N) \longrightarrow E(H_o)$. Of course, the analogous statement is true with $G_o(N)$ replaced by $G_o(n)$, $n \geq N$. Since $G_o = \varinjlim G_o(n)$, the desired commutativity follows.

To prolong $E(u_o)$ at all is equivalent to finding:

(2.7.3) $\quad v' : G \longrightarrow E(H)$, $v'' : \underline{V}(G) \longrightarrow E(H)$ satisfying

1) v' lifts v'_o, v'' lifts v''_o

2) $v' \circ \iota_G = v'' \circ \alpha$.

<u>Lemma</u> (2.7.4) Suppose there is a unique way to prolong v'_o to $v' : G \longrightarrow E(H)$. Then the problem of the theorem can be solved uniquely.

<u>Proof:</u> By the statement of the problem it is clear that the set of solutions is in one to one correspondence with the set of $v'' : \underline{V}(G) \longrightarrow E(H)$ such that:

1) v'' lifts v''_o

2) $v'' \circ \alpha = v' \circ \iota_G$

3) $d = i \circ w - v''$ is an exponential.

Consider the diagram:

$$\begin{array}{ccc} G(N) & \xrightarrow{v' \circ \iota_G} & \\ \alpha \downarrow & & \searrow \\ \underline{V}(G) & \xrightarrow{i \circ w} & E(H) \end{array}$$

Since v' lifts v'_o and w lifts $\underline{V}(u_o)$, the pullback of this diagram to S_o is commutative. Thus by (2.6.3) there is a unique v'' having the same restriction to S_o as $i \circ w$ (namely $i_o \circ \underline{V}(u_o)$), making the diagram commute ($v'' \circ \alpha = v' \circ \iota_G$), and differing from $i \circ w$ by an exponential. This completes the proof of the lemma.

Let $j : S_o \hookrightarrow S$ be the inclusion and let $M = \mathrm{Ker}[E(H) \longrightarrow j_*(E(H_o))]$. By (1.1 8) $E(H)$ is formally smooth and this implies that $E(H) \longrightarrow j_*(E(H_o))$ is an epimorphism. (In fact if T is an affine scheme over S, the map $\Gamma(T, E(H)) \longrightarrow \Gamma(T, j_*(E(H_o))) = \Gamma(T_o, E(H))$ is surjective.)

Consider the exact sequence

$$0 \longrightarrow M \longrightarrow E(H) \longrightarrow j_*(E(H_o)) \longrightarrow 0 .$$

The obstruction to lifting $v_o' : G_o \longrightarrow E(H_o)$ is an element of $\mathrm{Ext}^1(G, M)$.

Let us assume for the moment that this obstruction can be calculated by looking at the restrictions of G and M to the full sub-category consisting of schemes T over S which are flat.

Since M is clearly equal to the kernel of $\overline{E(H)} \longrightarrow j_*(\overline{E(H)}_o)$, and since $\overline{E(H)}$ is a formal Lie group, [III (2.2.5), (2.2.6)] can be applied to tell us that $\Gamma(S, M) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}_S}\left(\underline{\omega}_{\overline{E(H)}}, I\right)$.

More generally if T is flat over S, then since

$$\Gamma(T, M) = \Gamma(T, M_T) = \text{Kernel of } \Gamma\left(T, \overline{E(H_T)}\right) \longrightarrow \Gamma\left(T, j_{T_*}(\overline{E(H_T)}_o)\right)$$

we see $\Gamma(T, M) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}_T}\left(\underline{\omega}_{\overline{E(H_T)}}, I \cdot \mathcal{O}_T\right)$ since the divided powers on I extend. p^N kills S, and hence p^N kills the restriction of M to flat arguments.

Consider the exact sequence

$$0 \longrightarrow G(N) \longrightarrow G \xrightarrow{p^N} G \longrightarrow 0.$$

Applying $\mathrm{Ext}^*(-, M)$ to it there is an exact sequence

$$\mathrm{Ext}^1(G, M) \xrightarrow{p^N} \mathrm{Ext}^1(G, M) \longrightarrow \mathrm{Ext}^1(G(N), M).$$

Thus there is an injection $\mathrm{Ext}^1(G, M) \hookrightarrow \mathrm{Ext}^1(G(N), M)$.

Hence we are reduced to showing that the obstruction to lifting

$v_o' | G_o(N)$ to $G(N)$ is zero.

By its definition v_o' is the composite of $G_o \longrightarrow E(G_o)$ with $E(u_o)$. By looking at (2.7.2) it is obvious that if w is a lifting of $\underline{V}(u_o)$, then $i \circ w \circ \alpha$ is a lifting of $v_o' | G_o(N)$. But as has been noted several times $\underline{V}(G)$ is a projective module and hence such a lifting w certainly exists. This gives us the existence of v'.

The set of all such v' is principal homogeneous under the group $\mathrm{Hom}(G, M)$. But this group is zero because it can be written as $\varprojlim \mathrm{Hom}(G(n), M)$. If (φ_n) were an element of this inverse limit, then:

$$\text{(2.7.5)} \qquad \begin{array}{ccccc} G(n+N) & \xrightarrow{p^N} & G(n) & \hookrightarrow & G(n+N) \\ & & \downarrow \varphi_n & \swarrow \varphi_{n+N} & \\ & & M & & \end{array}$$

$\varphi_{n+N} \circ p^N \cdot \mathrm{id}_{G(n+N)} = 0$ since $G(n+N)$ is flat and $\varphi_{n+N} \in M(G(n+N))$ which is killed by p^N. Thus $\varphi_n \circ p^N = 0$ which implies $\varphi_n = 0$, since p^N is an epimorphism.

This tells us v' is unique and hence completes the proof of the theorem.

In the course of the proof the following lemma has been used.

Lemma (2.7.6): Let S_{Flat} denote the ordinary f.p.p.f. site of S and let S_{flat} denote the site which is the full sub-category of Sch/S consisting of those T over S which are flat (provided with the induced topology). For a sheaf F on S_{Flat} denote by F' its restriction to S_{flat}. Then, the map $G \longrightarrow i_* E(H_o)$ can be lifted to a map $G \longrightarrow E(H)$ if (and only if) the map $G' \longrightarrow (i_* E(H_o))'$ can be lifted to a map $G' \longrightarrow (E(H))'$.

Proof: Let $w : G' \longrightarrow (E(H))'$ be a lifting. Because $G(n)$ is flat, w is an element in $\varprojlim \Gamma(G(n), (E(H))') = \varprojlim \Gamma(G(n), E(H)) = \mathrm{Hom}_{\tilde{S}_{Flat}}(G, E(H))$.

Because the $G(n)$ are affine and $E(H)$ is a filtering direct limit of sub-group schemes, w , when viewed as a morphism $G \longrightarrow E(H)$, is a homomorphism of groups. Since the mapping $E(H) \longrightarrow i_*(E(H_o))$ induces the same mapping on $G(n)$-valued points as the mapping $(E(H))' \longrightarrow (i_*E(H_o))'$, w when viewed as a homomorphism $G \longrightarrow E(H)$ is a lifting of $G \longrightarrow i_*E(H_o)$

(2.8) Let us examine how the preceding results are to be modified so as to apply to abelian schemes. The only difference is that no restriction on the abelian scheme need be made. This follows from the following lemma.

Lemma (2.8.1) Let A be a ring, I an ideal of square zero in A and $A_o = A/I$. Let X_o be an abelian scheme on A_o. Then there is an abelian scheme X on A lifting X_o.

Proof: Let us write $A = \varinjlim A_\lambda$ where A_λ is a Noetherian subring of A. Then $A_o = \varinjlim A_\lambda / I \cap A_\lambda$. By [E.G.A. IV 8.8.3, 8.10.5 (xii), 9.7.7, 17.7.9] there is an abelian scheme $X_{o,\lambda}$ on $A_\lambda/I \cap A_\lambda$ (for some sufficiently large λ) which satisfies $X_{o,\lambda} \otimes_{A_\lambda/I \cap A_\lambda} A_o = X_o$. It is obvious that if we could lift $X_{o,\lambda}$ to A_λ, then there would be a lifting X of X_o to A. This allows us to assume A is Noetherian and hence Spec (A) is locally connected.

By [25, 2.2] the scheme X_o can be lifted to a smooth X over A. This scheme X is separated over A by [E.G.A. I 3.4.8, 5.3.4]. Thus

it is proper by [E.G.A. II 5.4.6]. Now following Mumford's argument in Geometric Invariant Theory (prop. 6.15) we construct a map $\mu : X \otimes_A X \longrightarrow X$ which lifts the subtraction map $\mu_o : X_o \otimes_{A_o} X_o \longrightarrow X_o$. It remains only to see that μ defines a group law on X. Again, following Mumford we want to apply the rigidity lemma to see that certain identities (i.e., associative law, ...) are satisfied.

Now we use the local connectedness of Spec (A). Namely consider for a connected open set $U \subseteq \mathrm{Spec}\,(A)$, $X|U$, $\mu|U, \ldots$. Applying the reasoning of [21, pg. 126], we see $X|U$ is an abelian scheme over U. Obviously this implies X is an abelian scheme.

(2.8.2) Thus as was mentioned above the arguments of §2 apply to abelian schemes exactly as they are stated. Hence we conclude that if p is locally-nilpotent on S_o and A is an abelian scheme on S_o, then crystals

$$\mathbb{E}(A),\quad \overline{\mathbb{E}}(A),\quad D(A) \text{ are defined.}$$