Lecture Notes in Mathematics

William Messing

The Crystals Associated to Barsotti-Tate Groups

264

With Applications to Abelian Schemes

Springer

Lecture Notes in Mathematics

A collection of informal reports and seminars
Edited by A. Dold, Heidelberg and B. Eckmann, Zürich

264

William Messing

Cranbury, NJ/USA

The Crystals Associated to Barsotti-Tate Groups: with Applications to Abelian Schemes

Springer-Verlag
Berlin · Heidelberg · New York 1972

AMS Subject Classifications (1970): 14K05, 14L05

ISBN 3-540-05840-0 Springer-Verlag Berlin · Heidelberg · New York
ISBN 0-387-05840-0 Springer-Verlag New York · Heidelberg · Berlin

Offsetdruck: Julius Beltz, Hemsbach/Bergstr.

Contents

INTRODUCTION

The concept of Barsotti-Tate group was introduced in [1] where the name equidimensional hyperdomain was used (actually for an equivalent concept) and in [30] where the name p-divisible group was used. Following Grothendieck, we prefer the term Barsotti-Tate group because the concept of "p-divisible group" has a meaning for any abelian group object in an arbitrary category and does not indicate any relation with algebraic geometry.

Barsotti-Tate groups arise in "nature" when one considers the sequence of kernels of multiplication by successive powers of p on an abelian variety. Also, as Grothendieck has observed, there are Barsotti-Tate groups which are naturally associated with the crystalline cohomology of a proper smooth scheme which is defined over a perfect field of characteristic p. Since we do not discuss crystalline cohomology no further mention is made of this example.

Returning to the situation where A is an abelian variety over a (perfect) field of characteristic p, let $A(n)$ denote the kernel of multiplication by p^n on A. The system $(A(n))_{n \geq 1}$ constitute a Barsotti-Tate group. As opposed to the situation where one looks at the kernel of multiplication by ℓ, $(\ell, p) = 1$, the groups $A(n)$ are never étale unless $A = (0)$. Each $A(n)$ can be written uniquely as a product of a connected group with an étale group. The sequence of these connected components yield, by passage to the limit, the formal group obtained by completing A along the identity. Thus the Barsotti-Tate group contains more information

than just this formal group. Another advantage which Barsotti-Tate groups possess over formal groups is that there is a duality (generalizing Cartier duality) defined for them.

In this paper Barsotti-Tate groups over an arbitrary base scheme S (on which p is locally nilpotent) are studied. Intuitively we can think of these as nicely varying families of Barsotti-Tate groups parametrized by S. The basic theorems are those which allow us to associate various crystals to such groups. Actually in order to construct these crystals we assume that the Barsotti-Tate groups in question are, locally, liftable to infinitesimal neighborhoods. This restriction is surely unnecessary. In fact, recent work of L. Illusie (modulo several verifications of compatabilities he has yet to make) shows that the obstruction to the existence of such liftings lie in a particular Ext group.* Combining this with a result of Grothendieck showing that the obstruction question is zero, we see it has "essentially" been proven that all Barsotti-Tate groups satisfy the above lifting hypothesis. Thus, for the rest of the introduction, assume all Barsotti-Tate groups are locally liftable in the above sense.

Let us now give a more detailed summary of the various chapters. For simplicity we restrict to the affine case: Let A be a ring, I a nilpotent ideal of A, $A_o = A/I$. Assume p is nilpotent in A. Set $S = \mathrm{Spec}\,(A)$, $S_o = \mathrm{Spec}\,(A_o)$ and generally denote with the subscript "o" the result of restricting an object defined over S to S_o.

In Chapter I the concept of a Barsotti-Tate group over S is defined, several sorites and several examples are given. This chapter consists

* These verifications have been made [17 bis].

primarily of definitions.

In Chapter II the relation between formal Lie groups and Barsotti-Tate groups is studied. First assuming A_o is of characteristic p, we show how to associate a formal Lie group to any Barsotti-Tate group G defined on S_o. Via the use of the relative cotangent complex this result is extended to a Barsotti-Tate group G over S (in the case where $I = pA$). The procedure employed is to actually reduce to the case already treated when the base is of characteristic p. Next we treat the question of when is a formal Lie group a Barsotti-Tate group. The results here are certainly partial and only the case when S is artin is explicitly dealt with. Finally necessary and sufficient conditions for a Barsotti-Tate group to be expressible as an extension of an ind-étale Barsotti-Tate group by a formal Lie group are given.

Chapter III is largely preliminary. The first and third sections recall the relevant definitions and properties of divided powers and crystals respectively. The second section treats the "exponential" which is used extensively later. In order to illustrate this concept assume the ideal I has nilpotent divided powers. Let $H = \mathrm{Spec}(B)$ be an affine commutative S-group such that $\underline{\mathrm{Lie}}(H)$ is locally-free of finite type. Denote by $\eta: B \longrightarrow A$ the augmentation corresponding to the unit section of H. The exponential will be a homomorphism:

$$\exp: \operatorname*{Hom}_{\mathcal{O}_S}(\mathbb{G}_a, I \otimes \underline{\mathrm{Lie}}(H)) \hookrightarrow \mathrm{Ker}\left[\operatorname*{Hom}_{S\text{-gr.}}(\mathbb{G}_{a_S}, H) \longrightarrow \operatorname*{Hom}_{S_o\text{-gr.}}(\mathbb{G}_{a_{S_o}}, H_o)\right].$$

For $\theta: \mathbb{G}_a \longrightarrow I \otimes \underline{\mathrm{Lie}}(H)$, let $\theta(1) = \sum i_j \otimes D_j$ where D_j is an A-linear

invariant derivation of B to itself. $\exp(\theta)$ is to be a homomorphism $\mathbb{G}_a \longrightarrow H$ and hence to describe it we give the corresponding algebra map $B \longrightarrow A[T]$. This algebra map is given explicitly via:

$$b \longmapsto \sum_{n \geq 0} \eta((\Sigma i_j D_j)^{(n)}(b))\, T^n.$$

This is an algebra map by Leibniz's rule, and is a bi-algebra map because the D_j's are invariant. Additivity in θ is checked directly and finally it is clear that $\exp(\theta)$: $\mathbb{G}_a \longrightarrow \mathrm{Ker}(H \longrightarrow H_o)$.

The exponential is studied in various contexts more general than the above. Unfortunately we have to resort to an ad hoc construction at one point and hence the discussion can not be regarded as truly satisfactory. Finally we utilize the exponential in order to define a notion of linear equivalence between certain vector subgroups of a given smooth group. This allows us to "linearize" the deformation theory of Chapter V.

Chapter IV is technically the heart of the work. It is here that we construct the crystals alluded to above. The first section constructs for any Barsotti-Tate group G on S a "universal" extension of G by a vector group:

$$(*) \qquad 0 \longrightarrow \underline{V}(G) \longrightarrow E(G) \longrightarrow G \longrightarrow 0$$

Here $\underline{V}(G) = \underline{\omega}_{C^*}$, the invariant differentials on the Cartier dual of G. This extension is universal in the sense that given any extension $0 \longrightarrow W \longrightarrow E \longrightarrow G \longrightarrow 0$ of G by a vector group W, there is a unique linear homomorphism $\underline{V}(G) \longrightarrow W$ which induces it from the extension (*).

The construction of the universal extension is functorial in G and commutes with all base changes.

Let us endeavor to explain how the crystals are obtained. For each G_o, a Barsotti-Tate group on S_o, crystals $\mathbb{E}(G_o)$, $\bar{\mathbb{E}}(G_o)$, $\mathbb{D}(G_o)$ are defined. The latter two are obtained from $\mathbb{E}(G_o)$ by "completing along the identity" or by taking the Lie algebra in the respective cases. Thus $\mathbb{E}(G_o)$ is the fundamental crystal to be constructed. The idea is to "crystallize" $E(G_o)$, the universal extension mentioned above. This means we want to show that if G_1 and G_2 are two liftings of G_o to S, then $E(G_1)$ and $E(G_2)$ are canonically isomorphic. The main theorem of Chapter IV proves this. The proof relies heavily on the exponential. Why is this? Well, we want an isomorphism $v: E(G_1) \xrightarrow{\sim} E(G_2)$ which reduces to $id_{E(G_o)}$. Let us consider the two extensions:

$$0 \longrightarrow \underline{V}(G_1) \xrightarrow{i_1} E(G_1) \longrightarrow G_1 \longrightarrow 0$$

$$0 \longrightarrow \underline{V}(G_2) \xrightarrow{i_2} E(G_2) \longrightarrow G_2 \longrightarrow 0$$

Let w be any lifting of $id_{V(G_o)}$ to a linear map $\underline{V}(G_1) \longrightarrow \underline{V}(G_2)$. If we could construct v and w such that $v \circ i_1 = i_2 \circ w$, then v would induce a homomorphism $G_1 \longrightarrow G_2$ reducing to id_{G_o}. It is easy to see that this would imply $G_1 \cong G_2$. But it is <u>definitely false</u> that G_1 is necessarily isomorphic to G_2. In fact if $A_o = \mathbb{Z}/p\mathbb{Z}$, $A = \mathbb{Z}/p^2\mathbb{Z}$, $G_o = \hat{\mathbb{G}}_m \times \mathbb{D}_p/\mathbb{Z}_p$, then there are (up to canonical isomorphism) precisely p distinct liftings of G_o to S. Thus the commutativity condition above

is too strong. Surely though we want $d = v \circ i_1 - i_2 \circ w$ to induce zero on S_o (since v is to lift $id_{E(G_o)}$ and w is to lift $id_{\underline{V}(G_o)}$). Thus d need not be zero but d_o should be zero; i.e., $d \in \mathrm{Ker}[\mathrm{Hom}(V(G_1), E(G_2)) \longrightarrow \mathrm{Hom}(\underline{V}(G_o), E(G_o))]$. It is precisely maps of this type which will be studied in Chapter III: the exponentials. Thus it is <u>natural</u> to ask if v can be chosen such that d is an exponential (it is easy to see the answer is independent of the w chosen to lift $id_{\underline{V}(G_o)}$). The answer is yes: there is a unique such v.

This enables us to construct the crystal $\mathbb{E}(G_o)$. Finally let us note that the developments of Chapter IV go through mutatis mutandis to the situation when the Barsotti-Tate groups are replaced by abelian schemes. This will be of crucial importance in Chapter V.

Chapter V treats the deformation theory of Barsotti-Tate groups and abelian schemes. We continue to assume the ideal I has nilpotent divided powers. We prove that to lift a Barsotti-Tate group G_o to S is equivalent to lifting the natural vector subgroup $\underline{V}(G_o) \hookrightarrow \underline{\mathrm{Lie}}(E(G_o)) = \mathbb{D}(G_o)_{S_o}$ to an "admissible" filtration $\mathrm{Fil}^1 \hookrightarrow \mathbb{D}(G_o)_S$. Actually a more precise result giving us information about lifting homomorphisms also, is proven. There is a completely analogous theorem concerning abelian schemes. In order to relate the deformation theory for abelian schemes with that for Barsotti-Tate groups we prove the following result: If A_o is an abelian scheme on S_o and $\bar{A}_o$ the corresponding Barsotti-Tate group, then there is a functorial isomorphism $\mathbb{D}(\bar{A}_o) \xrightarrow{\sim} \mathbb{D}(A_o)$.

Combining this result with the already stated results on deformations of abelian schemes and of Barsotti-Tate groups, it is quite easy to obtain the theorem of Serre-Tate, which says essentially: To lift A_o to S is equivalent to lifting $\bar{A}_o$ to S (and similarly for morphisms). (There are of course no assumptions concerning divided powers in this theorem.)

In the final section of the chapter we apply the above results to obtain the Serre-Tate canonical lifting of an ordinary abelian variety defined over a perfect field.

Results of the type obtained here have been previously announced in Cartier's Bourbaki talk [7] . He assumes the ring A_o is a perfect field of characteristic p and that the Barsotti-Tate groups in question are p-divisible formal Lie groups. Apparently he uses a more "Dieudonné module theoretic" approach. He obtains finer results about the structure of the crystal $\mathbb{D}(G)$ than those obtained here, in particular the result labeled 1) below.

In the appendix a characterization of the canonical lifting of an ordinary abelian variety is given. In the case of ordinary elliptic curves * the theorem of Serre-Tate is illustrated by giving Tate's elegant formulation of the result in terms of "q". This portion of the appendix is taken entirely from a letter of Tate to Dwork, dated November 1968.

Professor Serre has kindly informed me that for elliptic curves, the canonical lifting has a rather long history. Hasse used it in his first demonstration of the Riemann hypothesis for elliptic curves [16bis, 16ter]. Deuring in his fundamental paper [9bis] proved that for any elliptic curve E_o over a finite field and any endomorphism φ_o of E_o, there exists a "lifting" of the pair (E_o, φ_o) to characteristic zero. In our context the analogue is proposition (1.2) of the appendix. For the analytical aspects of the theory one should consult [9ter].

There are several results and problems which are not mentioned in the text. I shall limit myself to mentioning three such. The first two have been announced by Grothendieck while the third is, as far as I know, completely open.

1) If S_o is a perfect field of characteristic p, then $\mathbb{D}^*(G) = \mathbb{D}(G^*)$ is canonically isomorphic to the ordinary Dieudonné module of G.

2) If $\pi; A_o \longrightarrow S_o$ is an abelian scheme, then $\mathbb{D}(A_o^*)$ is canonically isomorphic to $R^1\pi_{*,\,crys}(\mathcal{O}_{A_o,\,crys})$.

3) Assuming S_o is of characteristic p and is perfect, to study more closely the functor $\mathbb{D}$. In particular to attempt to describe its essential image. Also to decide if this functor is fully-faithful.

As Grothendieck has observed his result 1) above renders "plausible" the belief that $\mathbb{D}$ is fully-faithful since $\mathbb{D}$ commutes with base change and is an equivalence of categories when the base is a perfect field.

During the summer of 1970 Grothendieck lectured in Montreal on "Barsotti-Tate groups and Dieudonné crystals". It was my good fortune to not only be able to attend these lectures, but also to have extensive personal contact with Grothendieck through which I was able to profit greatly.

Therefore, it is indeed my pleasure to thank A. Grothendieck for the time and effort he was so generously willing to devote to me as well as for his permission to use many of his unpublished results and ideas.

During the fall semester, 1970, N. Katz and I conducted a seminar at Princeton on Dieudonné theory and Barsotti-Tate groups. In the course of the seminar I presented most of the results which appear here. Throughout the entire seminar and even after it officially terminated Katz showed great patience and interest in discussing this work. This is especially true of the appendix where his assistance both in its initial conception and in the execution of several technical results was invaluable.

Conventions

1. "p" denotes a prime number fixed once and for all.

2. "group" always means commutative group.

3. "group over S, S-group, ... " will always mean a f.p.p.f. sheaf of (commutative) groups on the site $(Sch/S)_{f.p.p.f.}$. Groups which are representable will be referred to as such or via a modifying adjective (i.e., flat, finite, and locally-free, ...) which makes clear that they are group-schemes.

4. The references [8], [9], [12], [13] which are frequently cited in the text are referred to as:

   a) [8] G.A.

   b) [9] S.G.A.3

   c) [12] E.G.A.

   d) [13] S.G.A.

Following standard conventions E.G.A.IV denotes a particular reference in the 4^{th} chapter of E.G.A. Similarly S.G.A.$_{*}$ **, ... refers to a particular place in expose ** of the $*^{th}$ seminar held at Bures.

Chapter I. Definitions and Examples

§1. (1.0). Let S be a scheme and G a group on S (i.e., following the conventions introduced above, G is a commutative f.p.p.f. sheaf of groups on the site Sch/S) such that $p^n G = (0)$. Then we have the following lemma:

Lemma (1.1). The following conditions are equivalent

(i) G is a flat $\mathbb{Z}/p^n\mathbb{Z}$-module

(ii) $\mathrm{Ker}(p^{n-i}) = \mathrm{Im}(p^i)$ for $i = 0, \ldots, n$

Proof: First we show (i) implies (ii). From (i) it follows that $gr^\cdot(\mathbb{Z}/p^n\mathbb{Z}) \otimes_{\mathbb{Z}/p\mathbb{Z}} gr^0(G) \cong gr^\cdot(G)$ (the associated graded group being taken with respect to the filtration defined by powers of p). Because of this we know that p^i induces an isomorphism from G/pG to $p^iG/p^{i+1}G$ for $i \leq n-1$. Thus $\mathrm{Ker}(p^{n-1}) \subseteq \mathrm{Im}(p)$ and hence $\mathrm{Ker}(p^{n-i}) \subseteq \mathrm{Ker}(p^{n-1}) \subseteq \mathrm{Im}(p)$ which implies that $\mathrm{Ker}(p^{n-i}) = p \cdot \mathrm{Ker}(p^{n-i+1}) = p(p^{i-1}G) = p^iG$ (by induction on i).

To prove that (ii) $\Rightarrow$ (i), we observe by taking i=1 that $pG = \mathrm{Ker}(p^{n-1})$ and hence that p^{n-1} induces an isomorphism $G/pG \xrightarrow{\sim} p^{n-1}G$. Since this map factors as $G/pG \longrightarrow pG/p^2G \longrightarrow \cdots \longrightarrow p^{n-1}G$ we see that each of these maps is an isomorphism. Thus, since

$$gr^0(\mathbb{Z}/p^n\mathbb{Z}) \otimes_{\mathbb{Z}/p\mathbb{Z}} gr^0(G) \xrightarrow{\sim} gr^0(G),$$

we have $$gr^\cdot(\mathbb{Z}/p^n\mathbb{Z}) \otimes_{\mathbb{Z}/p\mathbb{Z}} gr^0(G) \xrightarrow{\sim} gr^\cdot(G).$$

To complete the proof we want to utilize a version of the "criterion of flatness."

By [16;II §4] to prove the flatness of G it suffices to show

$\mathrm{Tor}_1^{\mathbb{Z}/p^n\mathbb{Z}}(M, G) = 0$ for any $\mathbb{Z}/p^n\mathbb{Z}$-module M. But the reasoning of [4; Chap. III §5 #3 remark 1 and prop. 1] is completely formal and hence applies in the general context. Consider the exact sequence:

$$M \otimes \mathrm{Tor}_1^{\mathbb{Z}/p^n\mathbb{Z}}(\mathbb{Z}/p, G) \longrightarrow \mathrm{Tor}_1^{\mathbb{Z}/p^n\mathbb{Z}}(M, G) \longrightarrow \mathrm{Tor}_1^{\mathbb{Z}/p\mathbb{Z}}(M, G/pG) \longrightarrow 0$$

which arises from the terms of low degree in the spectral sequence for "associativity" of Tor.

$\mathrm{Tor}_1^{\mathbb{Z}/p^n\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, G) = 0$ by hypothesis (as noted above). $\mathrm{Tor}_1^{\mathbb{Z}/p\mathbb{Z}}(M, G/pG) = 0$ since $\mathbb{Z}/p\mathbb{Z}$ is a field. This shows that $\mathrm{Tor}_1^{\mathbb{Z}/p^n\mathbb{Z}}(M, G)$ is zero for any $\mathbb{Z}/p\mathbb{Z}$-module M and thus completes the proof.

Definition (1.2) If $n \geq 2$, a truncated Barsotti-Tate group of level n is an S-group G such that:

1) G is a finite locally-free group scheme

2) G is killed by p^n and satisfies the equivalent conditions of lemma (1.1).

Remark (1.3) For completeness let us define a truncated Barsotti-Tate group of level 1 (on a scheme S where p is locally nilpotent) as a group G which satisfies:

1) G is finite and locally free and killed by p.

2) Denoting by S_o the closed subscheme $\mathrm{Var}(p.1_S)$ of S and $G_o = G \times_S S_o$, $\mathrm{im}\, v_{G_o} = \mathrm{Ker}\, f_{G_o}$, $\mathrm{im}\, f_{G_o} = \mathrm{Ker}\, v_{G_o}$ (see [II 3.3.11, 3.3.12]).

Notation (1.4) If G is a group, we will write $G(n)$ for the kernel of p^n. If G is killed by p^n, we write $G = G(n)$.

Lemma (1.5) a) If $G(n)$ is a flat $\mathbb{Z}/p^n\mathbb{Z}$-module then $G(n)$ is a finite locally-free group scheme if and only if $G(1)$ is and then all the $G(i)$ are.

b) If $G(n)$ is finite and locally free then $p^i: G(n) \longrightarrow G(n-i)$ is an epimorphism if and only if it is faithfully flat.

Proof: We prove b) first. Clearly if $p^i: G(n) \longrightarrow G(n-i)$ is faithfully flat it is an epimorphism. Conversely if it is an epimorphism, then by using the criterion for checking flatness fiber by fiber [E.G.A.IV 11.3.11] we are reduced to the case when S is the spectrum of a field and here the result is standard. [G.A. III, §3, 7.4]

To prove a) we observe that if $G(n)$ is flat over $\mathbb{Z}/p^n\mathbb{Z}$ and $G(1)$ is finite and locally free, then we have exact sequences:

$0 \longrightarrow G(1) \longrightarrow G(2) \xrightarrow{p} G(1) \longrightarrow 0$

$0 \longrightarrow G(1) \longrightarrow G(3) \xrightarrow{p} G(2) \longrightarrow 0, \ldots$. Therefore by induction we see that all the $G(i)$ are finite locally-free (since an extension of two such groups is another one by descent theory [G.A. III §4, 1.9]). Conversely, if $G(n)$ is finite and locally-free, then each $G(i)$ is certainly finite of finite presentation over S [E.G.A. II 6.15. (iii) and (v) for "finite," E.G.A. IV 1.6.2. (iii) and (v) for "of finite presentation"]. From part b) (proved above) we know each $G(i)$ is flat over S. Hence each $G(i)$ is finite and locally-free.

§2. (2.0) Let S be a scheme and G a group on S. Denote by $G(n)$ the kernel of multiplication by p^n on G. G is said to be of p-torsion if $\varinjlim G(n) = G$. G is said to be p-divisible if $p \cdot id_G: G \longrightarrow G$ is an

epimorphism.

Definition (2.1): G is a Barsotti-Tate group if it satisfies the following three conditions:

(2.1.1) G is of p-torsion

(2.1.2) G is p-divisible

(2.1.3) G(1) is a finite, locally-free group scheme

Notation (2.2): We write B.T.(S) for the category of Barsotti-Tate groups on S, whose objects are the Barsotti-Tate groups and whose morphisms are simply homomorphisms of S-groups.

Remarks (2.3): Let G be a Barsotti-Tate group

1) $G(n) = G(n+1)(n)$

2) For any i such that $0 \leq i \leq n$, p^{n-i} induces an epimorphism $G(n) \longrightarrow G(i)$ (because multiplication by p^{n-i} is an epimorphism of G).

3) From remarks 1) and 2) and the fact that G(1) is finite and locally-free it follows from 1.5 that the G(n) for $n \geq 2$ are truncated Barsotti-Tate groups and that we have exact sequences:

(2.3.1) $$0 \longrightarrow G(n-i) \longrightarrow G(n) \xrightarrow{p^{n-i}} G(i) \longrightarrow 0$$

4) It follows from the elementary theory of finite group schemes over a field that the rank of the fiber of G(1) at a point $s \in S$ is of the form $p^{h(s)}$ where h is a locally constant function on S. It also follows from remark 3) that the rank of the fiber of G(n) at s is $p^{nh(s)}$ [G.A. IV §3, 5].

5) Assume we have a system of groups G(n) with G(n) finite and locally-free such that:

a) $G(n) = G(n+1)(n)$

b) The rank of the fiber of $G(n)$ at s is $p^{nh(s)}$ where h is a locally constant function on S.

We consider the exact sequence

$$0 \longrightarrow G(n-i) \longrightarrow G(n) \xrightarrow{p^{n-i}} G(i) .$$

By looking at each fiber and using the multiplicativity of the ranks, $G(n)_s \xrightarrow{p^{n-i}} G(i)_s$ is faithfully flat. Therefore since $G(n)$ is flat over S, it follows

that $G(n) \xrightarrow{p^{n-i}} G(i)$ is faithfully flat

and hence an epimorphism. Thus we see that $G = \varinjlim G(n)$ is a Barsotti-Tate group and therefore (using also remarks 1) and 4)) it follows that our definition of Barsotti-Tate group is equivalent to that of Tate [30].

6) From remark 5) it follows that our definition of Barsotti-Tate group is essentially independent of the fact that we choose to work with f.p.p.f. sheaves. Nevertheless it will be quite convenient to view the category B.T.(S) as a full sub-category of the category of abelian sheaves (for the f.p.p.f. topology) on S.

Sorites (2.4)

(2.4.1) If $S' \xrightarrow{f} S$ is a morphism and G is in B.T.(S), then $f^*(G)$ is in B.T.(S').

That $f^*(G)$ is of p-torsion and p-divisible follows immediately from the fact that f^* is exact as does the formula $f^*(G)(n) = f^*(G(n))$. But since $f^*(G(1)) = G(1) \underset{S}{\times} S'$, it is immediate that $f^*(G)(1)$ is finite and

locally-free and hence $f^*(G)$ is in B.T.(S').

Remark (2.4.2): The assignment $S \longmapsto$ B.T.(S) gives a fibered category over the category of schemes. It is in fact a stack when (Schemes) is endowed with the f.p.q.c. topology. This follows easily from the definitions and descent theory [11, I 3.2].

(2.4.3) If $0 \longrightarrow G_1 \longrightarrow G_2 \longrightarrow G_3 \longrightarrow 0$ is exact and

a) G_1 and G_2 are in B.T.(S)

b) G_1 and G_3 are in B.T.(S),

then in either case the third group is in B.T.(S) also.

Proof: In both cases it follows from the serpent lemma that the sequence $0 \longrightarrow G_1(1) \longrightarrow G_2(1) \longrightarrow G_3(1) \longrightarrow 0$ is exact. The representability of $G_3(1)$ (in case a)) is given by [G.A. III, §2 3.2] while the representability of $G_2(1)$ (in case b)) is given by [G.A. III, §4, 1.9] which also tells us $G_2(1)$ is finite and locally-free. The fact that $G_3(1)$ is finite and locally-free (in case a)) is somewhat more involved. By [E.G.A. II 5.4.3(i), E.G.A. IV 1.6.2(v)] $G_1(1) \hookrightarrow G_2(1)$ is a proper monomorphism of finite presentation and hence it is a closed immersion [E.G.A. IV 8.11.5]. By [S.G.A. 3 VI B 9.2 (x), (xi), (xii), (xiii)] $G_3(1)$ is separated, flat, quasi-finite and of finite presentation over S. That $G_3(1)$ is finite and locally-free now follows from [E.G.A. II, 5.4.3 (i), IV 8.11.1, 1.4.7].

In either case a) or b) it is immediate that the relevant group is of p-torsion and p-divisible and thus a Barsotti-Tate group.

(2.4.4) By considering the exact sequences (2.3.1) we see that the family of Cartier duals $G(n)^*$ together with the maps $p^*: G(n)^* \longrightarrow G(n+1)^*$

(coming from the exact sequences) give us a Barsotti-Tate group G^*, the Cartier dual of G, with $G^*(n) = G(n)^*$. The assignment $G \longmapsto G^*$ extends to morphisms so that we obtain a duality on the category of Barsotti-Tate groups. Just as with ordinary Cartier duality, this duality is compatible with all base changes.

Remark (2.4.5). The category B.T.(S) is not abelian. Kernels do not exist in this category since the kernel of the morphism $G \xrightarrow{p} G$ must be killed by p and hence can not be a Barsotti-Tate group (unless G = 0).

§3. (3.0) We give in this paragraph several examples of Barsotti-Tate groups. First though, we recall some terminology about finite, locally-free group schemes, G, on an arbitrary base S.

(3.1) G is said to be of multiplicative type if the following three equivalent conditions hold:

(3.1.1) Locally on S for the étale topology, G is isomorphic to a group of the form Spec $(\mathcal{O}_S[M])$ where M is an ordinary finite abelian group.

(3.1.2) G^*, the Cartier dual of G, is étale.

(3.1.3) Locally, for the Zariski topology, there is a monomorphism $G \longrightarrow T$ where T is a torus (i.e., a group which locally for the étale topology is isomorphic to $\mathbb{G}_m^\ell$).

That (3.1.1) implies (3.1.2) is obvious. The reverse implication is an immediate consequence of [S.G.A. 3 X 4.5, 4.8]. To see that (3.1.1) implies (3.1.3) we can, since the question is local on S, assume S to be

affine and then by the standard arguments assume S to be Noetherian [E.G.A. IV 8.9.1, 8.5.5, 8.10.5(x), 17.7.8(ii)]. We decompose S into a disjoint union of open sub-schemes S_λ, such that for all s belonging to a given S_λ, $G_{\overline{s}}$, the geometric fiber, is isomorphic to $\mathrm{Spec}(\overline{k(s)}[M_\lambda])$ for a well-defined finite group M_λ. Replacing S by S_λ and then by a connected component of S_λ (which is open since S is locally noetherian) we reduce to the case where S is connected. Then by [S.G.A3 X 7.2] we see that to give G is equivalent to giving a finite π-module M where π is the "enlarged" fundamental group corresponding to the choice of some geometric point of S. But now writing M as a quotient of $\mathbb{Z}[M]$ when π operates on $\mathbb{Z}[M]$ in the obvious way, we see that the group corresponding to the abelian group $\mathbb{Z}[M]$ is a torus and hence we achieve the desired embedding.

Finally to prove that (3.1.3) implies (3.1.2) it suffices to check the implication when S is the spectrum of a field. But now as G is a finite closed sub-group of a torus, the implication follows immediately from [G.A. IV §1 2.4(a)].

(3.2) G is said to be <u>infinitesimal</u> if the structural morphism $G \longrightarrow S$ is radiciel. This is of course a condition which is verified fiber by fiber. We shall see in [II 4.4], that this use of the word "infinitesimal" is consistent with a later meaning we shall give it in connection with formal Lie groups.

(3.3) Recall finally the following definition.

Definition (3.3.1) An abelian scheme $A \xrightarrow{f} S$ is a commutative group scheme such that:

1) f is proper

2) f is smooth

3) f has geometrically connected fibers.

Example (3.4). If A/S is an abelian scheme then $\varinjlim A(n)$ is a Barsotti-Tate group of rank $2d$ where d is the relative dimension of A/S and hence a locally constant function on S. Since the group $\varinjlim A(n)$ is obviously of p-torsion, we must show it is p-divisible and $A(1)$ is finite and locally-free of rank p^{2d}. To know it is p-divisible it obviously suffices to check that $p: A \longrightarrow A$ is an epimorphism. Thus it suffices to know $p: A \longrightarrow A$ is faithfully flat and hence we are by [E.G.A IV 11.3.11] reduced to the case when we are over an algebraically closed field. But as is well known, multiplication by p on an abelian variety is surjective, and hence by the lemma of generic flatness [21; 6.12] we are done. Finally, since $A(1)$ has zero-dimensional and hence finite fibers and since $A(1) \longrightarrow S$ is proper (being obtained by the base change $S \longrightarrow A$ from the map $p: A \longrightarrow A$ which is proper by [E.G.A. II 5.4.3(i)]), it follows that $A(1) \longrightarrow S$ is finite [E.G.A. IV 8.11.1]. Since $A(1) \longrightarrow S$ is flat, finite and of finite presentation it is finite and locally free [E.G.A. IV 1.4.7]. Finally the statement about the rank follows immediately from [22; §6]. Later we shall have much more to say about Barsotti-Tate groups of this type which we denote by $\overline{A}$ or $A(\infty)$.

Example (3.5) Let T be a torus on S and consider $\varinjlim T(n) \overset{\text{def.}}{=\!=} T(\infty)$. Then $T(\infty)$ is a Barsotti-Tate group of rank d when d is the relative dimension of T/S. That $T(\infty)$ is of p-torsion is obvious. To see that $T(\infty)$ is p-divisible and $T(1)$ is finite and locally-free of rank d, we are by descent reduced to the case where $T \cong \mathbb{G}_m^d$ where both are completely trivial.

Example (3.6) We assume in this example that p is locally nilpotent on S. Also, this example will be treated in more detail later. Let G be a formal Lie group on S. We will verify in [II 4.2], that G is automatically of p-torsion. Assume that multiplication by p is an epimorphism of G and that $G(1)$ is finite and locally-free. This last condition follows from the hypothesis that $G \xrightarrow{p} G$ is an epimorphism when the base S is artin. These assumptions imply that G is a Barsotti-Tate group with $G(1)$ and hence all $G(n)$ infinitesimal. As we shall verify in detail later [II, 4.5] we have an equivalence of categories between the category of Barsotti-Tate groups on S with $G(1)$ infinitesimal and that of formal Lie groups G such that $G \xrightarrow{p} G$ is an epimorphism and $G(1)$ is finite and locally-free.

Example (3.7) Let G be a Barsotti-Tate group on S such that $G(1)$, and hence all $G(n)$, is étale. We call such a group ind-étale. Associated to G is the projective system $T_p(G)$: $G(1) \xleftarrow{p} G(2) \xleftarrow{p} G(3) \longleftarrow \dots$. By the very definition of the phrase, $T_p(G)$ is a "faisceau p-adique constant tordu sans torsion." [S.G.A. 5 VI 1.2] It is immediately checked that any homomorphism between $T_p(G)$ and $T_p(H)$ must come from a

homomorphism from G to H. Thus it is essentially a tautology that the category of Barsotti-Tate groups on S which are ind-étale is equivalent (via the functor $G \longmapsto T_p(G)$) to the category of "faisceaux p-adique constant tordu sans torsion." If S is connected and $\bar{s}$ is a geometric point of S, this last category is equivalent to that of continuous representations of $\pi_1(S, \bar{s})$ in finite free $\mathbb{Z}_p$-modules.

Example (3.8) A Barsotti-Tate group G on S is said to be toroidal if G(1) is of multiplicative type. Of course this implies that all G(n) are of multiplicative type. From 3.1 we know that G^*, the Cartier dual will be ind-étale and hence that the functor: $G \longmapsto T_p(G^*)$ induces an anti-equivalence between the category of toroidal Barsotti-Tate groups on S and that of "faisceaux p-adiques constant tordu sans torsion." To obtain a covariant equivalence between these two categories, let us first introduce the following notation.

$$(3.8.1) \qquad \mu \overset{\text{def.}}{=\!=} G_m(\infty) = \varinjlim \mu_{p^n} .$$

Consider the functor on toroidal groups defined by

$$G \longmapsto \underline{\mathrm{Hom}}_{S\text{-gr}}(\mu, G) \overset{\text{def.}}{=\!=}$$

the inverse system $(\underline{\mathrm{Hom}}_{S\text{-gr}}(\mu_{p^n}, G(n))_{n\geq 1}$. But this last inverse system is identified via Cartier duality with the inverse system

$$(\underline{\mathrm{Hom}}_{S\text{-gr}}(G(n)^*, \mathbb{Z}/p^n\mathbb{Z}))_{n\geq 1} = T_p(G^*)^\vee$$

[see S.G.A. 3 X 5.8].

Example (3.9) Assume S to be artin and let G be a Barsotti-Tate group on S. Then for each n, we have an extension: $0 \longrightarrow G(n)^{\circ} \longrightarrow G(n) \longrightarrow G(n)^{\text{ét}} \longrightarrow 0$ where $G(n)^{\circ}$ is the disjoint union of the connected components of the various fibers of $G(n)$. By reducing to the case when we are over a field we easily see that the various sequences:

$$0 \longrightarrow G(n-i)^{\circ} \longrightarrow G(n)^{\circ} \xrightarrow{p^{n-i}} G(i)^{\circ} \longrightarrow 0$$

$$0 \longrightarrow G(n-i)^{\text{ét}} \longrightarrow G(n)^{\text{ét}} \xrightarrow{p^{n-i}} G(i)^{\text{ét}} \longrightarrow 0$$

are exact [see S.G.A. 3 VIA 5.5]. Thus in passing to the limit we have an extension $0 \longrightarrow G^{\circ} \longrightarrow G \longrightarrow G^{\text{ét}} \longrightarrow 0$ with G° having connected fibers (and hence, if p is nilpotent on S, a formal Lie group) and $G^{\text{ét}}$ ind-étale. Applying Cartier duality to G°, taking the étale quotient of $G^{\circ *}$ and applying Cartier duality again we have a filtration:

$$\{e\} \subseteq G^{t} \subseteq G^{\circ} \subseteq G$$

with G^{t}, toroidal. As shall be seen later such representations of G as an extension of an ind-étale by a group with connected fibers do not in general exist.

Chapter II. The Relation Between Barsotti-Tate and Formal Lie Groups

§1. (1.0). Let S be a scheme, and X and Y with $Y \hookrightarrow X$ two sheaves on S for the f.p.p.f. topology. We make the following definition.

Definition (1.01): $\mathrm{Inf}_Y^k(X)$ is the subsheaf of X whose sections over an S-scheme T are given as follows: $\Gamma(T, \mathrm{Inf}_Y^k(X)) = \{t \in \Gamma(T, X) \mid$ there is a covering $\{T_i \longrightarrow T\}$ and for each T_i a closed subscheme T_i' defined by an ideal whose $k+1^{st}$ power is (0) with the property that $t_{T_i'} \in \Gamma(T_i', X)$ is actually an element of $\Gamma(T_i', Y)\}$.

Thus for each integer $k \geq 0$ we have defined the k^{th} infinitesimal neighborhood of Y in X. We first observe the following simple lemma.

Lemma (1.02) If X and Y are schemes and $Y \hookrightarrow X$ is an immersion, then the above definition coincides with the usual one of [E.G.A. IV §16].

Proof: Let us denote by $Y^{(k)}$ the k^{th} infinitesimal neighborhood of Y in X in the sense of E.G.A. We can obviously assume that Y is a closed subscheme of X defined by a quasi-coherent ideal $I \subseteq \mathcal{O}_X$. Thus $\mathcal{O}_{Y(k)} = \mathcal{O}_X/I^{k+1}$ and we certainly have a monomorphism $Y^{(k)} \longrightarrow \mathrm{Inf}_Y^k(X)$. To show this is an isomorphism we must show that for any affine scheme T (over S) the map $\Gamma(T, Y^{(k)}) \longrightarrow \Gamma(T, \mathrm{Inf}_Y^k(X))$ is surjective. Thus we are reduced to showing that if $T = \mathrm{Spec}\,(A)$, $T' = \mathrm{Spec}\,(A')$ with $A \longrightarrow A'$ faithfully flat, $J \subseteq A'$ is an ideal with $J^{k+1} = (0)$, and $\varphi: T \longrightarrow X$ is such that the composite $\mathrm{Spec}\,(A'/J) \hookrightarrow T' \longrightarrow T \xrightarrow{\varphi} X$ factors through Y,

then φ factors through $Y^{(k)}$. Let ψ denote the morphism $A \longrightarrow A'$ corresponding to $T' \longrightarrow T$. Then the hypothesis tells us that $I \cdot A \subseteq \psi^{-1}(J)$. But $A \longrightarrow A'$ being faithfully flat implies that it is injective, and hence $\psi^{-1}(J)$ has its $k+1^{st}$ power equal to (0). But this certainly implies that $\varphi: T \longrightarrow X$ factors through $Y^{(k)}$.

Lemma (1.03) (Compatability of the formation of infinitesimal neighborhoods with base change.) If $S' \longrightarrow S$ is a morphism then $\mathrm{Inf}^k_{Y_{S'}}(X_{S'}) = (\mathrm{Inf}^k_Y(X))_{S'}$.

Proof: Let $T' \longrightarrow S'$ be given and let $t' \in \Gamma(T', \mathrm{Inf}^k_{Y_{S'}}(X_{S'}))$. Then by definition there is a covering family $\{T'_i \longrightarrow T'\}$ and nilpotent immersions of order k $T'_{i_o} \hookrightarrow T'_i$ such that $t'_{T'_{i_o}} \in \Gamma(T'_{i_o}, Y_{S'})$. But considering T', T'_i, T'_{i_o} as S-schemes via $S' \longrightarrow S$ we see that this this t' belongs to $\Gamma(T', (\mathrm{Inf}^k_Y(X))_{S'})$. Conversely, if we begin with a t' in this last set and hence have T'_i, T'_{i_o} S-schemes as in the definition then T'_i can obviously be viewed as an S'-scheme in such a way that $\Gamma(T'_i, X_{S'}) = \Gamma(T'_i, X)$. Thus such a t' must belong to $\Gamma(T', (\mathrm{Inf}^k_{Y_{S'}}(X_{S'}))$ which completes the proof.

(1.1) Let X be a sheaf on S and $e_X: S \longrightarrow X$ be a section. If it is understood that X is given together with a section, then we will write $\mathrm{Inf}^k(X)$ rather than $\mathrm{Inf}^k_S(X)$, the latter having been defined in (1.01) via our section $e_X: S \hookrightarrow X$.

Definition (1.1.1) A pointed sheaf (X, e_X) as above is ind-infinitesimal if $X = \varinjlim \mathrm{Inf}^k(X)$.

Remark (1.1.2) It follows immediately from the definition that $\mathrm{Inf}^k(X) = \mathrm{Inf}^k(\mathrm{Inf}^{k+i}(X))$ for any $i \geq 0$.

Recall (1.1.3) Let X be an S-scheme and $e_X : S \longrightarrow X$ a section, then if $\underline{\omega}_{e_X}$ denotes the conormal sheaf of the immersion $e_X : S \hookrightarrow X$, we have $\underline{\omega}_{e_X} \tilde{=} e_X^* (\Omega^1_{X/S})$. This is seen by checking that both $\mathcal{O}_S$-modules represent the same functor: namely $\mathcal{F} \longmapsto \mathrm{Der}_S(\mathcal{O}_X, e_{X*}(\mathcal{F}))$ or else as in [G.A.I §4, 2.2]. Also recall that associated to such an immersion we have a graded quasi-coherent sheaf of $\mathcal{O}_S$-algebras [E.G.A.IV 16.1.5].

The following basic definition can now be made.

Definition (1.1.4) A pointed sheaf (X, e_X) on S is said to be a formal Lie variety if the following conditions are satisfied:

1) X is ind-infinitesimal and $\mathrm{Inf}^k(X)$ is representable for all $k \geq 0$.

2) $\underline{\omega}_X = e_X^* (\Omega^1_{\mathrm{Inf}'(X)/S} = e_X^* (\Omega^1_{\mathrm{Inf}^k(X)/S})$

is locally free of finite type.

3) Denoting by $\mathrm{gr}^{\mathrm{inf}}(X)$ the unique graded $\mathcal{O}_S$-algebra, such that $\mathrm{gr}_i^{\mathrm{inf}}(X) = \mathrm{gr}_i(\mathrm{Inf}^i(X))$ holds for all $i \geq 0$ (see remark 1.1.3), we have an isomorphism $\mathrm{Sym}(\underline{\omega}_X) \xrightarrow{\sim} \mathrm{gr}^{\mathrm{inf}}(X)$ induced by the canonical mapping $\underline{\omega}_X \xrightarrow{\sim} \mathrm{gr}_1^{\mathrm{inf}}(X)$.

We proceed to translate this definition into more down to earth terms. First condition 1) and remark (1.1.2) tell us that for each k $\mathrm{Inf}^k(X)$ is an affine S-scheme and that both S and $\mathrm{Inf}^k(X)$ have the same underlying

topological space. Thus $\mathrm{Inf}^k(X)$ is given by a quasi-coherent $\mathcal{O}_S$-algebra $\mathcal{A}_k$ which is augmented:

$$0 \longrightarrow I_k \longrightarrow \mathcal{A}_k \longrightarrow \mathcal{O}_S \longrightarrow 0$$

and furthermore $I_k^{k+1} = (0)$. We are also told that $\mathcal{A}_{k+1}/I_{k+1}^{k+1} \cong \mathcal{A}_k$, which makes obvious how we define the algebra $\mathrm{gr}^{\mathrm{inf}}(X)$. Conditions 2) and 3) imply that locally on S we have

$$\mathcal{A}_k \xleftarrow{\sim} \mathcal{O}_S[T_1, \ldots, T_N]/(T_1, \ldots, T_N)^{k+1},$$

these isomorphisms being compatible [4; Chap. III, §2, #8 Cor. 3]. Hence locally on S, X is given by a power series ring $\mathcal{O}_S[[T_1, \ldots, T_N]]$ in the sense that for an S-scheme S', $\Gamma(S', X) \tilde{=} \underbrace{\mathrm{Nil}(\mathcal{O}_{S'}) \times \cdots \times \mathrm{Nil}(\mathcal{O}_{S'})}_{N \text{ factors}}$

where $\mathrm{Nil}(\mathcal{O}_{S'})$ denotes the locally nilpotent sections of $\mathcal{O}_{S'}$. These correspond exactly to the continuous homomorphisms

$$\mathcal{O}_S[[T_1, \ldots, T_N]] \longrightarrow \Gamma(S', \mathcal{O}_{S'})$$

when the latter is given the discrete topology.

Definition (1.1.5) A formal Lie group over S, (e_G, G) is a group in the category of formal Lie varieties.

As usual we consider only commutative formal Lie groups and this will be always implicitly assumed in the following without further mention.

Lemma (1.1.6) Let G be a group on a scheme S. Then $\overline{G} = \varinjlim \mathrm{Inf}^k(G)$ is also a group.

Proof: Since $\overline{G}$ is closed under taking inverses it suffices to show it is closed under addition. Since $\overline{G}$ is a sheaf it suffices to check that if $f, g \in \Gamma(T, \mathrm{Inf}^k(G))$ then there is a $k' \geq k$ such that $f+g \in \Gamma(T, \mathrm{Inf}^{k'}(G))$. But since f belongs to $\Gamma(T, \mathrm{Inf}^k(G))$ there is a covering family $\{T_i \longrightarrow T\}$ and nilpotent immersions of order k, $\overline{T}_i \hookrightarrow T_i$ such that $f|\overline{T}_i = 0$. Similarly there is a covering family $\{T'_j \longrightarrow T\}$ and nilpotent immersions of order k $\overline{T}'_j \hookrightarrow T'_j$ corresponding to g. But $\{T_i \underset{T}{\times} T'_j \longrightarrow T\}$ is a covering family, $\overline{T}_i \underset{T}{\times} \overline{T}'_j \longrightarrow T_i \underset{T}{\times} T'_j$ is a nilpotent immersion of order $2k$ and obviously $f + g|\overline{T}_i \underset{T}{\times} \overline{T}'_j = 0$. Thus $\overline{G}$ is indeed a group.

§2. (2.0) In this paragraph we assume that S is of characteristic p and then associate to any G in B.T.(S) a subgroup $\overline{G}$ which is a formal Lie group. Later we will, by reducing to the case when S is of characteristic p, be able to extend this result to the case where p is locally nilpotent on S.

(2.1) Recall that if G is a flat S-group scheme there are defined two homomorphisms:

$$f_G : G \longrightarrow G^{(p)}$$

$$v_G : G^{(p)} \longrightarrow G$$

satisfying $v_G \circ f_G = p\,\mathrm{id}_G$ and $f_G \circ v_G = p\,\mathrm{id}_{G^{(p)}}$.

Here $G^{(p)} = G \underset{S}{\times} S$ when S is viewed as an S-scheme via the absolute Frobenius $F : S \longrightarrow S$. For the definition of v_G see [G.A. IV §3, 4] or [S.G.A. 3 VII A 4.2]. Note that the definition of f_G has nothing to do with G being either representable or a group but applies to any

contravariant functor from Sch/S to Sets.

Notation (2.1.1) G[n] will denote the kernel of the n^{th} iterate of the Frobenius homomorphism:

$$G \xrightarrow{f_G} G^{(p)} \xrightarrow{f_{G^{(p)}}} G^{(p^n)} \cdots \longrightarrow G^{(p^n)}$$

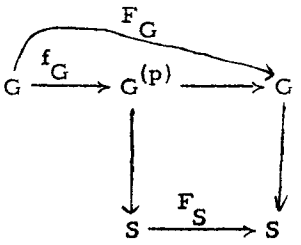
Proposition (2.1.2) Assume G is a finite, locally-free S-group such that G = G[n]. Then the following conditions are equivalent:

1) For all $i=0,\ldots,n$ $f_G^i : G \longrightarrow G[n-i]^{(p^i)}$ is flat.

2) For all $i=0,\ldots,n$ $f_G^i : G \longrightarrow G[n-i]^{(p^i)}$ is an epimorphism of f.p.p.f. sheaves of groups.

3) Locally on S we have an isomorphism of pointed S-schemes $G \tilde{=} \mathrm{Spec}\,(\mathcal{O}_S[T_1,\ldots,T_N]/(T_1^{p^n},\ldots,T_N^{p^n}))$.

Proof: Since we have the following diagram



in which the square is cartesian it follows that f_G is certainly bijective on the topological space level. Thus 1) implies that each f_G^i is in fact faithfully flat. Since it is also certainly locally of finite presentation by [E.G.A. IV 1.4.3(v)] it is covering for the f.p.p.f. topology and hence an epimorphism of groups. Conversely if we assume 2) then we can check

that f_G^i is flat by looking fiber by fiber, since to be faithfully flat or an epimorphism for groups over a field is equivalent by [G.A.III §3, 7.4]. 3) implies 2) because being an epimorphism is a local condition and f_G on G then corresponds to the map $\mathcal{O}_S \underset{\mathcal{O}_S}{\otimes} \mathcal{O}_S[T_1, \ldots, T_N]/(T^{p^n}) \longrightarrow$ $\mathcal{O}_S[T_1, \ldots, T_N]/(T^{p^n})$ given by $T_i \longrightarrow T_i^p$. Hence f_G is obviously an epimorphism. Finally it remains to see that 1) or 2) implies 3). First, if S = Spec (k) where k is a perfect field, then we can write G = Spec $k[T_1, \ldots, T_N]/(T_1^{p^{n_1}}, \ldots, T_N^{p^{n_N}})$ with $0 < n_i \leq n$ by [G.A.III §3 6.3]. But if n_1 (say) is strictly less than n and if we consider the ring homomorphism corresponding to f_G^{n-1} we will have $1 \otimes T_1 \longmapsto T_1^{p^{n-1}}$ which is zero in $k[T_1, \ldots, T_N]/(T_1^{p^{n_1}}, \ldots, T_N^{p^{n_N}})$. But this violates the hypothesis that $f_G^{n-1} : G \longrightarrow G[1]^{(p^{n-1})}$ is faithfully flat since the corresponding ring mapping would then be injective.

To prove the general implication we proceed to reduce to the special case just treated.

Since G is by hypothesis finite over S we can certainly assume G = Spec (B) where B is some S = Spec (A) augmented algebra of finite rank. Furthermore, if $\underline{p} \subseteq A$ is any prime ideal, any isomorphism of augmented algebras $B_{\underline{p}} \xrightarrow{\sim} A_{\underline{p}}[T_1, \ldots, T_N]/(T_1^{p^n}, \ldots, T_N^{p^n})$ will certainly extend to a neighborhood of $\underline{p}$. Hence we can assume S = Spec (A) where A is a local ring.

Let us consider $\underline{\omega}_G$ and then look at $\underline{\omega}_G \underset{A}{\otimes} k$ where k is the residue

field. This is a finite dimensional vector space over k and hence we can find elements $t_1, \ldots, t_N$ in I, the augmentation ideal of B, which generate $\underline{\omega}_G \otimes_A k$. Let us then define a map

$$A[T_1, \ldots, T_N] \Big/ (T_1^{p^n}, \ldots, T_N^{p^n}) \longrightarrow B$$

via $T_i \longmapsto t_i$. Note the hypothesis that $G = G[n]$ insures that $t_i^{p^n} = 0$ and hence the mapping is defined. By Nakayama the elements $t_1, \ldots, t_N$ have residue classes which generate I/I^2 and since I is finitely generated (being a direct summand of the A-module B) it is nilpotent because the $p^{n^{th}}$ power of any element in it is zero. Thus $t_1, \ldots, t_N$ in fact generate I and hence the above mapping is surjective. Thus to conclude that the mapping is an isomorphism it suffices to observe that both source and target are free finitely-generated A-modules and that $\operatorname{rank}_A(B) = \operatorname{rank}_k(B \otimes_A k) = \operatorname{rank}_{\bar{k}}(B \otimes_A \bar{k}) = p^{nN} = \operatorname{rank}_A(A[T_1, \ldots, T_N] \Big/ (T_1^{p^n}, \ldots, T_N^{p^n}))$.

Remark (2.1.3) It follows from the proof that the conditions of the proposition are equivalent to the conditions

(1 bis) $\quad G \xrightarrow{f^{n-1}} G[1]^{(p^{n-1})}$ is flat.

(2 bis) $\quad G \xrightarrow{f^{n-1}} G[1]^{(p^{n-1})}$ is an epimorphism.

Remark (2.1.4) It is immediate from condition 3) of the proposition that $\underline{\omega}_G$ is locally free of finite type.

Corollary (2.1.5) The hypotheses being as in (2.1.2) and S being affine, the three conditions of the proposition are equivalent to

4) $\underline{\omega}_G$ is locally free of finite type and G is isomorphic as pointed

scheme to Spec $(\mathrm{Sym}_{\mathcal{O}_S}[\underline{\omega}_G]/\underline{\omega}_G^{(p^n)})$, $\underline{\omega}_G^{(p^n)}$ denoting the ideal generated by the $p^{n\text{th}}$ powers of sections of $\underline{\omega}_G$.

Proof: That 4) implies the conditions of the proposition is obvious. Conversely if $G = \mathrm{Spec}(B)$ where B is a finite quasi-coherent $\mathcal{O}_S$-algebra, then the conditions of the proposition imply that $\underline{\omega}_G = I/I^2$ is locally free where I is the augmentation ideal of B. Thus we can choose an A-linear section of the morphism $I \longrightarrow \underline{\omega}_G$ (A being the ring of S). This defines a morphism $\mathrm{Sym}_A(\underline{\omega}_G) \longrightarrow B$ which factors through the algebra $\mathrm{Sym}_A(\underline{\omega}_G)/\underline{\omega}_G^{(p^n)}$. From the proof of the proposition it follows immediately that localizing the above homomorphism at any prime ideal $\underline{p}$ of A we obtain an isomorphism. Thus the constructed mapping is an isomorphism.

Using the corollary we can prove the theorem (2.1.7) below which gives an alternative definition of a formal Lie group when S is of characteristic p.

Definition (2.1.6) A sheaf of groups G on S is said to be of f-torsion if $G = \varinjlim G[n]$.

Definition (2.1.7) A sheaf of groups G on S is said to be f-divisible if $f_G : G \longrightarrow G^{(p)}$ is an epimorphism.

Theorem (2.1.7): In order that the sheaf of groups G on S be a formal Lie group it is necessary and sufficient that the following three conditions hold:

1) G is of f-torsion.

2) G is f-divisible.

3) The G[n] are finite and locally free S-group schemes.

Proof: The proof is essentially that of proposition 1 in Tate's paper [30]. From the fact that, locally on S, a formal Lie group is given by a power series ring, the necessity follows immediately. Since the definition of a formal Lie group is clearly local on S we can assume S is affine, say S = Spec (A). Then conditions 2) and 3) imply (via proposition (2.1.2) and its corollary (2.1.5)) that $G[n] = \mathrm{Spec}\,(B_n)$ when B_n is a finite locally-free A-algebra. From the fact that G[1] is the kernel of $f_{G[n]}: G[n] \longrightarrow G[n]^{(p)}$, we deduce from the cartesian diagram

$$\begin{array}{ccc} G[n] & \xrightarrow{f} & G[n]^{(p)} \\ \uparrow & & \uparrow \\ G[1] & \longrightarrow & S \end{array}$$

that $B_n/I_n^{(p)} \xrightarrow{\sim} B_1$ where I_n is the augmentation ideal of B_n and $I_n^{(p)}$ is the ideal generated by the p^{th} powers of elements in I_n. But this certainly implies that the natural map $I_n/I_n^2 \longrightarrow I_1/I_1^2$ is an isomorphism. By taking S to be smaller we can assume $\omega_{G[1]}$ to be free of finite rank. But now it is obvious that we can choose isomorphisms $\mathrm{Sym}(\omega_{G[1]})/\omega_{G[1]}^{(p^n)} \xrightarrow{\sim} B_n$ in a compatible way (via corollary (2.15) this simply amounts to choosing inductively liftings of generators of I_n to I_{n+1}). Passing to the inverse limit we find that $B = \varprojlim B_n$ is isomorphic to a power series ring. Hence, for any A-algebra C, the points of G with values in Spec(C) are the elements of $\varinjlim \mathrm{Hom}\,(B_n, C) = \mathrm{Nil}(C) \times \cdots \times \mathrm{Nil}(C)$ and hence G is a formal Lie variety and therefore a formal Lie group.

Theorem (2.1.8) Let G be a Barsotti-Tate group over S; then $\varinjlim G[n]$ is a formal Lie group and is equal to $\overline{G} \overset{\text{def.}}{=\!=} \varinjlim \mathrm{Inf}^k(G)$.

Proof: By theorem (2.17) it suffices to show $\varinjlim G[n]$ is of f-torsion, f-divisible and that the $G[n]$ are finite and locally free. By its very definition it is obvious that $\varinjlim G[n]$ is of f-torsion. Since by hypothesis $p: G^{(p)} \longrightarrow G^{(p)}$ is an epimorphism and since we have a factorization of this morphism $G^{(p)} \xrightarrow{v} G \xrightarrow{f} G^{(p)}$ it follows that $f: G \longrightarrow G^{(p)}$ is an epimorphism. But now it is clear that $f^{-1}[(\varinjlim G[n])^p]$ is contained in $\varinjlim G[n]$ and hence that $f: \varinjlim G[n] \longrightarrow (\varinjlim G[n])^{(p)}$ is an epimorphism. Thus it remains to show that the $G[n]$ are finite and locally free. Since we have the exact sequences

$$0 \longrightarrow G[i] \longrightarrow G[n] \xrightarrow{f^{n-i}} G[n-i]^{(p^{n-i})} \longrightarrow 0$$

we are reduced to showing that $G[1]$ is finite and locally free. Notice first that because $p = v_G \circ f_G$ we have $G[1] \subseteq G(1)$ and thus $G[1] = G(1)[1]$ is certainly representable. Using the usual references [E.G.A.II 6.1.5(v), E.G.A.IV 1.6.2(v), 1.6.3, 1.4.7] we see that the morphism $G(1) \xrightarrow{f} G(1)^{(p)}$ is finite and of finite presentation and hence it is the same for the morphism $G[1] \longrightarrow S$. Thus to show $G[1]$ is finite and locally free it remains to show it is flat over S. But $v_{G(1)}: G(1)^{(p)} \longrightarrow G[1]$ since $f \circ v = p$, and we must have $v_G^{-1}(G[1]) \subseteq G(1)^{(p)}$ for the same reason. But just like f, v_G is also an epimorphism, and hence the morphism $v_G^{-1}(G[1]) \longrightarrow G[1]$ induced by v is an epimorphism. Thus we have an exact sequence:

$$0 \longrightarrow \mathrm{Ker}\, v \longrightarrow G(1)^{(p)} \xrightarrow{v} G[1] \longrightarrow 0 \ .$$

Passing to the fibers we see that for all $s \in S$, v_s is faithfully flat and hence as $G(1)^{(p)}$ is flat over S, it follows that $v: G(1)^{(p)} \longrightarrow G[1]$ is faithfully flat [E.G.A. IV 11.3.11]. This of course implies that $G[1]$ is flat over S and hence we have shown that $\varinjlim G[n]$ is a formal Lie group. To prove the last statement of the theorem we observe that $G' = \varinjlim G[n]$ is ind-infinitesimal since this was part of the definition of a formal Lie group. On the other hand for any $n \geq 0$ we have $\mathrm{Inf}^{p^n-1}(G) \subseteq G[n]$. To see this we observe that for any T over S, $f_G: \Gamma(T, G_1) \longrightarrow \Gamma(T, G^{(p)})$ is simply the mapping arising because G is a contravariant functor from the commutative diagram:

$$\begin{array}{ccc} T & \xrightarrow{F_T} & T \\ \downarrow & & \downarrow \\ S & \xrightarrow{F_S} & S \end{array}$$

Finally we observe that if $T' \hookrightarrow T$ is a nilpotent immersion of order $< p^n$, then we have a commutative diagram:

$$\begin{array}{ccc} T & \xrightarrow{F_T^n} & T \\ & \searrow \quad \nearrow & \\ & T' & \end{array}$$

Thus we have $G' = \overline{G'} = \varinjlim \mathrm{Inf}^k(G') \subseteq \varinjlim \mathrm{Inf}^k(G) \subseteq G'$ which completes the proof.

§3. (3.0) In this section we show that if p is locally nilpotent on S and G is in B.T.(S), then $\overline{G} = \varinjlim \mathrm{Inf}^k(G)$ is a formal Lie group. In order

to do this we make a detailed study of the $G(n)$ making use of the relative cotangent complex $L_{\cdot}^{G(n)/S}$.

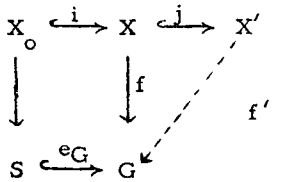
(3.1) We begin by studying smoothness properties of pointed schemes. For the next proposition no hypothesis on the base, S, is necessary.

Proposition (3.1.1) Let (G, e_G) be a pointed scheme, locally of finite presentation on S; that is e_G is a section of the structural morphism $G \longrightarrow S$. Then the following two conditions are equivalent:

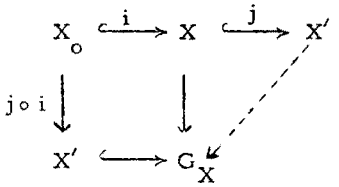
1) Locally (for the Zariski topology) on S, $\mathrm{Inf}_e^k(G)$ is isomorphic to a pointed scheme of the form $\mathrm{Spec}\,(\mathcal{O}_S[T_1, \ldots, T_n]/(T_1, \ldots, T_n)^{k+1})$; i.e., $\underline{\omega}_G = e_G^*(\Omega^1_{G/S})$ is locally free of finite type, and $\mathrm{Sym}^i(\underline{\omega}_G) \xrightarrow{\sim} \mathrm{gr}^i(G, e_G)$ for $i \leq k$. Here the term gr^i has the obvious meaning coming from [E.G.A. IV §16].

2) For any affine scheme X_o over S, an S-infinitesimal neighborhood X' of X_o of order k, a sub-scheme X of X' containing X_o and any S-morphism $f: X \longrightarrow G$ such that $f|X_o$ factors through $S \xrightarrow{e_G} G$, there is a prolongation of f to an $f': X' \longrightarrow G$.

Before giving the proof we exhibit the diagram which (hopefully) makes condition 2) clearer:



Proof: We first show that 1) implies 2). Thus consider the data given to us in the above diagram. We can form the new diagram



Here $X \longrightarrow G_{X'}$ is the morphism (f, j) and $X' \hookrightarrow G_{X'}$ is $e_G \times 1_{X'}$.

It is immediately checked that the left-hand square commutes and and that if we find an X'-morphism to make the diagram commute $g: X' \longrightarrow G_{X'}$, then composing g with the projection $G_{X'} \longrightarrow G$ we find an S-morphism which solves our original problem. Since hypothesis 1) for $G \longrightarrow S$ evidently implies the analogous statement for $G_{X'} \longrightarrow X'$ we have reduced ourselves to the following situation: $X' = S$ and hence S is affine. Notice also that the morphism $f: X \longrightarrow G$ factors through the k^{th} infinitesimal neighborhood of S in G. Thus translating into commutative algebra we have: rings A', A A_o with $A = A'/J$, $A_o = A'/J_o$, $J_o \supseteq J$, $J_o^{k+1} = (0)$, and an A' algebra B and a map of A'-algebras $f: B \longrightarrow A$. Furthermore B is an augmented A'-algebra. Let its augmentation ideal be I. Then under the composite map $B \longrightarrow A \longrightarrow A_o$, I is mapped to (0). Hence under the map $f: B \longrightarrow A$, $f(I) \subseteq J_o/J$. By hypothesis 1) $B = \mathrm{Sym}_{A'}[\underline{\omega}_G]/I^{k+1}$ and hence we have an A'-linear map $\underline{\omega}_G \longrightarrow J_o/J$. Since $\underline{\omega}_G$ is projective, we can lift this to a map $\underline{\omega}_G \longrightarrow J_o$. This allows us to define a map $\mathrm{Sym}_{A'}[\underline{\omega}_G] \longrightarrow A'$ which takes I into J_o. Hence

this map takes I^{k+1} into $J_o^{k+1} = (0)$ and thus we obtain a map $f': B \longrightarrow A'$ which lifts $f: B \longrightarrow A$.

We now turn to the proof that 2) implies 1). Observe that only $\mathrm{Inf}^k(G)$ enters into condition 2) since the given map f certainly factors through $\mathrm{Inf}^k(G)$ and any prolongation to an f' must also factor through $\mathrm{Inf}^k(G)$. To prove that 2) implies 1) we can assume S is affine and hence $\mathrm{Inf}^k(G)$ is also affine. Let the respective rings be A and B where B is an augmented A-algebra whose augmentation ideal I is such that $I^{k+1} = (0)$. In order to show that I/I^2 is locally-free, we are led to the case $k=1$ since condition 2) implies that B/I^2 satisfies the same hypotheses for first order immersions, as B does for k^{th} order immersions. Let us choose, in the notation of condition 2), $X_o = S = \mathrm{Spec}\,(A)$. For any two A-modules M and M' and any surjective homomorphism $M \longrightarrow M'$ we can look at the two rings $D_A(M)$ and $D_A(M')$ (i.e., the ring $D_A(M) = A \oplus M$ with $M^2 = (0), \ldots$). Then we find surjective homomorphisms:

$$D_A(M) \longrightarrow D_A(M') \longrightarrow A$$

But now by definition $B = D_A[\underline{\omega}_G]$ and condition 2) now says that any A-linear map $\underline{\omega}_G \longrightarrow M'$ can be lifted to a map $\underline{\omega}_G \longrightarrow M$. This says that $\underline{\omega}_G$ is projective. But G being locally of finite presentation on S implies that $\underline{\omega}_G$ is of finite presentation [E.G.A. IV 16.4.22] and hence that $\underline{\omega}_G$ is locally-free of finite rank.

It remains to prove that $\mathrm{Sym}^i[\underline{\omega}_G] \xrightarrow{\sim} \mathrm{gr}^i(G, e)$ for $i \leq k$. In order to do this let $B' = \mathrm{Sym}\,[\underline{\omega}_G]/I'^{k+1}$ where I' is the augmentation ideal in

$\mathrm{Sym}[\underline{\omega}_G]$. Consider the map $I \longrightarrow \underline{\omega}_G$, and because $\underline{\omega}_G$ is projective choose a section $\underline{\omega}_G \longrightarrow I$. This section allows us to define a map $u: B' \longrightarrow B$ because $I^{k+1} = (0)$. We will show that this map is an isomorphism, which will complete the proof that 2) implies 1). Let us apply hypothesis 2) to $X' = \mathrm{Spec}\,(B')$, $X = \mathrm{Spec}\,(B)$ and $X_o = \mathrm{Spec}\,(A)$. Notice that $u: B' \longrightarrow B$ is surjective modulo squares of the augmentation ideals and hence is surjective. Then by 2) the identity morphism $B \longrightarrow B$ can be lifted to a homomorphism of A-algebras $v: B \longrightarrow B'$ such that $u \circ v = 1_B$. But now from the case $k=1$, we know $v \circ u$ induces the identity on I'/I'^2. Hence $v \circ u$ induces the identity on $gr_{I'}(B')$. Thus as I' is nilpotent, $v \circ u$ is an automorphism of B' and hence u is an isomorphism.

Definition (3.1.2) G is said to be smooth along the section e_G up to order k if G satisfies the equivalent conditions of proposition (3.1.1).

(3.2) In this section we define the "naive" relative cotangent complex in the special context in which we shall need it. The word "naive" is used to distinguish the complex which we define, from that defined in general by Illusie [17], although in this special case his definition agrees with the one which we will adopt.

(3.2.1) Let G be a finite and locally-free S group scheme (no hypothesis on S is necessary). Thus $G = \mathrm{Spec}\,(\mathcal{A})$ where $\mathcal{A}$ is a finite and locally-free $\mathcal{O}_S$-algebra. To say G is a group amounts to saying $\mathcal{A}$ is a bi-algebra (i.e., we have algebra homomorphisms $\Delta: \mathcal{A} \longrightarrow \mathcal{A} \otimes \mathcal{A}$ and $\epsilon: \mathcal{A} \longrightarrow \mathcal{O}_S$ satisfying well known identities). Thus $\check{\mathcal{A}}$, the linear dual of $\mathcal{A}$, is

equipped with an algebra structure via the transpose of Δ and that of ϵ.

Definition (3.2.2) The situation being as in (3.2.1) the hyperalgebra, $U(G)$, of G is by definition $\mathcal{A}$ endowed with its algebra structure.

Remark (3.2.3) As is well known $\mathcal{A}$ is in fact a bi-algebra and Spec $(\check{\mathcal{A}}) = G^*$, the Cartier dual of G.

(3.2.4) Since $U(G)$ is a finite locally free $\mathcal{O}_S$-algebra we obtain a smooth group scheme $U(G)^X$ whose points with values in the S scheme T are by definition the invertible elements in the ring $\Gamma(T, U(G_T)) = \Gamma\left(T, \check{\mathcal{A}} \otimes_{\mathcal{O}_S} \mathcal{O}_T\right)$. Also we have a natural monomorphism $G \hookrightarrow U(G)^X$ which is defined by viewing a T-valued point of G as a homomorphism of $\mathcal{O}_T$-algebras $\mathcal{A} \otimes_{\mathcal{O}_S} \mathcal{O}_T \longrightarrow \mathcal{O}_T$ and hence as a global section of $\Gamma\left(T, \check{\mathcal{A}} \otimes_{\mathcal{O}_S} \mathcal{O}_T\right)$. The fact that such a homomorphism when viewed as an element of $\Gamma(T, U(G_T))$ is invertible and that the morphism $G \hookrightarrow U(G)^X$ thus defined is indeed a homomorphism of group schemes, results easily from the definitions.

Lemma (3.2.5) The natural monomorphism $G \hookrightarrow U(G)^X$ is a closed immersion.

Proof: Observe $U(G)^X$ is of finite presentation and affine over S. Then by applying [S.G.A. 3 XVI (1.8)] with $G' = S$ (the trivial S-group) and $G'' = G$ and $H = U(G)^X$ we see that $G \longrightarrow U(G)^X$ is proper. Since it is also a monomorphism we use [E.G.A. IV 8.11.5] to finish.

Lemma (3.2.6) The morphism $G \hookrightarrow U(G)^X$ is a regular immersion.

Proof: By [S.G.A. 3 III 4.15], G is locally a complete intersection. Hence by [S.G.A. 6 VII 1.2, 1.4], we see $G \longrightarrow U(G)^X$ is a regular immersion.

(3.2.7) The notation being as above, let I be the ideal defining G in $U(G)^X$; then the definition of S.G.A. 6 for $L.^{G/S}$ which we adopt is:

Definition (3.2.8) The relative cotangent complex, $L.^{G/S}$, is the complex of $\mathcal{O}_G$-modules $I/I^2 \longrightarrow \Omega^1_{U(G)^X/S}\Big|G$.

Since both terms in this complex are locally-free we have $Le^*_G(L.^{G/S}) = e^*_G(L.^{G/S})$. Let $\pi: G \longrightarrow S$ be the structural morphism. We have the following proposition (which we will need later):

Proposition (3.2.9) $\pi^* e^*_G(L.^{G/S}) \xrightarrow{\sim} L.^{G/S}$.

To prove the proposition we use the following general lemma:

Lemma (3.2.10) Let T be a topos, G be a group of T and P a torseur under G. Assume we are given a fibered category $\mathcal{C}$ over T. Then the category of objects ξ in $\mathcal{C}_P$ given with descent data is equivalent to the category of objects ξ in $\mathcal{C}_P$ on which G acts in a manner compatible with its action on P. The last condition means precisely the following: for any object S' in T and $\varphi \in G(S')$ we are to be given a morphism $\bar{\varphi}: \xi_{P_{S'}} \longrightarrow \xi_{P_{S'}}$ lying over the mapping multiplication by φ on $P_{S'}$ in such a way that it is compatible with multiplication in G and with restriction morphisms.

Proof: Let data of the above type be given for an object $\xi \in \mathcal{C}_P$. First

observe that an equivalent way of stating the condition is to say that for any S' in T and any morphism $\eta: S' \longrightarrow P$ we are to be given an isomorphism $\eta^*(\xi) \xrightarrow{\sim} (\varphi \cdot \eta)^*(\xi)$. The fact that this map must be an isomorphism follows from the requirement that G "acts as a group." Applying this to $S' = P \times P$ and $\eta = p_1$ we choose $\varphi \in \mathrm{Hom}(P \times P, G)$ to be the unique element such that $\varphi \cdot p_1 = p_2$. Thus we obtain an isomorphism $\theta: p_1^*(\xi) \xrightarrow{\sim} p_2^*(\xi)$. To check the cocycle condition we observe by the above restriction and multiplicativity properties that since $p_{12}^*(\varphi) \cdot p_1' = p_2'$, $p_{23}^*(\varphi) \cdot p_2' = p_3'$, $p_{13}^*(\varphi) \cdot p_1' = p_3'$ (where $p_i': P \times P \times P \longrightarrow P$ is the i^{th} projection), we must have $p_{23}^*(\theta) \circ p_{12}^*(\theta) = p_{13}^*(\theta)$ by the multiplicativity property. Now to check that morphisms between such objects give rise to morphisms between objects with descent data is trivial. Since this is all we actually need for the proposition we omit the easy verification that we indeed have an equivalence of categories.

Proof of proposition (3.2.9) (continued): Take $G = P =$ our finite locally-free group scheme G, $T = \widetilde{Sch/S}$ with the Zariski topology (for example) on Sch/S. Take $\mathcal{E}$ = fibered category of modules. Observe now that if we consider $G \hookrightarrow U(G)^X$, then sections of G induce commutative diagrams via translation:

$$\begin{array}{ccc} G & \hookrightarrow & U(G)^X \\ \downarrow & & \downarrow \\ G & \hookrightarrow & U(G)^X \end{array}$$

Therefore by functoriality they induce an action of the above type (i.e., as

in the lemma) on the conormal bundle I/I^2 and on $\Omega^1_{U(G)^X/S}\big|G$. These translations are obviously compatible with the morphism $I/I^2 \longrightarrow \Omega^1_{U(G)^X/S}\big|G$ [E.G.A. IV 16.2 and 16.4]. Hence as $G \longrightarrow S$ has a section it is a morphism of effective descent and thus we can write:

$$L_\cdot^{G/S} \xrightarrow{\sim} \pi^* e_G^*(I/I^2) \xrightarrow{\pi^*(v)} \pi^* e_G^* \left(\Omega^1_{U(G)^X/S}\big|G\right)$$

for a unique morphism $v: e_G^*(I/I^2) \longrightarrow e_G^*\left(\Omega^1_{U(G)^X/S}\big|G\right)$. But as $\pi^* e_G^* \pi^*(v) = \pi^*(v)$ we must have $v = e_G^* \pi^*(v)$ and hence $L_\cdot^{G/S} \xrightarrow{\sim} \pi^* e_G^*(L_\cdot^{G/S})$.

Lemma (3.2.11) The formation of $L_\cdot^{G/S}$ commutes with an arbitrary base change $S' \longrightarrow S$.

Proof: Since the formation of $U(G)^X$ obviously commutes with all base changes we must only show that the ideal defining $G_{S'}$ in $U(G)^X \underset{S}{\times} S'$ is the inverse image of the ideal defining G in $U(G)^X$. Since this problem is local on S', we can assume $S' = \mathrm{Spec}\,(A')$, $S = \mathrm{Spec}\,(A)$, $U(G)^X = \mathrm{Spec}\,(B)$, $G = \mathrm{Spec}\,(B/I)$. But since B/I is flat over A the following sequence is exact: $0 \longrightarrow I \underset{A}{\otimes} A' \longrightarrow B \underset{A}{\otimes} A' \longrightarrow B/I \underset{A}{\otimes} A' \longrightarrow 0$. Hence $I \underset{A}{\otimes} A'$ is identified with its image in $B \underset{A}{\otimes} A'$ which is precisely what we wanted to show.

Recall (3.2.12) The construction of $U(G)$ being functorial in G it follows that if $u: G \longrightarrow H$ is a homomorphism of finite locally-free groups we have a commutative diagram:

$$\begin{array}{ccc} G & \hookrightarrow & U(G)^X \\ {\scriptstyle u}\downarrow & & \downarrow \\ H & \hookrightarrow & U(H)^X \end{array}$$

and hence deduce that there is a morphism $u^*(L_\cdot^{H/S}) \longrightarrow L_\cdot^{G/S}$ corresponding to u.

Definition (3.2.13) The co-Lie complex, $\ell_\cdot^G$ is by definition $e_G^*(L_\cdot^{G/S})$. From (3.2.12) we see that $G \longrightarrow \ell_\cdot^G$ is a contravariant functor.

(3.3) The following propositions give us the necessary results in order to associate a formal Lie group to a Barsotti-Tate group.

Proposition (3.3.1) Let G(n) be an inductive system of finite locally-free groups on an arbitrary scheme S. (The n is just an index which for typographical is not written as a subscript .) Let J be a quasi-coherent ideal of $\mathcal{O}_S$ such that $J^N = (0)$. Let $S_o = \mathrm{Var}(J)$, $G_o(n) = G(n) \times_S S_o$ and in general let the subscript "o" denote the restriction to S_o. Assume we are given a mapping φ: $\mathbb{N} \longrightarrow \mathbb{N}$ such that $\varphi(n) \geq n$ for all n. Assume that whenever M is a quasi-coherent module on an affine open set $U_o \subseteq S_o$, $\mathrm{Ext}^1_{\mathcal{O}_{U_o}}(\ell_\cdot^{G_o(n)}|U_o, M) \longrightarrow \mathrm{Ext}^1(\ell_\cdot^{G_o(\varphi(n)}|U_o, M)$ is the zero map. (In the rest of the proposition we shall omit the $\mathcal{O}_{U_o}$ and $|U_o$ and simply write S_o, or S depending on the context. This will not lead to any confusion.) Let X′ be an affine scheme over S and X be the subscheme defined by an ideal I such that $I^2 = (0)$. Assume we are given an S-morphism f: $X \longrightarrow G(n)$. Then there is an S-morphism f′: $X' \longrightarrow G(\varphi^N(n))$ such that the following diagram commutes:

$$\begin{array}{ccc} X & \hookrightarrow & X' \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f'} \\ G(n) & \longrightarrow & G(\varphi^N(n)) \end{array}$$

Proof: Let $U \subseteq S$ be any affine open set and let M be a quasi-coherent module on U which is killed by J so that M is in a natural way an $\mathcal{O}_{U_o}$-module. By hypothesis the map $\mathrm{Ext}^1(\ell.^{G_o(n)}, M) \longrightarrow \mathrm{Ext}^1(\ell.^{G_o(\varphi(n))}, M)$ is zero. But now since $U_o \hookrightarrow U$ is a closed immersion (and hence an affine morphism) it follows immediately from [S.G.A.4 XVII 4.1.3(iii), 16; I 6.4] that $\mathrm{Ext}^1(\ell.^{G_o(n)}, M)$ is isomorphic to $\mathrm{Ext}^1(\ell.^{G(n)}, M)$. Thus the map $\mathrm{Ext}^1(\ell.^{G(n)}, M) \longrightarrow \mathrm{Ext}^1(\ell.^{G(\varphi(n))}, M)$ is also the zero map.

By induction on the integer j we have M(q. coherent on U) killed by J^j implies $\mathrm{Ext}^1(\ell.^{G(n)}, M) \longrightarrow \mathrm{Ext}^1(\ell.^{G(\varphi^j(n))}, M)$ is the zero map. In fact writing the exact sequence

$$0 \longrightarrow JM \longrightarrow M \longrightarrow M/JM \longrightarrow 0$$

and forming the commutative diagram:

$$\begin{array}{ccccc}
\mathrm{Ext}^1(\ell.^{G(n)}, JM) & \longrightarrow & \mathrm{Ext}^1(\ell.^{G(n)}, M) & \longrightarrow & \mathrm{Ext}^1(\ell.^{G(n)}, M/JM) \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{Ext}^1(\ell.^{G(\varphi(n))}, JM) & \longrightarrow & \mathrm{Ext}^1(\ell.^{G(\varphi(n))}, M) & \longrightarrow & \mathrm{Ext}^1(\ell.^{G(\varphi(n))}, M/JM)
\end{array}$$

we see that the image of $\mathrm{Ext}^1(\ell.^{G(n)}, M)$ is contained in that of $\mathrm{Ext}^1(\ell.^{G(\varphi(n))}, JM)$. Therefore we can apply the inductive assumption to the map $\mathrm{Ext}^1(\ell.^{G(\varphi(n))}, JM) \longrightarrow \mathrm{Ext}^1(\ell.^{G(\varphi^j(n))}, JM)$ to conclude.

This tells us that for any quasi-coherent module M on U the map $\mathrm{Ext}^1(\ell.^{G(n)}, M) \longrightarrow \mathrm{Ext}^1(\ell.^{G(\varphi^N(n))}, M)$ is zero since by hypothesis $J^N = (0)$.

Now let us return to the situation of the proposition:

$$\begin{array}{ccc}
X & \hookrightarrow & X' \\
{\scriptstyle f}\downarrow & & \downarrow \\
G(n) & \xrightarrow{j} & G(\varphi^N(n))
\end{array}$$

We cover X' by affine open sets V_i' such that the image of each V_i' in S is contained in an affine U as above. Denote by V_i the affine open subscheme of X having V_i' as its underlying space. If we could prolong $f|V_i$ to an f' on V_i' as desired in the conclusion of the proposition, then because X is affine we could prolong f to X' itself. This follows from the standard obstruction theory, which tells us once we have local solutions of the problem, that the obstruction to having a global solution is an element of $H^1\Big(X, \underline{\mathrm{Hom}}_{\mathcal{O}_X}(f^*j^*\Omega^1_{G(\varphi^N(n))/S'}, I)\Big)$ and this group is zero since $\Omega^1_{G(\varphi^N(n))/S}$ is of finite presentation. [E.G.A.IV 16.4.22]. Thus we see that we can assume S to be affine. But now we know from [14; 11.1.5, 11.1.7] that the obstruction to lifting $j \circ f: X \longrightarrow G(\varphi^N(n))$ to X' is the image of the "obstruction element" in $\mathrm{Ext}^1_{\mathcal{O}_X}\Big(Lf^*L_\cdot^{G(n)/S}, I\Big)$ in $\mathrm{Ext}^1_{\mathcal{O}_X}\Big(L(j\circ f)^*L_\cdot^{G(\varphi^N(n))/S}, I\Big)$. But now it follows from (3.2.9) that if $\pi_X: X \longrightarrow S$ is the structural map $Lf^*(L_\cdot^{G(n)/S}) = L\pi_X^*(\ell_\cdot^{G(n)})$ and similarly of course for $L(j\circ f)^*(L_\cdot^{G(\varphi^N(n))/S})$. Thus we want to know that the image of an element in $\mathrm{Ext}^1_{\mathcal{O}_X}(L\pi_X^*(\ell_\cdot^{G(n)}), I)$ under the map $\mathrm{Ext}^1(L\pi_X^*(\ell_\cdot^{G(n)}), I) \longrightarrow \mathrm{Ext}\Big(L\pi_X^*(\ell_\cdot^{G(\varphi^N(n))}), I\Big)$ is zero. But by adjointness (same reference to Hartshorne and S.G.A. 4 as above) this map is the same as the map

$$\mathrm{Ext}^1_{\mathcal{O}_S}\Big(\ell_\cdot^{G(n)}, \pi_{X*}(I)\Big) \longrightarrow \mathrm{Ext}^1_{\mathcal{O}_S}\Big(\ell_\cdot^{G(\varphi^N(n))}, \pi_{X*}(I)\Big)$$

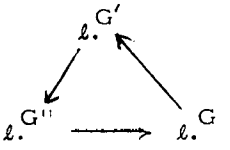
which we've seen is the zero map. This completes the proof.

Corollary (3.3.2) $G = \varinjlim G(n)$ is, under the hypotheses of the proposition, formally smooth.

Proof: If X is any affine scheme over S $\Gamma(X, G) = \varinjlim \Gamma(X, G(n))$, since X is quasi-compact.

Definition (3.3.3) Writing the cotangent complex $L.^{G/S}$ so that $\Omega^1_{U(G)^X/S}\big|^G$ is in degree 0 and I/I^2 is in degree 1, we define $\underline{\omega}_G = H_o(\ell.^G)$, $\underline{n}_G = H_1(\ell.^G)$. Notice this use of the symbol $\underline{\omega}_G$ is of course consistent with our previous notation.

Proposition (3.3.4): Consider an exact sequence of finite locally-free S groups: $0 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 0$. Then there is an exact triangle in the derived category, $D(S)$:



giving rise to an exact sequence of $\mathcal{O}_S$-modules:

(3.3.5) $0 \longrightarrow \underline{n}_{G''} \longrightarrow \underline{n}_G \longrightarrow \underline{n}_{G'} \longrightarrow \underline{\omega}_{G''} \longrightarrow \underline{\omega}_G \longrightarrow \underline{\omega}_{G'} \longrightarrow 0$

Proof: Let us first observe that by [E.G.A. IV 19.3.9(ii)] the morphism $G \longrightarrow G''$ makes G locally a complete intersection relative to G'' because after a f.p.q.c. base change G is as G''-scheme isomorphic to $G'_{G''}$. Since G is a finite and locally-free G'' scheme we can certainly embed G in a smooth G''-scheme; for example if G is defined by the $\mathcal{O}_{G''}$-algebra $\mathcal{A}$ then we can use $W(\mathcal{A})$. [E.G.A. II 1.4.10]. Thus the

relative cotangent complex $L_{\cdot}^{G/G''}$ is defined [S.G.A. 6 VIII 2.3]. But now by [14; 10.5.21] we have an exact triangle in the derived category D(G)

$$\begin{array}{ccc} & L_{\cdot}^{G/G''} & \\ \swarrow & & \nwarrow \\ \overline{L_{\cdot}^{G''/S,G}} & \longrightarrow & L_{\cdot}^{G/S} \end{array}$$

which comes from the commutative diagram

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G'' \\ & \searrow \quad \swarrow & \\ & S & \end{array}$$

and where $\overline{L_{\cdot}^{G''/S,G}} = L\pi^{*}(L_{\cdot}^{G''/S}) \,/ K[1]$ with K the kernel of $H_1(L\pi^{*}(L_{\cdot}^{G''/S})) \longrightarrow H_1(L_{\cdot}^{G/S})$ But now if $S' \subseteq S$ is any affine open then it is immediate that the diagram

$$\begin{array}{ccc} G \underset{S}{\times} S' & \xrightarrow{\pi_{S'}} & G'' \underset{S}{\times} S' \\ & \searrow \quad \swarrow & \\ & S' & \end{array}$$

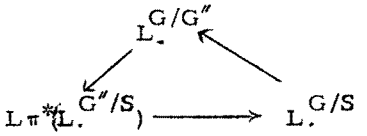
satisfies the hypothesis of [S.G.A. 6 VIII 2.6]. Thus we find an exact triangle in $D(G \underset{S}{\times} S')$

$$\begin{array}{ccc} & L_{\cdot}^{G \times S'/G'' \times S'} & \\ \swarrow & & \nwarrow \\ L\pi_{S'}^{*}(L_{\cdot}^{G'' \times S'/S'}) & \longrightarrow & L_{\cdot}^{G \times S'/S'} \end{array}$$

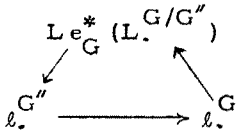
Taking the corresponding homology sequence we see that when restricted to $G \underset{S}{\times} S'$ the map

$$H_1(L\pi^*(L^{G''/S})) \longrightarrow H_1(L_\cdot^{G/S})$$

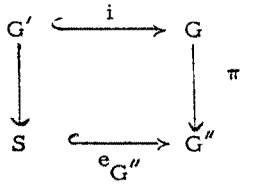
is injective (i.e., $K|G \underset{S}{\times} S' = (0)$) Since S' was any affine open subset of S it follows that $K = (0)$ and hence $\overline{L_\cdot^{G''/S,G}} = L\pi^*(L_\cdot^{G''/S})$ and thus we obtain an exact triangle:



Let $e_G : S \longrightarrow G$ be the unit section. Then applying Le_G^* to the above exact triangle we obtain an exact triangle:



But using that $\pi : G \longrightarrow G''$ is flat and [S.G.A. 6 VIII 2.2] we see (just as in 3.2.11) from the cartesian diagram:



that $$Li^*(L_\cdot^{G/G''}) = L_\cdot^{G'/S}$$

and therefore $\ell_\cdot^{G'} = Le_{G'}^*(L_\cdot^{G'/S}) = Le_G^*(L_\cdot^{G/G''})$.

This gives us our desired exact triangle and completes the proof of the proposition.

Lemma (3.3.6) Suppose G is finite and locally-free on S. Then $\underline{\omega}_G$ is locally free if and only if it is flat. If this is the case then $\underline{n}_G$ is also locally free (of finite rank) and rank $(\underline{\omega}_G)$ = rank $(\underline{n}_G)$.

Proof: Let us write $\ell_\cdot^G = L_1 \longrightarrow L_o$. Then with obvious notation we have exact sequences:

$$0 \longrightarrow \underline{n}_G \longrightarrow L_1 \longrightarrow \text{im} \longrightarrow 0$$

$$0 \longrightarrow \text{im} \longrightarrow L_o \longrightarrow \underline{\omega}_G \longrightarrow 0$$

Hence, since $\underline{\omega}_G$ is of finite presentation, if it is flat, then it is locally-free which implies the image of the morphism $L_1 \longrightarrow L_o$ is locally-free of finite rank. But certainly this implies $\underline{n}_G$ is locally-free of finite rank. In this case we have rank (L_o) - rank (L_1) = rank $(\underline{\omega}_G)$ - rank $(\underline{n}_G)$. Because the relative dimension of G over S is zero it follows that rank $(\underline{\omega}_G)$ = rank $(\underline{n}_G)$.

The following are corollaries of 3.3.4.

Corollary (3.3.7) Given $0 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 0$ as in (3.3.4) then:

a) The following conditions are equivalent and if S is of characteristic p, they are implied by $G' \subseteq G[1]$

1) $\underline{\omega}_G \longrightarrow \underline{\omega}_{G'}$ is an isomorphism

2) $\underline{\omega}_{G''} \longrightarrow \underline{\omega}_G$ is the zero map

3) $\underline{n}_{G'} \longrightarrow \underline{\omega}_{G''}$ is surjective

b) Suppose $\underline{\omega}_{G''}$ is locally-free and $\underline{n}_{G'}$ is of finite type and that $\text{rank}_{k(s)} (\underline{n}_{G'} \otimes k(s)) \leq \text{rank}_{k(s)} (\underline{\omega}_{G''} \otimes k(s))$ holds for all $s \in S$. Then the above conditions of a) are equivalent to

3 bis) $\underline{n}_{G'} \longrightarrow \underline{\omega}_{G''}$ is an isomorphism and in this case $\underline{n}_{G} \longrightarrow \underline{n}_{G'}$ is the zero map.

Proof: That the three conditions of a) are equivalent is immediate from (3.3.5). If S is of characteristic p, then $G' \subseteq G[1]$ implies $G'[1] = G[1]$ and hence since $\mathrm{Inf}^1(G) \subseteq G[1]$ (see the end of the proof of 2.1.8) we have $\underline{\omega}_G = \underline{\omega}_{G'}$ which is condition 1).

b) Assume the additional conditions and that $\underline{n}_{G'} \longrightarrow \underline{\omega}_{G''}$ is surjective. Then because $\underline{\omega}_{G''}$ is locally free we must (locally on S) have a splitting $\underline{n}_{G'} = \mathrm{Ker} \times \underline{\omega}_{G''}$ where Ker denotes the kernel of $\underline{n}_{G'} \longrightarrow \underline{\omega}_{G''}$. By our assumption on the ranks we must have $\mathrm{Ker} \otimes_{\mathcal{O}_S} k(s) = (0)$ for all $s \in S$. Ker is of finite type because $\underline{n}_{G'}$ is. Therefore by Nakayama we must have each stalk of Ker is zero and therefore Ker = (0). This completes the proof since the last assertion is obvious.

Remark (3.3.8) From (3.3.6) it follows that the inequality in the last corollary can be written $\mathrm{rank}\,(\underline{\omega}_{G'_s}) \leq \mathrm{rank}\,(\underline{\omega}_{G''_s})$ for all $s \in S$.

Corollary (3.3.9) Assume given the exact sequence $0 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 0$ as above and assume further that:

1) $\underline{\omega}_G \longrightarrow \underline{\omega}_{G'}$ is an isomorphism

2) $\underline{\omega}_G$ and $\underline{\omega}_{G''}$ are locally free

3) $\mathrm{rank}\,(\underline{\omega}_{G'_s}) \leq \mathrm{rank}\,(\underline{\omega}_{G''_s})$ holds for all $s \in S$

Then for any affine open $U \subseteq S$ and for any quasi-coherent module M on U, the map

$$\mathrm{Ext}^1_{\mathcal{O}_U}(\ell_\cdot^{G'} \mid U, M) \longrightarrow \mathrm{Ext}^1_{\mathcal{O}_U}(\ell_\cdot^{G} \mid U, M)$$

is the zero map. In particular for any quasi-coherent M on S the map $\underline{Ext}^1(\ell_\cdot^{G'}, M) \longrightarrow \underline{Ext}^1(\ell_\cdot^{G}, M)$ is zero.

Proof: Because $\underline{Ext}^1(\ell^G, M)$ is the sheaf associated to the presheaf $U \longmapsto Ext^1(\ell_\cdot^G|U, M|U)$ it follows that the last assertion follows from the preceding one. We can obviously assume S is affine. Let $I^\cdot$ be an injective resolution of M. By inspecting the complex $Hom^\cdot(\ell_\cdot^G, I^\cdot)$ whose component of degree m is

$$Hom\,(L^{-1}, I^{m-1}) \oplus Hom\,(L^o, I^m)$$

($\ell_\cdot^G$ being $L^{-1} \longrightarrow L^o$ of course), we find a functorial exact sequence:

$$0 \longrightarrow Ext^1(\underline{\omega}_G, M) \longrightarrow Ext^1(\ell_\cdot^G, M) \longrightarrow Hom\,(\underline{n}_G, M) \longrightarrow Ext^2\,(\underline{\omega}_G, M)$$

and a similar sequence for G'. Hence because $\underline{\omega}_G$ and $\underline{\omega}_{G'}$ are locally free we have isomorphisms:

$$Ext^1(\ell_\cdot^G, M) \xrightarrow{\sim} Hom\,(\underline{n}_G, M)$$

$$Ext^1(\ell_\cdot^{G'}, M) \xrightarrow{\sim} Hom\,(\underline{n}_{G'}, M)$$

But now we know from (3.3.8) that our hypotheses insure that $\underline{n}_{G'} \longrightarrow \underline{n}_G$ is the zero map and hence we are done.

Corollary (3.3.10) Let S be a scheme such that p^{N+1} kills S, and G be a finite locally-free S-group satisfying the equivalent conditions of lemma (1.1) of Chapter I for an $n \geq N+1$. Then for any affine open subset U of S, the mapping (defined for any q. coherent M) $Ext^1(\ell_\cdot^{G(n-N-1)}, M)$ $\longrightarrow Ext^1(\ell_\cdot^G, M)$ is zero.

Proof: Just as in the proof of (3.3.1) we are immediately led, via the adjointness relation recalled there, to the case when $N = 0$, i.e., when S is of characteristic p. Then if $n = 1$, $G(n-N-1) = G(0) = (0)$ and there is nothing to prove. If $n \geq 2$ we must verify the conditions of the previous corollary for $G' = G(n-1)$. Condition 1) is clear as $G'[1] = G[1]$ and hence $\underline{\omega}_G \longrightarrow \underline{\omega}_{G'}$ is an isomorphism. Condition 3) is also trivial as $G'' = G(1)$. To verify that condition 2) holds we use the following proposition.

Proposition (3.3.11) Let S be a scheme of characteristic p and $G = G(n)$ a truncated Barsotti-Tate group on S, or if $n = 1$ assume there is a truncated B. T. group $G(2)$ giving rise to G. Then

a) For all i such that $0 \leq i \leq n$ we have

$$f^{n-i}: G[n] \longrightarrow G[i]^{p^{n-i}} \text{ is an epimorphism}$$

b) $\operatorname{Ker} f^n = \operatorname{im} v^n$ and $\operatorname{Ker} v^n = \operatorname{im} f^n$

c) $G[n]$ is finite and locally free on S

Proof: Let us first observe that c) allows us to appeal to [I, (2.1.4)] to conclude the proof of (3.3.10). Condition a) is trivial if $n=1$. If $n \geq 2$ we have (for each i) the following commutative diagram:

$$\begin{array}{ccc} (p^{n-i})^{-1}\left(G[i]^{p^{n-i}}\right) & \xrightarrow{p^{n-i}\,\mathrm{id}_G(p^{n-i})} & G[i]^{(p^{n-i})} \\ & {\scriptstyle v^{n-i}} \searrow \quad \nearrow {\scriptstyle f^{n-i}} & \\ & G[n] & \end{array}$$

As the morphism $p^{n-i}.\mathrm{id}_G(p^{n-i})$ is an epimorphism, it follows that f^{n-i}

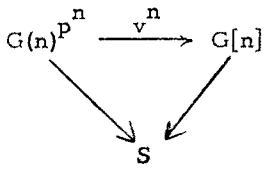
is also. To prove b) let us first assume that $G(n)$ comes from a $G(2n)$ which is a truncated Barsotti-Tate group. But then we have an exact sequence:

$$0 \longrightarrow G(n) \longrightarrow G(2n) \xrightarrow{p^n} G(n) \longrightarrow 0$$

Therefore $G[n] \subseteq G(n)$ and the map $(p^n)^{-1}(G[n]) \longrightarrow G[n]$ is an epimorphism. But once again we can write $p^n = v^n \circ f^n$ and since obviously $f^n: (p^n)^{-1}(G[n]) \longrightarrow G(n)^{(p^n)}$ we see $v^n: G[n]^{(p^n)} \longrightarrow G[n]$ is an epimorphism. That $\operatorname{im} f^n = \ker v^n$, is of course handled analogously. Thus we have in particular proved b) if $n = 1$. We proceed to establish its truth in general by induction on n. Consider the diagram:

$$\begin{array}{ccc} G(n)^{p^n} & \xrightarrow{v^n} & G[n] \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle f} \\ G(n-1)^{p^n} & \xrightarrow[v^{n-1}]{} & G[n-1]^p \end{array}$$

By the induction hypothesis $v^{n-1}: G[n-1]^{p^n} \longrightarrow G[n-1]^p$ is an epimorphism. Therefore $f \circ v^n$ is an epimorphism. Hence if we can show $G[1] \subseteq \operatorname{im} v^n$ it will follow that v^n is an epimorphism. But by the case $n = 1$ settled above $G[1] = v(G(1)^p) = v \circ p^{n-1}(G(n)^p) = v^n(f^{n-1}(G(n)^p)) \subseteq v^n(G(n)^{(p^n)})$. The other case is of course handled in the same way. To prove c) we observe that $G[n]$ is certainly finite and of finite presentation over S. Therefore to conclude it is locally free it suffices to show it is flat. But this follows immediately from b) because we have a commutative diagram:



and v^n being an epimorphism is faithfully flat while $G(n)^{p^n}$ is certainly flat over S.

Remark (3.3.12) The condition that G(1) comes from a G(2) can not be dropped. To see this consider the following example. Let k be a field of characteristic p, $S = \mathrm{Spec}(k[[t]])$ and $G = \mathrm{Spec}(k[[t]][X]/(X^p - tX))$ with addition as group law. Then at the generic point G is étale while at the closed point G becomes α_p. But this implies $\underline{\omega}_G$ has rank 0 at the generic point and rank 1 at the closed point. As S is connected, $\underline{\omega}_G$ certainly can not be locally free.

Theorem (3.3.13) If p is locally nilpotent on S and G is in B.T.(S), then G is formally smooth.

Proof: Let X′ be an affine scheme over S and X a closed subscheme defined by an ideal of square zero. Let $f: X \longrightarrow G$ be in $\Gamma(X, G)$. We must show f can be lifted to an $f': X' \longrightarrow G$. As X is quasi-compact we have $\Gamma(X, G) = \varinjlim \Gamma(X, G(n))$ and hence can assume $f: X \longrightarrow G(n)$ for some n. We cover X by a finite number of affine opens U_i $i=1,\ldots,m$ such that the image of U_i in S is contained in an affine open V_i. Since p is nilpotent on each V_i there is an integer N such that p^{N+1} is zero on $\cup V_i$. Replacing S by $S' = \cup V_i$ and G by $G_{S'}$ we are led to the

case when p is nilpotent on S, $p^{N+1} \cdot 1_S = 0$. But now by (3.3.10) and (3.3.1) we see f can be lifted to an f' and the theorem is proved.

The following example shows that if p is not locally nilpotent on S, a Barsotti-Tate group need not be formally smooth.

Example (3.3.14) Let $S = \mathrm{Spec}(A)$ and consider the Barsotti-Tate group μ_{p^∞} (I, 3.8.1). To say μ_{p^∞} is formally smooth means that whenever C is an A-algebra, I a nilpotent ideal of C (of square zero) and $x \in C/I$ is such that $x^{p^n} = 1$, then there is an $x' \in C$ which reduces modulo I to x and has the property that for some $m \geq n$, $x'^{p^m} = 1$.

Writing $x' = u + y$ where u is some definite lifting of x and $y \in I$ we have $x'^{p^n} = u^{p^n} + p^n y$ (since I has square zero) and since $x^{p^n} = 1$ we see $u^{p^n} = 1 + \zeta$ for some $\zeta \in I$. Since $x'^{p^m} = 1$ this means $(1+\zeta)^{p^{m-n}} + p^m y = 1$ and hence $p^{m-n}\zeta + p^m y = 0$, or equivalently $p^{m-n}(\zeta + p^n y) = 0$. Since given x we have chosen u and thus ζ, we see that we can find an x' so as to lift the point of μ_{p^∞} with values in $\mathrm{Spec}(C/I)$ to $\mathrm{Spec}(C)$ if and only if we can find a $y \in I$ and integer m' such that $p^{m'}(\zeta + p^n y) = 0$. But this is true if and only if the element $\frac{\zeta}{p^n}$ in I_p belongs to the image of I. But now (n being fixed) we have $\zeta = u^{p^n} - 1$ and $\zeta^2 = 0$ and hence there is a homomorphism of the ring $A[T]/(T^{p^n} - 1)^2$ into C which takes $T \longmapsto u$ and induces a homomorphism $A[T]/(T^{p^n} - 1) \longrightarrow C/I$ taking $T \longmapsto x$. Thus we see it suffices to check our condition for the ring $C = A[T]/(T^{p^n} - 1)^2$ and the element $\zeta = T^{p^n} - 1$ in this ring. Since $C/(T^{p^n} - 1)$ is a free A-module we have

$C = (T^{p^n} - 1) \oplus C/(T^{p^n} - 1)$ as A-module. Thus we see $\frac{\zeta}{p^n}$ is in the image of the ideal $(T^{p^n} - 1)$ if and only if it is in the image of C in C_p. But since C is a free A-module with base $1, T, \ldots, T^{2p^n-1}$ we see this will be true if and only if $\frac{1}{p^n}$ belongs to the image of A in A_p (i.e., if and only if $\frac{1}{p}$ belongs to the image of A in A_p). Thus we can conclude that μ is formally smooth if and only if $\frac{1}{p}$ belongs to the image of A in A_p. Therefore if $A = \mathbb{Z}$ or $\mathbb{Z}_p$ (the p-adic integer and not the localization of $\mathbb{Z}$ with respect to the element p) we see μ is not formally smooth over A.

Finally we shall prove that if p is locally nilpotent on S then $\overline{G}$ is a formal Lie group. We begin with a lemma.

Lemma (3.3.15) Let G be a p-torsion group on S with all G(n) representable. Assume we are given an S-scheme X' and a subscheme X defined by an ideal I such that $I^{k+1} = (0)$ and $p^N \cdot I/I^2 = 0$. Then if $f': X' \longrightarrow G$ is such that $f = f'|X: X \longrightarrow G(n)$, we have $f': X' \longrightarrow G(n+kN)$.

Proof: The problem is local on X' and hence we can assume X' to be affine and thus quasi-compact. But then $f' \in \Gamma(X', G) = \varinjlim \Gamma(X', G(m))$ and hence we can assume $f': X' \longrightarrow G(n')$ for some n'. Therefore we can assume that G is representable. We use induction on k. If we could show $f'|\mathrm{Var}(I^k): \mathrm{Var}(I^k) \longrightarrow G(n + (k-1)N)$, then by the case k=1 we would know $f': X' \longrightarrow G(n+kN)$. Thus it suffices to treat the case k=1, i.e., $I^2 = 0$. Since $f: X \longrightarrow G(n)$ we have $p^n \cdot f = 0$ and thus $p^n f' \in G(X')$ has the property that its restriction to G(X) is zero. Since

I^2 is zero and G is representable we know the group of sections of G over X′ whose restriction to X is zero is isomorphic to the group $\mathrm{Hom}_{\mathcal{O}_X}\left(\omega_G \otimes_{\mathcal{O}_S} \mathcal{O}_{X'}, I\right)$ [S.G.A. 3 III 0.9]. But since p^N kills I, we certainly have $p^N(p^n f') = 0$ which implies $f' \in G(n+N)(X)$.

Corollary (3.3.16) Let p^N kill S and let G be as in the proposition. Then the k^{th} infinitesimal neighborhood of G(n) in G is the same as that of G(n) in G(n+kN). In particular $\mathrm{Inf}^k(G) = \mathrm{Inf}^k(G(kN))$ and is therefore representable.

Proof: If $f: T' \longrightarrow G$ belongs to the k^{th} infinitesimal neighborhood of G(n) in G, then there is a covering family $\{T_i' \longrightarrow T'\}$ and schemes T_i such that $T_i \hookrightarrow T_i'$ is a nilpotent immersion of order k and $f|T_i: T_i \longrightarrow G(n)$. But then by the proposition $f|T_i': T_i' \longrightarrow G(n+kN)$ and hence $f \in \Gamma(T', G(n+kN))$ which proves the corollary.

Corollary (3.3.17) If p^N kills S and if $k < p^n$ we have $\mathrm{Inf}^k(G) \subseteq G(n+N-1)$ and hence $\mathrm{Inf}^k(G) = \mathrm{Inf}^k(G(n+N-1))$.

Proof: Let X′ be an S-scheme and $X \hookrightarrow X'$ be a nilpotent immersion of order k. Denote with the subscript "o" the object obtained by reducing a given object modulo p. Given $f': X' \longrightarrow G$ whose restriction to X is zero, then we have $f_o': X_o' \longrightarrow G_o$ belongs to $\mathrm{Inf}^k(G_o)$. By the reasoning at the end of the proof of (2.1.8) (where we show that $\varinjlim G[n] = \varinjlim \mathrm{Inf}^k(G)$) we know that $\mathrm{Inf}^k(G_o) \subseteq G_o[n] \subseteq G_o(n)$. But this means that $f' \in G(X')$ has its restriction to $G(X_o') = G_o(X_o')$ belonging to $G(n)(X_o')$.

If we now apply the proposition (3.3.15) with $I = p\mathcal{O}_{X'}$, $k = N-1$ and $N = 1$, we find $f' \in G(n+N-1)(X')$

Theorem (3.3.18) Let p be locally nilpotent on S and G be a Barsotti-Tate group on S. Then $\overline{G} = \varinjlim \mathrm{Inf}^k(G)$ is a formal Lie group.

Proof: By (1.1.6) we know $\overline{G}$ is a subgroup of G and hence we must show it is a formal Lie variety. By (3.3.16) $\mathrm{Inf}^k(G)$ is, locally on S, representable and therefore since it is a sheaf it is representable.

By Theorem (3.3.13) we know G is formally smooth and obviously this implies that $\overline{G}$ is formally smooth. This tells us that $\mathrm{Inf}^k(G)$ satisfies the lifting condition 2) of (3.1.1) and hence, since locally on S $\mathrm{Inf}^k(G) = \mathrm{Inf}^k(G(m))$ for an appropriate m, it follows from (3.1.1) that locally on S $\mathrm{Inf}^k(G)$ satisfies condition 1) of that proposition. But now it is obvious that $\overline{G}$ satisfies condition 2) of Definition (1.1.4) and hence is a formal Lie group.

Definition (3.3.19) We define for a Barsotti-Tate group G on S (p locally nilpotent on S) $\underline{\omega}_G$ to be $\underline{\omega}_{\overline{G}}$.

Remark (3.3.20) It follows immediately from (3.3.18) that $\underline{\omega}_G$ is locally-free of finite rank and from (3.3.16) or, for a better estimate, (3.3.17) that locally on S $\underline{\omega}_G = \underline{\omega}_{G(m)}$ if m is sufficiently large. If p^N kills S, then $\underline{\omega}_G = \underline{\omega}_{G(N)}$ as follows from (3.3.17).

Remark (3.3.21) Let p be nilpotent on S and G, H two B. T. groups on S. Let $S_o = \mathrm{Var}(p)$. The map $\mathrm{Hom}(G,H) \longrightarrow \mathrm{Hom}(G_o, H_o)$ is

injective.

Proof: Let $u: G \longrightarrow H$ be such that $u_o = 0$. If p^N kills S, this implies $im(u) \subseteq Inf^{p^N}(H)$. By (3.3.17) $im(u) \subseteq H(n)$ for n sufficiently large. But then $u \circ p^n \cdot id_G = p^n \cdot id_H \circ u = 0$. Since G is p-divisible, $u = 0$.

§4. In this section we study the relation between formal Lie groups and Barsotti-Tate groups on a scheme S, with p locally nilpotent on S.

Lemma (4.1) Let B be a ring in which p is nilpotent and I be a nilpotent ideal of B. Define a sequence of ideals $I_1 = pI + I^2, \ldots, I_{n+1} = pI_n + (I_n)^2$. Then for n sufficiently large $I_n = (0)$.

Proof: Let $J = pB + I$. Then one checks immediately that $I_n \subseteq J^{n+1}$, from which the result follows.

Lemma (4.2) If p is locally nilpotent on S and $\overline{G}$ is a formal Lie group over S, then $\overline{G}$ is of p-torsion.

Proof: We must show $\overline{G} = \varinjlim \overline{G}(n)$ and since this is a statement about sheaves it suffices to check it locally on S. Thus we can assume $S = Spec(A)$ with p nilpotent on A and $\overline{G}$ is given by a power series ring $A[[X_1, \ldots, X_N]]$. If T is any affine S-scheme, say $T = Spec(B)$, then an element of $\overline{G}(T)$ will be an N-tuple $(b_1, \ldots, b_N)$ with each b_i nilpotent. Let I be the ideal generated by $\{b_1, \ldots, b_N\}$. Then each component of $p \cdot (b_1, \ldots, b_N)$ belongs to $pI + I^2$ and $p^2(b_1, \ldots, b_N) \in p \cdot (pI + I^2) + (pI + I^2)^2, \ldots$. Thus by (4.1) we see $\overline{G}$ is of p-torsion.

Let S be the spectrum of an artin local ring with residue field of

characteristic p and let G be a p-divisible formal Lie group on S. We shall show that G is a Barsotti-Tate group. To do this it suffices to prove that G(1) is finite and locally-free.

Proposition (4.3) Let A be an artin local ring with residue field k of characteristic p and let $u: G \longrightarrow G$ be an epimorphism of a formal Lie group to itself. Then Ker(u) is finite and locally-free.

Proof: Denote by the subscript "o" the result of reducing an object defined over A to k the residue field of A. Let $(Sch/k)'$ denote the full sub-category of (Sch/k) consisting of those schemes which are locally of finite type over k. Endow $(Sch/k)'$ with the topology induced by the f.p.p.f. topology on (Sch/k). Observe that the restriction of $u: G \longrightarrow G$ to $(Sch/k)'$ is obviously an epimorphism. By [S.G.A.3 VII B 1.3.4] there is a morphism of sites $v: (Vf/k) \longrightarrow (Sch/k)'_{f.p.p.f.}$ given by the "inverse image" functor $v^{-1}: (Sch/k)' \longrightarrow Vf/k$ which is defined by $v^{-1}(X) = \hat{X}/k$ in the notation of [S.G.A.3 VII B 1.2.6]. Since the extension of v^{-1} to sheaves is exact it transforms G into itself thought of as a "formal variety" in the sense of [S.G.A.3 VII B] and transforms u into an epimorphism in the category of formal groups over k. Since k is a field [S.G.A.3 VII B 1.4] implies that the map $\tilde{u}_o: k[[X]] \longrightarrow k[[X]]$ corresponding to u_o is "topologically flat" and because the power series ring is Noetherian this means it is flat.

Because the category of commutative formal groups over k is antiequivalent to the category of commutative affine groups over k

[S.G.A.3 VII B 2.2.2] it follows from [G.A. III §3, 5.5 a)] that $\mathrm{Ker}(u_o)$ is finite over k. Since A is artin this implies Ker(u) is finite over A. To see Ker(u) is flat over A it suffices to show the map $\tilde{u}: A[[X]] \longrightarrow A[[X]]$ corresponding to u is flat. Let $\underline{m}_A$ denote the maximal ideal of A. Consider the following sequence of maps

$$A \longrightarrow A[[X]] \xrightarrow{\tilde{u}} A[[X]] .$$

Because the first map and the composite are flat, the map

$$m_A \cdot A[[X]] \otimes_{A[[X]]} A[[X]] \longrightarrow \tilde{u}(m_A \cdot A[[X]]) \cdot A[[X]]$$

is bijective. Since we already know $\tilde{u}_o$ is flat we can because $\underline{m}_A$ is nilpotent apply the criterion of flatness [4, Chap. 3 §5 Theorem 1] to conclude $\tilde{u}$ is flat. This completes the proof.

Proposition (4.4) Let p be locally nilpotent on S and let G be in B. T. (S). Then the following conditions are equivalent:

1) $G = \overline{G}$.

2) G is a formal Lie group.

3) For all n G(n) is radiciel.

4) G(1) is radiciel.

Proof: 1) implies 2) by (3.3.18). 2) implies 1) because, by definition, a formal Lie group is ind-infinitesimal. Since property 2) is stable under base change by (1.03), to prove that 2) implies 3) we must show the map $G(n) \longrightarrow S$ is injective. Clearly we can assume S is affine and hence G(n) is quasi-compact and therefore $G(n) \subseteq \mathrm{Inf}^k(G)$ for some k. But

since the map $\mathrm{Inf}^k(G) \longrightarrow S$ is obviously injective it follows that $G(n)$ is radiciel. Conversely if $G(n)$ is radiciel, then since the closed immersion $S \longrightarrow G(n)$ is surjective, the ideal of this immersion must be locally nilpotent. Obviously this implies that $G(n)$ is ind-infinitesimal (and in fact is equal to one of its infinitesimal neighborhoods locally on S) and hence $G = \varinjlim G(n)$ is ind-infinitesimal. Thus $G = \overline{G}$ and 3) implies 1) (and 2)). Finally as 3) obviously implies 4) we must see that 4) implies 3). But this follows immediately via using the exact sequence $0 \longrightarrow G(n-1) \longrightarrow G(n) \xrightarrow{p^{n-1}} G(1) \longrightarrow 0$.

Corollary (4.5) If p is locally nilpotent on S, there is an equivalence of categories between that of Barsotti-Tate groups on S, with $G(1)$ radiciel, and the category of formal Lie groups G with $p: G \longrightarrow G$ an epimorphism and $G(1)$ finite and locally-free.

Proof: By (4.2) and (4.4) both categories are identified with the same full sub-category of f.p.p.f. sheaves of groups on S.

Corollary (4.6) If S is artin, a p-divisible formal Lie group is a Barsotti-Tate group with $G(1)$ radiciel and conversely

Proof: (4.3) and (4.5).

Proposition (4.7) Let p be loc.nilpotent on S and G in B.T.(S). In order that $\overline{G} = 0$ it is necessary and sufficient that G be ind-étale.

Proof: If G is ind-étale, then for all k, $\mathrm{Inf}^k(G) = (0)$, since locally a point of $\mathrm{Inf}^k(G)$ with values in an S-scheme T must be a point of $G(n)$ with values in T for some n, and hence must be zero since $G(n)$ is

étale. Conversely if $\overline{G} = 0$, then for any $s \in S$, $\overline{G}_s = 0$, which implies $(G(n))_s$ has no connected (= radiciel) part and hence is étale. But $G(n)$ being flat over S, this implies that $G(n)$ is étale.

Apologies are offered in advance to the reader for the proof in the following lemma.

Lemma (4.8) Let $X \xrightarrow{f} S$ be finite and locally-free. Then the function $s \longmapsto$ separable rank (X_s) is locally constant if and only if there are morphisms $i: X \longrightarrow X'$, $f': X' \longrightarrow S$ which are finite and locally-free with i radiciel and surjective, f' étale and $f = f' \circ i$. The factorization is "unique" up to unique isomorphism and is functorial in X/S.

Proof: Observe that because of the uniqueness assertion it suffices to prove the lemma locally on S. Thus we can assume S affine and separable rank $(X_s) = n$ for all $s \in S$ (n some integer). Also observe that the "if" assertion is trivial. Now, by [E.G.A. IV 8.9.1, 8.10.5 (x), 11.2.6 (ii), 9.7.8, 9.3.3] we can assume S is noetherian in order to prove the existence uniqueness and functoriality assertions. We proceed in several steps which we outline:

1) existence and uniqueness when S is a field.

2) existence and uniqueness when S is a complete (Noetherian) local ring.

3) uniqueness for arbitrary $S = \mathrm{Spec}\,(A)$, A Noetherian.

4) existence of $f': X' \longrightarrow S$ when S is a local ring.

5) existence of $i: X \longrightarrow X'$ when S is a local ring.

6) existence for arbitrary $S = \mathrm{Spec}\,(A)$, A Noetherian.

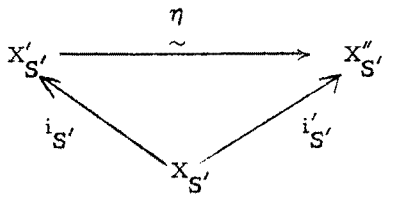
7) functoriality.

1) If $S = \mathrm{Spec}(k)$ and $X = \mathrm{Spec}(B)$, we write $B = B_1 \times \dots \times B_t$ as a product of finite dimensional local k-algebras. For each i we let k_i' be the maximal separable extension of k in the residue class field of B_i. Since B_i is artin we see there is a unique homomorphism $k_i' \longrightarrow B_i$ lifting the natural inclusion. Thus we can take $X' = \mathrm{Spec}(k_1' \times \dots \times k_t')$. This gives us existence. Uniqueness is clear because of the uniqueness of a field of representatives for k_i' in B_i.

2) Using the constancy of the separable rank to show $X \xrightarrow{i} X'$ is radiciel and surjective we see from [E.G.A. IV 18.3.2, 18.5.14, 18.5.12, 11.3.11, 1.5.4 (v)] that there is a unique solution of the problem when $S = \mathrm{Spec}(A)$, A a complete Noetherian local ring.

3) Let $X \xrightarrow{i} X' \xrightarrow{f'} S$ and $X \xrightarrow{i'} X'' \xrightarrow{f''} S$ be two solutions. To construct a unique isomorphism between them it suffices to show that there is a unique isomorphism between their localizations at any point $s \in S$. For, if this were done, then for each $s \in S$, there would be a neighborhood U_s of s to which this isomorphism extends, since we are really dealing with modules of finite type over a Noetherian ring. But by the uniqueness these isomorphisms would have to agree on $U_s \cap U_{s'}$ for any two points $s, s' \in S$. Therefore they could be patched together to give the desired uniqueness statement for all of S. Hence we have reduced ourselves to the case when S is a Noetherian local ring A. Let $S' = \mathrm{Spec}(\hat{A})$ and $S'' = \mathrm{Spec}(\hat{A} \underset{A}{\otimes} \hat{A})$. The morphism $S' \longrightarrow S$ is faithfully flat and quasi-

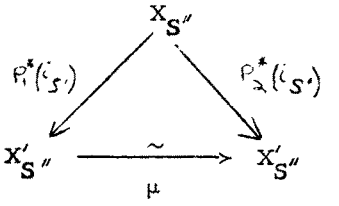
compact and hence we will apply descent [S.G.A. 1 VIII 2.1]. By 2) we have a commutative diagram:



We must show that η is a morphism of objects with descent data. To see this let τ_X(resp. $\tau_{X'}$, $\tau_{X''}$) denote the canonical isomorphism $p_1^*(X_{S'}) \xrightarrow{\sim} p_2^*(X_{S'})$ (resp. ...) We must show $\tau_{X''} \circ p_1^*(\eta) = p_2^*(\eta) \circ \tau_{X'}$. But we know $p_2^*(\eta) \circ \tau_{X'} \circ p_1^*(i_{S'}) = p_2^*(\eta) \circ p_2^*(i_{S'}) \circ \tau_X = p_2^*(i'_{S'}) \circ \tau_X = \tau_{X''} \circ p_1^*(i'_{S'}) = \tau_{X''} \circ p_1^*(\eta) \circ p_1^*(i_{S'})$. But $i: X \longrightarrow X'$ is faithfully flat and hence $p_1^*(i_{S'})$ is faithfully flat. But this implies it is an epimorphism of schemes and hence $p_2^*(\eta) \circ \tau_{X'} = \tau_{X''} \circ p_1^*(\eta)$, completing the proof.

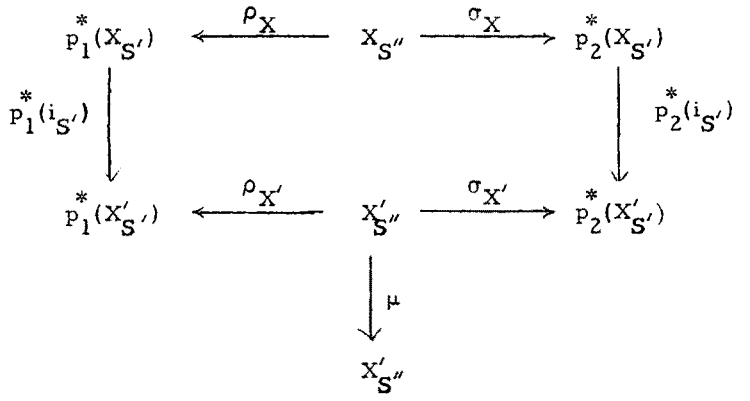
4) To show $f': X \longrightarrow S$ exists we shall show that, using the notation of 3) above, the X' which we know from 2) to exist over S' can be descended to S. Thus we have the standard situation $S'' \rightrightarrows S' \longrightarrow S$ and we have a solution of our problem for $X_{S'}$, call this solution Y. We want to descend Y to S. But by the uniqueness proved in 3) we see there is an isomorphism $p_1^*(Y) \xrightarrow{\sim} p_2^*(Y)$ (since both are solution for $X_{S''}$). But using the uniqueness of isomorphisms between solutions we see the isomorphism $p_1^*(Y) \xrightarrow{\sim} p_2^*(Y)$ must satisfy the cocycle condition and hence Y can be descended to an X' étale and finite over S [E.G.A. IV 17.7.3(ii), 2.7.1].

5) From 2) and 4) we know that over S' we have a morphism $i_{S'}: X_{S'} \longrightarrow X'_{S'}$. We want to see that this implies the existence of a similar morphism $i: X \longrightarrow X'$. When we pull back to S'' we find a commutative diagram



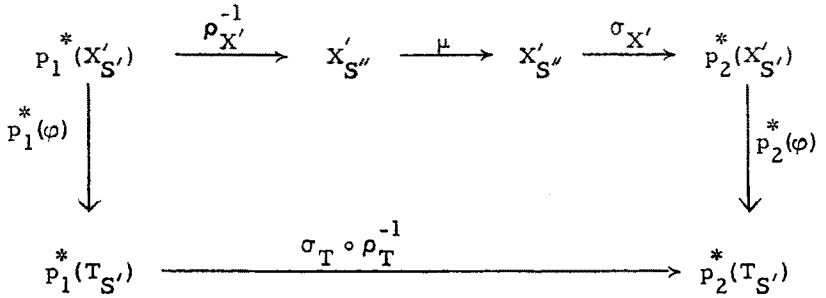
because of the uniqueness established in part 3). While μ need not be the identity it follows again from part 3) that the isomorphism μ must satisfy the cocycle condition $p_{13}^*(\mu) = p_{23}^*(\mu) \circ p_{12}^*(\mu)$. But now this implies (same reference to S.G.A. 1 as above) that there is a scheme T finite and étale over S and an isomorphism $\varphi: X'_{S'} \xrightarrow{\sim} T_{S'}$ such that φ establishes an isomorphism between X' with descent datum μ, and $T_{S'}$ with its canonical descent datum. If we now replace $i: X_{S'} \longrightarrow X'_{S'}$ by $\varphi \circ i: X_{S'} \longrightarrow T_{S'}$ we see easily from the following calculation that $\varphi \circ i$ is a morphism between objects equipped with descent data and hence can be descended.

Consider the following diagram in which all morphisms σ, ρ have obvious meaning:



We are told that $\mu \circ \rho_{X'}^{-1} \circ p_1^*(i_{S'}) \circ \rho_X = \sigma_{X'}^{-1} \circ p_2^*(i_{S'}) \circ \sigma_X$ and that $\sigma_{X'} \circ \mu \circ \rho_{X'}^{-1} : p_1^*(X'_{S'}) \xrightarrow{\sim} p_2^*(X'_{S'})$ satisfies the cocycle condition.

Thus we find a T/S and an isomorphism $\varphi: X'_{S'} \xrightarrow{\sim} T_{S'}$ which makes the following diagram commute:



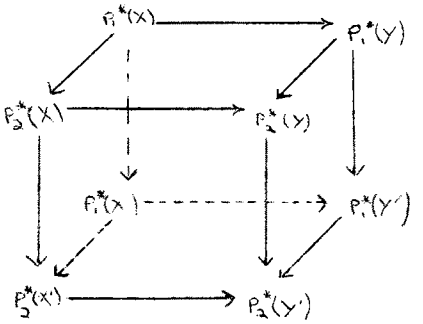
Therefore we have $\sigma_{X'} \circ \mu \circ \rho_{X'}^{-1} \circ p_1^*(i_{S'}) \circ \rho_X = p_2^*(i_{S'}) \circ \sigma_X$ giving $p_2^*(\varphi) \circ \sigma_{X'} \circ \mu \circ \rho_{X'}^{-1} \circ p_1^*(i_{S'}) \circ \rho_X = p_2^*(\varphi) \circ p_2^*(i_{S'}) \circ \sigma_X$. But by the diagram above, the left-hand side is

$$\sigma_T \circ \rho_T^{-1} \circ p_1^*(\varphi \circ i_{S'}) \circ \rho_X$$

Therefore $\sigma_T \circ \rho_T^{-1} \circ p_1^*(\varphi \circ i_{S'}) = p_2^*(\varphi \circ i_{S'}) \circ \sigma_X \circ \rho_X^{-1}$ which tells us $\varphi \circ i_{S'}$ is a morphism between objects with descent data. This completes the proof of 5).

6) We observe that the solution which we know from 4) and 5) to exist at each local ring $\mathcal{O}_s$ can be prolonged to some neighborhood of s. See [E.G.A. IV 10.8.5]. By the uniqueness proved in part 3) these solutions can be patched together to give us a solution valid over all of S.

7) Since functoriality is obvious when S is a field, it follows formally from [E.G.A. IV 18.5.12] for the case when S is a complete Noetherian local ring. To know we can descend the morphism from S′ to S (in the notation used above) we use the fact that all faces except possibly the bottom one in the following diagram commute and that $p_1^*(i)$ is an epimorphism.



This gives us functoriality when S is a local ring. Now just as above, we extend this first to an open neighborhood of any point and finally to all of our scheme S.

Proposition (4.9) Let p be locally nilpotent on S and G be in B.T.(S). The following conditions are equivalent

1) $\overline{G}$ is a B.T. group.

2) G is an extension of an ind-étale B.T. group G'' by an ind-infinitesimal B.T. group G'.

2 bis) G is an extension of an ind-étale B.T. group by a p-divisible formal Lie group.

3) For all n $G(n)$ is an extension of a finite étale group by a finite locally-free radiciel group.

3 bis) $G(1)$ is an extension of a finite étale group by a finite locally free radiciel group.

4) $s \longmapsto$ separable rank $(G(1)_s)$ is a locally constant function.

Proof: 4) implies 3 bis) by the lemma, since the functoriality assertion together with the obvious fact that the construction of the scheme X' in the lemma commutes with products, tells us that if G is a group then the associated scheme G' is also a group and $G \longrightarrow G'$ is a homomorphism which is an epimorphism since it is faithfully flat.

It is clear that 3 bis) implies 4) since the separable rank of $G(1)$ at s will then be equal to the rank of the étale quotient of $G(1)$ at s and hence is certainly a locally constant function.

Obviously 3) implies 3 bis) and conversely 3 bis) implies 3) via 4) since the separable rank of $G(n)_s$ = (separable rank $G(1)_s)^n$ as follows from the exact sequences: $0 \longrightarrow G(n-1) \longrightarrow G(n) \xrightarrow{p^{n-1}} G(1) \longrightarrow 0$.

Now let us assume that 3) holds so that for each n we have an exact sequence: $0 \longrightarrow G'(n) \longrightarrow G(n) \longrightarrow G''(n) \longrightarrow 0$ with $G'(n)$ finite, locally free and radiciel, $G''(n)$ finite and étale. We will show that the systems $(G'(n))$ and $(G''(n))$ give us Barsotti-Tate groups. To do this it suffices to see that if $0 \longrightarrow G \longrightarrow H \longrightarrow K \longrightarrow 0$ is an exact sequence of finite locally-free groups satisfying the condition of the lemma, then the corresponding sequences of étale quotients or radiciel kernels are exact. But this will follow from (4.10) proved below. For by (4.10) and [E.G.A. IV 2.61(i), 2.7.1 (viii), 2.2.11 (iv)] it then suffices to check the corresponding when S is the spectrum of an algebraically closed field. But in this case it is obvious because for any finite group H we have $H=H^{o} \times H^{ét}$. Therefore by applying the above discussion to the sequences $0 \longrightarrow G(i) \longrightarrow G(n) \xrightarrow{p^i} G(n-i) \longrightarrow 0$ we see that $G' = \varinjlim G'(n)$ and $G'' = \varinjlim G''(n)$ are Barsotti-Tate groups. Furthermore by passage to the limit we see we have an exact sequence $0 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 0$ with G' ind-infinitesimal and G'' ind-étale. This shows that 3) implies 2).

2) implies 3) is trivial because from the exactness of the sequence $0 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 0$ follows that of $0 \longrightarrow G'(n) \longrightarrow G(n) \longrightarrow G''(n) \longrightarrow 0$ [I, 2.4.3]. 2) implies 2bis) is also clear because G' being ind-infinitesimal we have $G' = \overline{G'}$ and is therefore a formal Lie group by (3.3.18). Conversely let $0 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 0$ be an exact sequence with G' a p-divisible formal Lie group and G'' an ind-étale B.T. group. In order to show 2bis) implies 2) we must prove G' is a B.T. group. To do this

it suffices (because of (4.2)) to show $G'(1)$ is finite and locally free. But from our exact sequence we obtain a sequence $0 \to G'(1) \to G(1) \to G''(1) \to 0$ since G' is p-divisible. Therefore $G'(1)$ is finite and locally-free.

Finally it remains to show 1) and 2) are equivalent. To do this we shall utilize (4.11) which is proved below. Assuming 2) we have from (4.11) and (4.7) that $G' = \overline{G}$ and hence $\overline{G}$ is a Barsotti-Tate group. Conversely if $\overline{G}$ is a B.T. group then we can form the sequence $0 \to \overline{G} \to G \to G/\overline{G} \to 0$. From [I 2.4.3] we know $G/\overline{G}$ is a Barsotti-Tate group. But by (4.11) $\overline{(G/\overline{G})} = (0)$ and hence by (4.7) $G/\overline{G}$ is ind-étale. This completes the proof.

Lemma (4.10) Let $0 \to G \xrightarrow{i} H \xrightarrow{u} K \to 0$ be a complex of finite locally-free groups on S. The sequence is exact if and only if for all $s \in S$, the sequence $0 \to G_s \to H_s \to K_s \to 0$ is exact.

Proof: Only the "if" part requires proof. By the criterion for checking flatness fiber by fiber [E.G.A. IV 11.3.11] we know that $H \to K$ is an epimorphism if all maps $H_s \to K_s$ are epimorphisms. Thus it remains to prove the map $G \to \mathrm{Ker}(u)$ is an isomorphism. This can be checked locally on S and hence we can assume S is affine, say $S = \mathrm{Spec}(A)$, $G = \mathrm{Spec}(C)$, $\mathrm{Ker}(u) = \mathrm{Spec}(B)$ where B and C are projective (finitely generated) A-modules. To show $B \to C$ is an isomorphism it suffices to prove this at each point. Hence we can assume A is a local ring with maximal ideal $\underline{m}$. By hypothesis $B/\underline{m}B \to C/\underline{m}C$ is an isomorphism. By Nakayama (since C is finitely generated) the map $B \to C$ is surjective.

To show it is injective let W be its kernel. Then because C is projective the sequence $0 \longrightarrow W \longrightarrow B \longrightarrow C \longrightarrow 0$ splits and hence W is finitely generated since B is. But then we have $W/\underline{m}W = (0)$ and hence using Nakayama again we see $W = (0)$.

Lemma (4.11) Let p be locally nilpotent on S and let $0 \longrightarrow G_1 \longrightarrow G_2 \longrightarrow G_3 \longrightarrow 0$ be an exact sequence of Barsotti-Tate groups on S. Then $0 \longrightarrow \overline{G}_1 \longrightarrow \overline{G}_2 \longrightarrow \overline{G}_3 \longrightarrow 0$ is also exact.

Proof: The exactness of $0 \longrightarrow \overline{G}_1 \longrightarrow \overline{G}_2 \longrightarrow \overline{G}_3$ is trivial. We must prove $\overline{G}_2 \longrightarrow \overline{G}_3$ is an epimorphism. Let T be an S-scheme and $y \in \overline{G}_3(T)$ be given. Then because $G_2 \longrightarrow G_3$ is an epimorphism we can find a covering $\{T_i \longrightarrow T\}$ such that for each i, there is an x_i in $G_2(T_i)$ with the image of x_i being $y|T_i$. By passing to a covering of each T_i we can assume $y|T_i$ has the property that $y|\overline{T}_i = (0)$ where $\overline{T}_i \hookrightarrow T_i$ is a nilpotent immersion and T_i is affine. But this tells us that $x_i|\overline{T}_i$ belongs to $G_1(\overline{T}_i)$. Since G_1 is formally smooth by (3.3.13), we know there is an x_i' in $G_1(T_i)$ which lifts $x_i|\overline{T}_i$. Then $x_i - x_i' \in G_2(T_i)$ maps to $y|T_i$ and has its restriction to $\overline{T}_i$ equal to zero. Therefore $x_i - x_i' \in \overline{G}_2(T_i)$ and hence the map $\overline{G}_2 \longrightarrow \overline{G}_3$ is indeed an epimorphism.

Let A be an adic ring for the topology defined by the powers of an ideal I with I/I^2 of finite type over A/I. Set $A_n = A/I^{n+1}$, $S = \text{Spec } (A)$, $S_n = \text{Spec } (A_n)$.

Lemma (4.13): The natural functor Formal Lie Varieties (S) $\longrightarrow \varprojlim$ Formal Lie Varieties (S_n) is an equivalence of categories. In

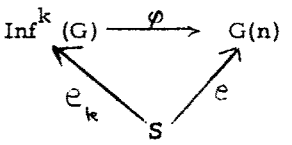
particular it induces an equivalence of categories between the category of formal Lie groups on S and the inverse limit of the categories of formal Lie groups on the various S_n's.

Proof: First observe that a formal Lie variety X on S can be thought of as the sheaf corresponding to the formal scheme $\mathrm{Spf}\,(\widehat{\mathrm{Sym}}[\underline{\omega}_X])$ where the symmetric algebra is completed with respect to the topology defined by powers of the augmentation ideal. Under this identification $X|S_n$ is identified with $\mathrm{Spf}\left(\mathrm{Sym}\,[\underline{\omega}_X \hat{\otimes}_A A_n]\right)$. But a mapping $Y \longrightarrow X$ of formal Lie varieties on S then corresponds to an A-linear map $\underline{\omega}_X \longrightarrow \mathrm{Sym}[\underline{\omega}_Y]^+ = \prod_{i=1}^{\infty} S^i[\underline{\omega}_Y]$ where the "+" denotes the augmentation ideal and $S^i[\underline{\omega}_Y]$ is the i^{th} symmetric power of $\underline{\omega}_Y$. Thus $\mathrm{Hom}\,(Y, X)$ is identified with

$$\prod_{i\geq 1} \mathrm{Hom}_A\,(\underline{\omega}_X, S^i[\underline{\omega}_Y]) = \prod_{i\geq 1} \varprojlim \mathrm{Hom}_{A_n}\,(\underline{\omega}_X \otimes A_n, S^i\,(\underline{\omega}_Y \otimes A_n))$$

[E.G.A. 0_{I} 7.2.10] $= \varprojlim \prod_{i\geq 1} \mathrm{Hom}_{A_n}\,(\underline{\omega}_X \otimes A_n, S^i\,(\underline{\omega}_Y \otimes A_n))$, as inverse limits commute. But this last is via the above simply identified with $\varprojlim \mathrm{Hom}\,(Y|S_n, X|S_n)$. Thus the functor is fully faithful. To show it is essentially surjective assume we are given a compatible family of formal Lie varieties X_n. Then we obtain a family of finite locally-free A_n-modules $\underline{\omega}_{X_n}$ with $\underline{\omega}_{X_n} \otimes A_{n-1} = \underline{\omega}_{X_{n-1}}$. But let $\underline{\omega} = \varprojlim \underline{\omega}_{X_n}$. $\underline{\omega}$ is of finite type over A by [E.G.A. 0 I 7.2.9]. But by [E.G.A. IV 18.3.2.1 (ii)] we know $\underline{\omega}$ is projective. But now it is clear that setting $X = \mathrm{Spf}\,(\widehat{\mathrm{Sym}}[\underline{\omega}])$ we have $X|S_n = X_n$ and hence our functor is indeed an equivalence of categories.

(4.14) Let us assume that p is nilpotent on S_o and let G belong to B.T. (S). Then for each n, we have the formal Lie group $\overline{G}_n$ and since these obviously are compatible we can by (4.13) define a formal Lie group $\overline{G}$. Thus we obtain a functor $G \mapsto \overline{G}$ from B.T. (S) $\longrightarrow$ Form Lie Gr.(S). But notice that we can not in general define a homomorphism $\overline{G} \longrightarrow G$ inducing the given map $\overline{G}_n \hookrightarrow G_n$ on S_n. To see this take $S = \text{Spec}(\mathbb{Z}_p)$ and let G be any Barsotti-Tate group on S. Then since $\overline{G} = \varinjlim \text{Inf}^k(G)$, any homomorphism $\overline{G} \longrightarrow G$ induces for each k a morphism of pointed sheaves $\text{Inf}^k(G) \longrightarrow G$. But as S is affine, any such morphism must factor through some $G(n)$. Thus we are led to examine a morphism of pointed schemes $\text{Inf}^k(G) \xrightarrow{\varphi} G(n)$. Thus we have a commutative diagram



and restricting to the generic fiber we still have such a diagram. But we know:

1) $\text{Inf}^k(G)$ is an infinitesimal thickening of S.

2) $G(n) \mid \mathbb{Q}_p$ is étale.

3) $\varphi \circ e_k = e \circ \pi_{\text{Inf}^k(G)} \circ e_k$.

Therefore $\varphi | \mathbb{Q}_p$ is the trivial map. But since φ corresponds to a mapping of free $\mathbb{Z}_p$-modules, it is determined by its restriction to the generic fiber. Thus φ is trivial and we see there is no non-zero way to

map $\overline{G}$ to G.

(4.15) Keeping the same notation as above, we see that the obvious functor from finite locally free groups on S to $\varprojlim$ fin. loc. free gr.(S_n) is an equivalence of categories, because such groups are given in terms of modules of finite type over the appropriate ring with additional structure making them into bi-algebras also defined in terms of the underlying modules. Thus using [E.G.A. 0_{I} 7.2.9, 7.2.10] and the criterion of flatness we obtain the equivalence. This equivalence preserves exact sequences. To see this observe that it suffices to treat the case of epimorphisms and show it is kernel preserving. For epimorphisms this follows from the fact that they can be expressed in terms of the bi-algebras of the groups. Thus if $G_n \longrightarrow H_n$ is an epimorphism of groups on S_n, then we have C_n is a finite locally free B_n-module for all n where $G_n = \text{Spec}\,(C_n)$, $H_n = \text{Spec}\,(B_n)$. But $B = \varprojlim B_n$ satisfies the same ring theoretic hypotheses made on A (for the ideal IB). Thus C is a finite locally free B-module $(C = \varprojlim C_n)$, and hence the morphism $G \longrightarrow H$, between the two groups associated to the families (G_n) and (H_n), is an epimorphism. The kernel preserving property is proved in an analogous manner using the fact that the kernel is expressed in terms of a tensor product of rings. But now it is clear, since exact sequences of the form $0 \longrightarrow G(i) \longrightarrow G(n) \xrightarrow{p^i} G(n-i) \longrightarrow 0$ are preserved under the equivalence, that we have the following lemma.

Lemma (4.16) The natural functor establishes an equivalence of categories B.T. $(S) \xrightarrow{\sim} \varprojlim$ B.T. (S_n).

This equivalence is clearly compatible with extensions. Thus, if we assume p is nilpotent on S_o and G is a B.T. group on S such that G_o satisfies the conditions of (4.9), we can associate to G an exact sequence $0 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 0$ with the property that G'_o is ind-infinitesimal (i.e., a formal Lie group by (4.9)) and with G'' ind-étale since each $G''(n)$ is étale by [E.G.A. IV 18.3.2].

Note that G' need not be ind-infinitesimal even though G'_o is. For example take a family of elliptic curves near a point where the Hasse invariant is zero. Then G_o is ind-infinitesimal while G is not. Thus even when $p = 0$ on S we can not say $G' = \overline{G}'$. The difficulty arises because the function $s \longmapsto$ separable rank $(G(1)_s)$ is not locally constant.

Chapter III. Divided Powers, Exponentials and Crystals

(1.0) Let A be a ring and I an ideal of A. Recall that I is said to be equipped with divided powers if we are given a family of mappings $\gamma_n : I \longrightarrow I$, $n \geq 1$ which satisfy the following conditions:

(1.0.1) $$\gamma_n(\lambda x) = \lambda^n \gamma_n(x), \qquad \lambda \in A, \quad x \in I$$

(1.0.2) $$\gamma_n(x) \cdot \gamma_m(x) = \frac{(m+n)!}{m!\, n!} \gamma_{m+n}(x)$$

(1.0.3) $$\gamma_n(x+y) = \gamma_n(x) + \sum_{i=1}^{n-1} \gamma_{n-i}(x)\, \gamma_i(y) + \gamma_n(y)$$

(1.0.4) $$\gamma_m(\gamma_n(x)) = \frac{(mn)!}{(n!)^m m!} \gamma_{mn}(x)$$

Given such a system we define γ_o via $\gamma_o(x) = 1$ for all $x \in I$ and refer to (I, γ) as an ideal with divided powers. Also the map γ_n is sometimes written as $x \longmapsto x^{(n)}$.

Definition (1.1) Given (A, I, γ) as above we say the divided powers are nilpotent if there is an N such that the ideal generated by elements of the form $\gamma_{i_1}(x_1) \ldots \gamma_{i_k}(x_k)$ $i_1 + \ldots + i_k \geq N$ is zero.

Remark (1.2) This is the definition of Berthelot [2, pg. 298]. Other variants (for example requiring that for each $x \in I$, there be an n depending on x such that $\gamma_i(x) = 0$ for $i \geq n$) are possible, but we shall use the condition (1.1). The definition implies (taking $k=N$, $i_1 = \ldots = i_N = 1$) that $I^N = (0)$.

Definition (1.3) Given an A-module M, $\Gamma(M)$ is the graded A-algebra generated by elements $m^{(n)}$, $m \in M$, $n \geq 1$ with the relations:

(1.3.1) $(\lambda m)^{(n)} = \lambda^n m^{(n)}$, $\lambda \in A$, $m \in M$

(1.3.2) $m^{(n)} m^{(n')} = \frac{(n+n')!}{n!\, n'!} m^{(n+n')}$

(1.3.3) $(m+m')^{(n)} = m^{(n)} + \sum_{n=1}^{n-1} m^{(n-i)} m'^{(i)} + m'^{(n)}$

Remark (1.4) We shall use (sometimes implicitly) the following properties of $\Gamma(M)$ which are proved by Roby [26, 27].

1) The map $M \longrightarrow \Gamma(M)$ given by $m \longmapsto m^{(1)}$ is an isomorphism of A-modules $M \xrightarrow{\sim} \Gamma^1(M)$.

2) There is a unique system of divided powers on the augmentation ideal $\Gamma^+(M) = \bigoplus_{n \geq 1} \Gamma^n(M)$ such that $\gamma_n(m) = m^{(n)}$ for all $m \in M$ and all $n \geq 1$.

3) Consider the category of augmented A-algebras B whose augmentation ideal B^+ is equipped with divided powers. Morphisms are of course to be compatible with the augmentations and with the divided power structures. Then the functor on this category $B \longmapsto \mathrm{Hom}_A(M, B^+)$ is represented by $\Gamma(M)$. This implies that $M \longmapsto \Gamma(M)$ is a functor commuting with filtering direct limits and with direct sums (i.e., $\Gamma(M \oplus N) \cong \Gamma(M) \otimes \Gamma(N)$).

4) The functor $M \longmapsto \Gamma(M)$ is compatible with a base change $A \longrightarrow A'$.

Definition (1.5) A morphism $u: (A, I, \gamma) \longrightarrow (B, J, \delta)$ is a ring homomorphism u such that $u(I) \subseteq J$ and $u(\gamma_n(x)) = \delta_n(u(x))$ holds for all $x \in I$.

(1.6) If the divided powers (A, I, γ) are nilpotent we define two maps:

$$\exp: I \longrightarrow (1+I)^*$$

$$\log: (1+I)^* \longrightarrow I$$

via the formulas $\exp(x) = \sum_{n \geq 0} \gamma_n(x)$ and $\log(1+x) = \sum_{n \geq 1} (-1)^{n-1}(n-1)!\ \gamma_n(x)$.

To check that exp and log are inverse we can clearly reduce to the "universal" case where $A = \hat{\Gamma_{\mathbb{Z}}}(\mathbb{Z})$, the completion being taken with respect to the filtration coming from the gradation on $\Gamma(\mathbb{Z})$. But then we are reduced to checking an assertion coefficient by coefficient. This means it suffices to verify the desired identities over $\mathbb{Q}$ (i.e., for the ring $\mathbb{Q}[[T]]$) and hence we win.

(1.7) The considerations of this section can all be globalized as follows: We replace A by a scheme S, I by a quasi-coherent ideal of $\mathcal{O}_S$, M by a quasi-coherent $\mathcal{O}_S$-module. Divided powers on I are given by assigning to each open set U a system of divided powers on $\Gamma(U, I)$ such that the restriction maps commute with the divided powers.

Given (S, I, γ) and (S', I', γ') a divided power morphism f between them is a morphism of schemes $f: S \longrightarrow S'$ such that $f^{-1}(I')$ maps into I under the map $f^{-1}(\mathcal{O}_{S'}) \longrightarrow \mathcal{O}_S$ and such that the divided powers induced on the image of $f^{-1}(I')$ "coincide" with those defined by γ'.

$\Gamma(M)$ is obtained by looking at the sheaf associated to the presheaf

$U \longmapsto \Gamma_{\mathcal{O}_S(U)}(M(U))$. The divided powers on $I \subseteq \mathcal{O}_S$ are said to be nilpotent if, locally on S, they satisfy the condition in Definition (1.1).

The following lemma was observed by Berthelot [2].

Lemma (1.8) Let (A, I, γ) be as above and assume that B is a flat A-algebra. The divided powers extend to the ideal $I \cdot B$.

Proof: We define a sequence $(\gamma'_n)_{n \geq 1}$ of mappings of $I \underset{A}{\otimes} B$ to itself via requiring that $\gamma'_n(i \otimes b) = \gamma_n(i) \otimes b^n$ and that these mappings satisfy the axioms for divided powers. To show this procedure works we proceed inductively. Obviously γ'_1 is well-defined as $id_{I \otimes B}$. Assume $\gamma'_1, \ldots, \gamma'_{n-1}$ have been defined so as to satisfy the above condition. Consider $I \times B$ and define a map $\varphi: A^{(I \times B)} \longrightarrow B$ via the formula

$$\varphi(a_1 (i_1, b_1) + \ldots + a_\ell (i_\ell, b_\ell))$$

$$= \sum (a_1 b_1)^{k_1} \gamma_{k_1}(i_1) \ldots (a_\ell b_\ell)^{k_\ell} \gamma_{k_\ell}(i_\ell)$$

where this sum runs over the ℓ-tuples $(k_1, \ldots, k_\ell)$ satisfying $k_j \geq 0$ and $\sum_{j=1}^{\ell} k_j = n$. As this map is to factor through $I \underset{A}{\otimes} B$, it must be shown that $\varphi(x+y) = \varphi(x)$ if y belongs to the kernel of $A^{(I \times B)} \longrightarrow I \otimes B$. This kernel is generated by elements of one of the following forms:

1) $(i_1 + i_2, b) - (i_1, b) - (i_2, b)$

2) $(i, b_1 + b_2) - (i, b_1) - (i, b_2)$

3) $(ai, b) - (i, ab)$

Thus it suffices to show that $\varphi(x+y) = \varphi(x)$ where y is an element of the form $a' \cdot z$ and z is either of types 1), 2), or 3). We shall deal with type 1) for example (the others being entirely similar).

Let $x = a_1(i_1, b_1) + \ldots + a_\ell(i_\ell, b_\ell)$ and $y = a'(i^* + i^{**}, b) - a'(i^*, b) - a'(i^{**}, b)$.

Since φ is well-defined we can obviously assume that $(i_1, b_1) = (i^* + i^{**}, b)$, $(i_2, b_2) = (i^*, b)$, $(i_3, b_3) = (i^{**}, b)$. (If this is not the case then we can put $0 \cdot (i^* + i^{**}, b)$ into our sum defining x without affecting the value of φ, etc.) Thus we must show

$$\varphi(a_1 + a'(i^* + i^{**}, b) + a_2 - a'(i^*, b) + a_3 - a'(i^{**}, b) + \ldots) = \varphi(x).$$

For every ℓ-tuple of indices which defines a term in either of the sums, the factors appearing after the third in the corresponding term are identical. Hence to show $\varphi(x+y) = \varphi(x)$ it is sufficient to show that for any fixed t we have:

$$\sum_{k_1+k_2+k_2=t} ((a_1+a')b)^{k_1} \gamma_{k_1}(i^*+i^{**})((a_2-a')b)^{k_2} \gamma_{k_2}(i^*)((a_3-a')b)^{k_3} \gamma_{k_3}(i^{**})$$

$$= \sum_{k_1+k_2+k_3=t} (a_1 b)^{k_1} \gamma_{k_1}(i^*+i^{**})(a_2 b)^{k_2} \gamma_{k_2}(i^*)(a_3 b)^{k_3} \gamma_{k_3}(i^{**})$$

But the first sum is

$$b^t \sum_{k_1+k_2+k_2=t} \gamma_{k_1}(a_1+a'(i^*+i^{**})) \cdot \gamma_{k_2}[(a_2-a')i^*] \gamma_{k_3}[a_3-a'(i^{**})]$$

$$= b^t \cdot \gamma_t[(a_1+a_2)\, i^* + (a_1+a_3)\, i^{**})]$$

which is obviously the same as the second sum. This shows that φ

factors through $I \underset{A}{\otimes} B$ and enables us to define γ'_n via composing φ with the inverse of the map $I \underset{A}{\otimes} B \longrightarrow IB$ (using the flatness of B over A). It is now obvious that the sequence of maps (γ'_n) define "divided powers" on $I \underset{A}{\otimes} B$ and hence by transport of structure (as $I \otimes B \xrightarrow{\sim} IB$) we obtain the desired divided powers on I·B.

§2. (2.0) Let S be a scheme and U a quasi-coherent $\mathcal{O}_S$ co-algebra which is co-commutative. Recall that this means we have two $\mathcal{O}_S$-linear maps $\Delta: U \longrightarrow U \otimes U$ and $\eta: U \longrightarrow \mathcal{O}_S$ satisfying identities which are obtained by reversing the arrows in the diagrams which define a commutative algebra.

Definition (2.1) Cospec (U) is the functor $(Sch/S)^{\circ} \longrightarrow$ Sets given by $S' \longmapsto \{y \in \Gamma(S', U_{S'}) \mid \eta(y) = 1, \Delta(y) = y \otimes y\}$.

It is clear that Cospec (U) is a sheaf for the f.p.q.c. topology because by descent $S' \longmapsto \Gamma(S', U_{S'})$ is a sheaf [S.G.A. 1 VIII, 1.7] and the above subset is obviously stable under descent conditions. Thus we obtain a covariant functor $U \longmapsto$ Cospec (U) from the category of (co-commutative) $\mathcal{O}_S$ co-algebras to the category of f.p.q.c. sheaves on S. This functor is obviously compatible with inverse images.

(2.1.1) Recall the category of co-algebras has finite products: Given U and V, two co-algebras, the underlying module of their product is $U \otimes V$. The two projections are $id_U \otimes \eta_V$ and $\eta_U \otimes id_V$ while the "co-product" morphism is given by the following composition where τ denotes

the interchange of factors map:

$$U \otimes V \xrightarrow{\Delta_U \otimes \Delta_V} U \otimes U \otimes V \otimes V \xrightarrow{id \otimes \tau \otimes id} U \otimes V \otimes U \otimes V.$$

Given W, a third co-algebra, and two morphisms

$$f: W \longrightarrow U, g: W \longrightarrow V; (f,g): W \longrightarrow U \otimes V$$

is $(f \otimes g) \circ \Delta_W$.

This allows us to see that Cospec $(U \otimes V) \xrightarrow{\sim}$ Cospec $(U) \times$ Cospec (V) because $\Gamma(S', \text{Cospec } (U)) = \text{Hom}_{\mathcal{O}_{S'}\text{-co-alg.}} (\mathcal{O}_{S'}, U_{S'})$ via the identification which associates to $\varphi: \mathcal{O}_{S'} \longrightarrow U_{S'}$, the element $\varphi(1) \in \Gamma(S', U_{S'})$.

(2.1.2) If A is a finite locally-free $\mathcal{O}_S$ algebra, then $\check{A} = \underline{\text{Hom}}(A, \mathcal{O}_S)$ is a co-algebra. We have a natural identification Cospec $(\check{A}) \xrightarrow{\sim}$ Spec(A) via $\Gamma(S', \text{Cospec } (\check{A})) = \text{Hom}_{\mathcal{O}_{S'}\text{-co-alg.}} (\mathcal{O}_{S'}, \check{A}_{S'}) = \text{Hom}_{\mathcal{O}_{S'}\text{ alg.}} (A_{S'}, \mathcal{O}_{S'})$ $= \Gamma(S', \text{Spec } (A))$.

Hence Cospec $(\check{A})$ is representable and the category of finite locally-free S-schemes is equivalent to the category of finite locally-free (co-commutative) $\mathcal{O}_S$ co-algebras.

(2.1.3) Let $U = \varinjlim U_i$ be a filtered direct limit of co-algebras. Then $\varinjlim$ Cospec $(U_i) \xrightarrow{\sim}$ Cospec (U). To check this it is sufficient to look at sections over an affine S' which maps into an affine open subset of S. This reduces us to the assertion in the affine case. But if $y \in U$ satisfies $\eta(y) = 1$ and $\Delta(y) = y \otimes y$ and if $y' \in U_i$ is a representative of y, then $\eta(y') = 1$ and $\Delta(y') - y' \otimes y'$ is mapped to zero in $U \otimes U$. Thus there is a $j \geq i$ such that the image of y' in U_j satisfies the two conditions.

From the above we know a filtered direct limit of finite locally-free S-schemes is given by Cospec (U) for an appropriate $\mathcal{O}_S$ co-algebra U. If $\mathcal{C}_f$ is the category of finite locally-free $\mathcal{O}_S$ co-algebras and $\mathcal{C} = \text{ind}\,(\mathcal{C}_f)$, then by (2.1.2) we have an equivalence of $\mathcal{C}$ with ind (finite locally-free S-schemes). The functor $\varinjlim$ is faithful from ind (finite locally-free S-schemes) to sheaves on S. Furthermore if S is affine then this functor is full. Because Hom (U, V) and Hom (Cospec (U), Cospec (V)) are the sets of global sections of locally isomorphic sheaves we see that the functor is full without any hypothesis on S. Thus the category of $\mathcal{O}_S$ co-algebras which are filtering direct limits of finite locally-free co-algebras is equivalent to the category of sheaves on S which are filtering direct limits of finite locally-free S-schemes. In particular either a Barsotti-Tate group or a formal Lie variety can be written as Cospec (U) for an appropriate co-algebra U.

(2.1.4) Let M be a quasi-coherent $\mathcal{O}_S$ module and $\Gamma(M)$ the associated divided power algebra [(1.6)]. The diagonal map $\Delta: M \longrightarrow M \oplus M$ and the zero map $M \longrightarrow (0)$ give rise by functoriality to morphisms $\Gamma(M) \xrightarrow{\Delta} \Gamma(M) \otimes \Gamma(M)$ and $\Gamma(M) \xrightarrow{\eta} \mathcal{O}_S$ which make $\Gamma(M)$ into an $\mathcal{O}_S$ co-algebra. Recall that $M \longmapsto \Gamma(M)$ is compatible with all base changes [(1.4), 4]. We come to our first instance of an "exponential" map.

Definition (2.1.5) $\overline{M}$ is the sheaf on S whose sections over an S-scheme S′ are given by

$$\Gamma(S', \overline{M}) = \mathrm{Ker}\left[\Gamma(S', M_{S'}) \longrightarrow \Gamma\left(S'_{red}, M_{S'_{red}}\right)\right].$$

Remark (2.1.6) The fact that $\overline{M}$ is a sheaf is a consequence of the fact that it can also be described as the image in M of the sheaf $\mathrm{Nilrad} \otimes M$ (where M is thought of as an f.p.q.c. sheaf in the obvious way [S.G.A., 1 VIII 1.7] and Nilrad denotes the sheaf $S' \longmapsto \Gamma(S', \mathrm{Nil}(\mathcal{O}_{S'}))$).

We can think of $\overline{M}$ as being the "formal group" associated to M. Indeed, if $M = \mathcal{O}_S$, then $\overline{M} = \overline{G}_a$.

Definition (2.1.7) $\exp_M : \overline{M} \longrightarrow \mathrm{Cospec}(\Gamma(M))$ is the mapping given by $\exp_M(m) = \sum_{n \geq 0} m^{(n)}$.

To check that this definition makes sense it suffices to look at the case $S = \mathrm{Spec}(A)$, $S' = \mathrm{Spec}(A')$. Then $m \in M \underset{A}{\otimes} A'$ can be written as $\sum_{i=1}^{r} m_i \otimes \lambda_i$ where the λ_i's are nilpotent. If $\lambda_i^N = 0$ for $i=1, \ldots, r$ then $m^{(n)} = 0$ if $n > Nr$. This shows that the series terminates and thus $\exp_M$ is well-defined locally and hence is really well-defined. A priori we have $\exp_M(m) \in \Gamma(S', \Gamma(M) \otimes \mathcal{O}_{S'})$ but it is clear that $\exp_M(m)$ actually lies in $\Gamma(S', \mathrm{Cospec}(\Gamma(M)))$.

Recall that M being an abelian group in the category of $\mathcal{O}_S$-modules, $\Gamma(M)$ is an abelian group in the category of $\mathcal{O}_S$ co-algebras and hence $\mathrm{Cospec}(\Gamma(M))$ is an abelian sheaf on S. Explicitly μ, the multiplication map making $\Gamma(M)$ an algebra is, when viewed as a co-algebra map $\Gamma(M) \otimes \Gamma(M) \longrightarrow \Gamma(M)$, the map defining the addition law on $\mathrm{Cospec}(\Gamma(M))$.

Since we have $\exp_M(m+m') = \sum (m+m')^{(n)} = (\sum m^{(n)}) \cdot (\sum (m')^{(n)})$, $\exp_M : \overline{M} \longrightarrow \text{Cospec}(\Gamma(M))$ is an additive map.

Proposition (2.1.8) If M is flat, then $\exp_M$ is an isomorphism.

Proof: Since we are dealing with sheaves it suffices to prove the statement locally. Thus we assume $S = \text{Spec}(A)$, $S' = \text{Spec}(A')$, I = nilradical of A', $M' = M \underset{A}{\otimes} A'$. We must show $\exp_M : IM' \longrightarrow \{y \in \Gamma(M') \mid \eta(y) = 1,\ \Delta(y) = y \otimes y\}$ is an isomorphism. The injectivity is clear because $\exp_M(\sum \lambda_i m_i) = 1 + \sum \lambda_i m_i + \sum \lambda_i m_i)^{(2)} + \ldots$ where $\lambda_i \in I$. To prove surjectivity we use Lazard's result that M can be written as $\varinjlim F_i$ where the F_i are free of finite type [18]. Then $\overline{M} = \varinjlim \overline{F}_i$, $\Gamma(M) = \varinjlim \Gamma(F_i)$ [1.4.3], $\text{Cospec}(\Gamma(M)) = \varinjlim \text{Cospec}(\Gamma(F_i))$ [2.1.3], $\text{Cospec}(\Gamma(F_i)) \cong \text{Cospec}(\Gamma(A) \otimes \cdots \otimes \Gamma(A))$ if $F_i \cong \oplus A$ [1.4.3], $\text{Cospec}(\Gamma(A) \otimes \cdots \otimes \Gamma(A)) \cong \text{Cospec}(\Gamma(A)) \times \cdots \times \text{Cospec}(\Gamma(A))$ [2.1.1]. Since $\exp_M$ is functorial in M, this reduces us to the case $M = A$. But now $\Gamma(A') = A' \oplus A'x_1 \oplus A'x_2 \oplus \ldots$ where $x_i x_j = \binom{i+j}{i} x_{i+j}$ and $\Delta(x_n) = 1 \otimes x_n + \sum_{i=1}^{n-1} x_i \otimes x_{n-i} + x_n \otimes 1$. Thus if $y = 1 + a_1 x_1 + a_2 x_2 + \ldots + a_n x_n$ is such that $\Delta(y) = y \otimes y$ we have $a_i = a_1^i$ and hence $a_1^{n+1} = 0$. Thus $\exp_M(a_1 x_1) = y$ and the map is surjective.

Remark (2.1.9) The following example shows that the flatness assumption can not be eliminated. Let A be an integral domain and B a non-reduced quotient of A. Then $\overline{B}(A) = 0$ while $\Gamma(A, \text{Cospec}(B))$ has elements such as $1 + \overline{a}_1 \cdot 1_B + \overline{a}_1^2 1_B^{(2)} + \ldots$ where $\overline{a}_1$ is a non-zero

nilpotent element in B.

Remark (2.10) Cospec ($\Gamma(M)$) is naturally equipped with a structure of $\underline{\mathcal{O}}_S$-module and $\exp_M$ is a homomorphism of $\underline{\mathcal{O}}_S$-modules. Indeed if $y = \sum y^{(i)} \in \Gamma(M)$ is such that $\Delta(y) = y \otimes y$ and $\eta(y) = 1$, then $\lambda \cdot y = \sum \lambda^i y^{(i)}$ satisfies the same conditions.

(2.2) Let U be an augmented co-algebra on S. This means we have a co-algebra map $\mathcal{O}_S \xrightarrow{\epsilon} U$ and hence $\epsilon(1_{\mathcal{O}_S}) = 1_U$ will be a distinguished element in $\Gamma(S, \text{Cospec } (U))$.

Definition (2.2.1) A section x of U is said to be primitive if $\Delta(x) = x \otimes 1 + 1 \otimes x$. This implies $\eta(x) = 0$ for $(id_U \otimes \eta) \circ \Delta = id_U$ and hence $x \cdot \eta(1) + \eta(x) \cdot 1 = x$. But $\eta(1) = 1_{\mathcal{O}_S}$ and thus $\eta(x) \cdot 1 = 0$ which implies $\eta(\eta(x) \cdot 1) = \eta(x) \cdot \eta(1) = \eta(x) = 0$.

We denote by Lie (U) the sheaf of $\underline{\mathcal{O}}_S$-modules whose sections over S' are the primitive elements in $\Gamma(S', U_{S'})$ and where the operations are induced by those on the underlying module of U.

Example (2.2.2) Let U be finite and locally-free and $X = \text{Cospec } (U) = \text{Spec } (\check{U})$. Then Lie (U) = $V(\underline{\omega}_X)$ = Lie (X), where $\underline{\omega}_X$ is defined via the section $e: S \longrightarrow X$ corresponding to the augmentation ϵ, and where V applied to an arbitrary $\mathcal{O}_S$-module M is the $\underline{\mathcal{O}}_S$-module $S' \longmapsto \text{Hom}_{\mathcal{O}_{S'}}(M_{S'}, \mathcal{O}_{S'})$. More generally this description is valid if $U = \varinjlim U_i$ a filtered direct limit with U_i finite locally-free and augmented and the transition morphisms compatible with the augmentations. In particular it

applies if Cospec (U) is a formal Lie variety.

(2.2.3) Let $S_o \hookrightarrow S$ be an immersion defined by an ideal I with nilpotent divided powers. Let U be a flat $\mathcal{O}_S$-bi-algebra (i.e., an augmentated co-algebra together with a co-algebra map $\mu: U \otimes U \longrightarrow U$ and a co-algebra map $c: U \longrightarrow U$ such that μ, ε, c make U a commutative group in the category of co-algebras). By (1.8), the ideal $I \cdot U$ in the algebra U has divided powers extending those on I. Since $I \cdot \underline{Lie}(U) \subseteq I \cdot U \cap \underline{Lie}(U)$, the divided powers of sections of $I \cdot \underline{Lie}(U)$ are defined. If V is a second flat bi-algebra and $\varphi: U \longrightarrow V$ is an algebra map then φ is compatible with the divided powers on $I \cdot U$. In particular taking $V = U \otimes U$ we see Δ is compatible with the divided powers. Let x be a section of $\underline{Lie}(U) \cap I \cdot U$ and define exp (x) to be $\sum_{n \geq 0} x^{(n)}$. The sum makes sense because the divided powers on I are nilpotent. Since

$$\Delta(\exp(x)) = \Delta(\sum x^{(n)}) = \sum (\Delta(x))^{(n)} = \sum (x \otimes 1 + 1 \otimes x)^{(n)}$$

$$= \sum_{i,j \geq 0} (x \otimes 1)^{(i)} (1 \otimes x)^{(j)} = \sum_{i,j \geq 0} (x^{(i)} \otimes 1)(1 \otimes x^{(j)}) = \exp(x) \otimes \exp(x),$$

it is clear that exp (x) determines an element of $\Gamma(S, \text{Cospec}(U))$. Let us restrict this map to $I \cdot \underline{Lie}(U) \subseteq \underline{Lie}(U) \cap I \cdot U$ so to obtain:

$$\exp: \Gamma(S, I \cdot \underline{Lie}(U)) \longrightarrow \Gamma(S, \text{Cospec}(U))$$

is additive. Furthermore the image of exp must lie in $\text{Ker}[\Gamma(S, \text{Cospec}(U)) \longrightarrow \Gamma(S_o, \text{Cospec}(U))]$ because $S_o = \text{Var}(I)$. Thus we have the following lemma:

Lemma (2.2.4) Let $S_o \hookrightarrow S$ be an immersion defined by an ideal with nilpotent divided powers and let U be a flat $\mathcal{O}_S$ bi-algebra. The map $\exp: \Gamma(S, I\cdot \underline{Lie}(U)) \longrightarrow \Gamma(S, \text{Cospec}(U))$ defined by $\exp(x) = \sum x^{(n)}$ is a homomorphism whose image lies in $\text{Ker}\,[\Gamma(S, \text{Cospec}(U)) \longrightarrow \Gamma(S_o, \text{Cospec}(U))]$.

Lemma (2.2.5) Assume (in the notation of (2.2.4)) that $U/\underline{Lie}(U)$ is a flat $\mathcal{O}_S$ module. Then $\exp: \Gamma(S, I\cdot\underline{Lie}(U)) \longrightarrow \text{Ker}\,[\Gamma(S, \text{Cospec}(U)) \longrightarrow \Gamma(S_o, \text{Cospec}(U))]$ is an isomorphism.

Proof: Without hypothesis on $U/\underline{Lie}(U)$ observe we can define a map $\log: \text{Ker} \longrightarrow I\cdot U \cap \underline{Lie}(U)$ via $\log(1+y) = \sum_{n\geq 1} (-1)^{n-1}(n-1)!\, y^{(n)}$. The map is defined since y belongs to $I\cdot U$. $\log(1+y)$ lies in $\underline{Lie}(U)$ since log is a functorial mapping and $\Delta(1+y) = (1+y)\otimes(1+y)$. Thus we see exp and log are inverse isomorphisms between $\Gamma(S, I\cdot U \cap \underline{Lie}(U))$ and $\text{Ker}\,[\Gamma S, \text{Cospec}(U)) \longrightarrow \Gamma(S_o, \text{Cospec}(U))]$. But the flatness hypothesis insures that $I\cdot U \cap \underline{Lie}(U) = I\cdot \underline{Lie}(U)$ [4, Chapter I, §2 #6 Corollaire].

Remark (2.2.6) We note explicitly the fact mentioned in the proof that there is always an isomorphism $\underline{Lie}(U) \cap I\cdot U \xrightarrow{\sim} \text{Ker}\,[\Gamma(S, \text{Cospec}(U)) \longrightarrow \Gamma(S_o, \text{Cospec}(U))]$, U of course being assumed flat.

(2.2.7) Note the above discussion will apply if U is the hyperalgebra of a formal Lie group or a Barsotti-Tate group or more generally of a group G which can be written as a filtering direct limit of finite locally-free S-schemes (2.1.3).

(2.3) Let S be a scheme, I an ideal of $\mathcal{O}_S$ with divided powers, U a flat bi-algebra on S and M a quasi-coherent $\mathcal{O}_S$-module. Consider the $\mathcal{O}_S$-algebra $\mathcal{O}_S \oplus I \cdot U$. It is obvious that the set of $\mathcal{O}_S$-algebra homomorphisms $\Gamma(M) \longrightarrow U$ which send $\Gamma^+(M)$ into $I \cdot U$ and which are compatible with the divided powers is in bijective correspondence with the set of divided power homomorphisms of augmented $\mathcal{O}_S$-algebras $\Gamma(M) \longrightarrow \mathcal{O}_S \oplus I \cdot U$. By (1.4) part 3, this last set is simply $\mathrm{Hom}_{\mathcal{O}_S}(M, I \cdot U)$. Let $u: \Gamma(M) \longrightarrow U$ be a map compatible with divided powers (so that $u(\Gamma^+(M)) \subset I \cdot U$). Let $\theta: M \longrightarrow I \cdot U$ be the corresponding linear map. Then it is clear that u is compatible with the augmentations if and only if $\theta(M) \subseteq I \cdot U \cap U^+ = I \cdot U^+$ (since $U/U^+ = \mathcal{O}_S$ is flat over S). For u to be compatible with the co-product mappings Δ, it is necessary and sufficient that $\Delta(u(m)) = u \otimes u\,(\Delta(m))$ since M generates $\Gamma(M)$. But $\Delta(m) = m \otimes 1 + 1 \otimes m$ and hence $\Delta(\theta(m)) = \Delta(u(m)) = u(m) \otimes 1 + 1 \otimes u(m) = \theta(m) \otimes 1 + 1 \otimes \theta(m)$ is the necessary and sufficient condition. Hence we can say u is a bi-algebra map if and only if $\theta \in \mathrm{Hom}\,(M, \underline{\mathrm{Lie}}(U) \cap I \cdot U^+)$.

Lemma (2.3.1) The above correspondence $\theta \longmapsto u$ establishes an isomorphism between $\mathrm{Hom}\,(M, \underline{\mathrm{Lie}}(U) \cap I \cdot U)$ and the group of bi-algebra homomorphisms, u, such that $u(\Gamma^+(M)) \subseteq I \cdot U$ and such that u is compatible with divided powers.

Proof: We have already defined a set-theoretic bijection. To show that the above bi-algebra homomorphisms constitute a group and that $\theta \longmapsto u$ is an isomorphism, it suffices to show $\theta \longmapsto u$ is additive. If

$\theta \longmapsto u$ and $\theta' \longmapsto u'$, then $u + u'(m) = \mu \circ (u \otimes u')(\Delta(m)) = u(m) + u'(m)$ and it is clear that $\theta + \theta'$ corresponds to this homomorphism.

Remark (2.3.2) The target of the above isomorphism is contained in $\mathrm{Ker}\,[\mathrm{Hom}_{\mathcal{O}_S\text{-bi-alg.}}(\Gamma(M), U) \longrightarrow \mathrm{Hom}_{\mathcal{O}_{S_o}\text{-bi-alg.}}(\Gamma(M_o), U_o)]$ where M_o and U_o denote the respective restrictions of M and U to $S_o = \mathrm{Var}(I)$. Also there is an evident functoriality in the above construction.

(2.3.3) Assume that M is flat. Let $G = \mathrm{Cospec}\,(U)$. Recall that $\overline{M} \xrightarrow{\sim} \mathrm{Cospec}\,(\Gamma(M))$ [2.1.8]. Thus we have defined a monomorphism:

(2.3.3.1) $\mathrm{Hom}(M, \underline{\mathrm{Lie}}(G) \cap I \cdot U) \hookrightarrow \mathrm{Ker}[\mathrm{Hom}_{S\text{-gr.}}(\overline{M}, G) \to \mathrm{Hom}_{S_o\text{-gr.}}(\overline{M}_o, G_o)]$

We make the map explicit as follows: Let $\theta: M \longrightarrow \underline{\mathrm{Lie}}(G) \cap I \cdot U$ and let u correspond to θ as in (2.3). Thus u defines a homomorphism $\mathrm{Cospec}\,(\Gamma(M)) \longrightarrow G$ and by composing with the isomorphism $\overline{M} \xrightarrow{\sim} \mathrm{Cospec}\,(\Gamma(M)$ we obtain our desired morphism $u' = u \circ \exp_M$. The map $\overline{M}(S) \longrightarrow G(S)$ can be written as $u'(x) = u(\sum x^{(n)} = \sum (\theta(x))^{(n)}$ where this last sum makes sense since $\theta(x) \in \mathrm{Nil}(\mathcal{O}_S) \cdot I \cdot U$. Thus we can write $u'(x) = \exp(\theta(x))$.

Intuitively we can think of an u' in

$$\mathrm{Ker}\,[\mathrm{Hom}_{S\text{-gr.}}(\overline{M}, G) \longrightarrow \mathrm{Hom}_{S_o\text{-gr.}}(\overline{M}_o, G_o)]$$

as having a tangent mapping $\theta: M \longrightarrow \underline{\mathrm{Lie}}(G) \cap I \cdot U$ and thus we think of certain u''s as being the exponentials of their tangent mappings (i.e., $u' = \exp(\theta)$).

(2.3.4) Let $U = \Gamma(N)$ where N is a flat $\mathcal{O}_S$-module. We have $\underline{\mathrm{Lie}}\,(G) = \underline{\mathrm{Lie}}\,(\mathrm{Cospec}\,(\Gamma(N))) = N$ (as is seen immediately by reducing to the affine case, writing $N = \varinjlim L_i$ each L_i free of finite type, . . . , and eventually observing that the assertion is trivial if $N = \mathcal{O}_S$). In this case we have $\underline{\mathrm{Lie}}\,(G) \cap I \cdot \Gamma(N) = I \cdot \underline{\mathrm{Lie}}\,(G) = I \cdot N$. If $\theta: M \longrightarrow I \cdot N$, $\exp(\theta): \Gamma(M) \longrightarrow \Gamma(N)$ is the natural prolongation of $\theta: M \longrightarrow N$. This follows because the divided powers on $I \cdot N \subseteq I \cdot \Gamma(N)$ arising from those on I, coincide with the divided powers on $I \cdot N$ coming from those on $\Gamma^+(N)$: $(i\,n)^{(j)} = i^{(j)}\, n^j = i^{(j)}\, j!\, n^{(j)} = i^j n^{(j)}$. Hence the map $\overline{M} \longrightarrow \overline{N}$ corresponding to θ is the obvious prolongation of $\theta: M \longrightarrow N$. Clearly this map respects the module structures.

Remark (2.3.5) If $U/\underline{\mathrm{Lie}}\,(U)$ is flat then we will have $\underline{\mathrm{Lie}}(U) \cap I \cdot U = I \cdot \underline{\mathrm{Lie}}\,(U)$ and the homomorphism (2.3.3.1) can be written as

$$\mathrm{Hom}\,(M,\ I \cdot \underline{\mathrm{Lie}}\,(G)) \hookrightarrow \mathrm{Ker}\,[\mathrm{Hom}(\overline{M}, G) \longrightarrow \mathrm{Hom}\,(\overline{M}_o,\ G_o)]$$

Remark (2.3.6) Let $G = \mathrm{Spec}\,(B)$ be a finite locally-free group scheme and assume that ω_G is locally-free. Then $B^\vee/\underline{\mathrm{Lie}}\,(G)$ is flat. To see this observe that it suffices by [E.G.A. IV 11.9.18] to know the map $\underline{\mathrm{Lie}}\,(G) \longrightarrow B^\vee$ is universally injective. But after an arbitrary base change $S' \longrightarrow S$, $\underline{\mathrm{Lie}}(G) \otimes_{\mathcal{O}_S} \mathcal{O}_{S'} = \underline{\mathrm{Lie}}\,(G_{S'})$ and hence the map is clearly injective.

Remark (2.3.7) Let U and V be two pointed co-algebras over a ring A. Let I be an ideal in A with $I^2 = (0)$. Assume that $I \cdot U \cap \underline{\mathrm{Prim}}(U) =$

$I \cdot \underline{\text{Prim}}\,(U)$ and similarly for V.

Claim: $U \otimes V$ has the same property.

Proof: Let $A[\epsilon]$ be the pointed co-algebra which is the linear dual of the "dual numbers" so that it has a base $\{1, \epsilon\}$ $\Delta(1) = 1 \otimes 1$, $\Delta(\epsilon) = \epsilon \otimes 1 + 1 \otimes \epsilon$, $\eta(1) = 1$, $\eta(\epsilon) = 0$. It is obvious that to give a homomorphism of pointed co-algebras $A[\epsilon] \longrightarrow U$ we simply have to tell the image of ϵ which must be primitive. Therefore on the category of pointed co-algebras the functor $U \longmapsto \underline{\text{Prim}}\,(U)$ is represented by $A[\epsilon]$. Clearly this category admits a product (namely the ordinary product of two co-algebras with the obvious "pointing"). Hence:

$$\underline{\text{Prim}}\,(U \otimes V) = \operatorname{Hom}_{\text{pt.-co-algebras}}(A[\epsilon],\ U \otimes V)$$

$$= \operatorname{Hom}(A[\epsilon], U) \times \operatorname{Hom}(A[\epsilon],\ V)$$

$$= \underline{\text{Prim}}\,(U) \times \underline{\text{Prim}}\,(V).$$

Thus the map $\underline{\text{Prim}}\,(U \otimes V) \longrightarrow \underline{\text{Prim}}\,(U) \times \underline{\text{Prim}}\,(V)$ of components $\mathrm{id}_U \otimes \eta_V$ and $\eta_U \otimes \mathrm{id}_V$ is an isomorphism. Let $u \in \underline{\text{Prim}}\,(U)$ and $v \in \underline{\text{Prim}}\,(V)$. The element $u \otimes 1 + 1 \otimes v$ is primitive and maps to the pair (u, v) under the isomorphism. This means any primitive element of $U \otimes V$ can be uniquely written as $u \otimes 1 + 1 \otimes v$ as above.

Let $x = u \otimes 1 + 1 \otimes v$ belong to $I \cdot (U \otimes V) \cap \underline{\text{Prim}}\,(U \otimes V)$. This implies $u = \mathrm{id}_U \otimes \eta_V\,(x) \in I \cdot U \cap \underline{\text{Prim}}\,(U)$ and hence $u = \sum i_\alpha u_\alpha$ with $u_\alpha \in \underline{\text{Prim}}(U)$, $i_\alpha \in I$. Similarly write $v = \sum i'_\beta v_\beta$. Then $x = \sum i_\alpha (u_\alpha \otimes 1 + 1 \otimes v) + \sum i'_\beta (u \otimes 1 + 1 \otimes v_\beta)$ since the $i_\alpha \cdot (1 \otimes v)$ and $i'_\beta (u \otimes 1) = 0$ because of

the hypothesis $I^2 = (0)$.

(2.4) So far we have (under appropriate circumstances) associated to a linear map $\theta: M \longrightarrow I \cdot \underline{Lie}(G)$ an element $u = \exp(\theta)$ in $\mathrm{Ker}\,[\mathrm{Hom}\,(\overline{M}, G) \longrightarrow \mathrm{Hom}\,(\overline{M}_o, G_o)]$. We now investigate the question of when $\overline{M}$ (resp. $\overline{M}_o$) can be replaced by M (resp. M_o). For simplicity assume $S = \mathrm{Spec}\,(A)$ is affine (this is the only case used later). Let $I \subseteq A$ be an ideal with nilpotent divided powers and let $A_o = A/I$, $S_o = \mathrm{Spec}\,(A_o)$. Let G be a group on S and V a locally-free of finite type $\mathcal{O}_S$-module. Assume $\overline{G} = \varinjlim \mathrm{Inf}^k(G)$ is Cospec (U) for a flat augmented co-algebra U and that all $\mathrm{Inf}^k(G)$ are finite and locally-free. Let $\theta: V \longrightarrow I \cdot \underline{Lie}\,(U)$ be given. Then θ corresponds to a $u: \Gamma(V) \longrightarrow U$ given by $u(x) = \sum (\theta(x))^{(n)}$ for $x \in V$. Because the divided powers on I are nilpotent u will map $\bigoplus_{i \geq n} \Gamma^i(V)$ to zero if n is sufficiently large. Thus u can be extended to the completion $\hat{\Gamma}(V)$ of $\Gamma(V)$. If $\mathrm{Inf}^k(G) = \mathrm{Spec}\,(B_i)$ so that $U = \varinjlim B_i^{\vee}$ then $\overline{G} = \mathrm{Spf}\,(\varprojlim B_i)$ where each B_i is given the discrete topology. Since $\overline{G}$ is a group, $B = \varprojlim B_i$ is a "topological" bi-algebra (i.e., $\hat{\otimes}$ replaces $\otimes$ in the ordinary bi-algebra axioms). By taking the transpose of $u: \hat{\Gamma}(V) \longrightarrow U$ we find a bi-algebra mapping $B \longrightarrow \mathrm{Sym}\,(\check{V})$ and this defines a group homomorphism $V \longrightarrow \overline{G}$. Since given $u: \hat{\Gamma}(V) \longrightarrow U$, the taking of its transpose commutes with the base change $A \longrightarrow A_o$, we see that the induced homomorphism $V_o \longrightarrow \overline{G}_o$ is trivial. Thus we have defined a mapping:

$$\mathrm{Hom}\,(V,\ I \cdot \underline{Lie}\,(G)) \hookrightarrow \mathrm{Ker}\,[\mathrm{Hom}\,(V, G) \longrightarrow \mathrm{Hom}\,(V_o, G_o)].$$

The fact that it is additive and injective comes from the fact that $\theta \longmapsto u$ had these properties.

Notice the above construction is valid if G is a smooth group scheme over S, if G is a formal Lie group or if G is a Barsotti-Tate group.

Note that it is clear that for the above mapping of $\mathrm{Hom}(V, I \cdot \underline{\mathrm{Lie}}(U))$ to $\mathrm{Ker}\,[\mathrm{Hom}\,(V,G) \longrightarrow \mathrm{Hom}\,(V_o, G_o)]$ we have $\theta \longmapsto u^T$ and $u^T(x) = \sum (\theta(x))^{(n)} = \exp(\theta(x))$ an element of $\mathrm{Ker}\,[G(S) \longrightarrow G(S_o)]$ for $x \in V$.

(2.5) Let A be a ring and B an A-bi-algebra which is complete with respect to a topology defined by a family of (open) ideals. Thus we have continuous maps (A being given the discrete topology)

$\epsilon: A \longrightarrow B$, $\mu: B \hat{\otimes} B \longrightarrow B$, $\eta: B \longrightarrow A$, $\Delta: B \longrightarrow B \hat{\otimes} B$ which satisfy the usual identities. Consider $B^\vee = \mathrm{Hom}_{\mathrm{cont.}}(B, A)$. As B is a co-algebra via η and Δ we can use the transposes η^T and Δ^T to make $B^\vee$ into an algebra:

(multiplication) $\quad B^\vee \otimes B^\vee \longrightarrow (B \hat{\otimes} B)^\vee \xrightarrow{\Delta^T} B^\vee$

(structure map) $\quad \eta^T: A \longrightarrow B^\vee$.

Also via $\epsilon^T: B^\vee \longrightarrow A$, $B^\vee$ becomes an augmented algebra.

In general $B^\vee$ will not be a co-algebra because the canonical map $B^\vee \otimes B^\vee \longrightarrow (B \hat{\otimes} B)^\vee$ is not necessarily invertible. But, observing that $B \hat{\otimes} B$ is a co-algebra we see (just as above) $(B \hat{\otimes} B)^\vee$ has a structure of augmented algebra. Corresponding to the two projections $\pi_1 = \mathrm{id}_B \hat{\otimes} \eta$ and $\pi_2 = \eta \hat{\otimes} \mathrm{id}_B$ we have by transposition two algebra maps

π_1^T, π_2^T: $B^\vee \longrightarrow (B \hat{\otimes} B)^\vee$. Consider the algebra map $\pi_1^T \otimes \pi_2^T$: $B^\vee \otimes B^\vee \longrightarrow (B \hat{\otimes} B)^\vee$. Using $(\pi_1 \hat{\otimes} \pi_2) \circ \Delta_{B \hat{\otimes} B} = id_{B \hat{\otimes} B}$, it follows that $\pi_1^T \otimes \pi_2^T$: $B^\vee \otimes B^\vee \longrightarrow (B \hat{\otimes} B)^\vee$ coincides with the canonical map $B^\vee \otimes B^\vee \longrightarrow (B \hat{\otimes} B)^\vee$.

(2.5.1) Assume in the above notation that $B^\vee$ is flat over A and that we are given an ideal $I \subseteq A$ with nilpotent divided powers. Thus using (1.8) the maps

$$\exp: I \cdot B^\vee \longrightarrow 1 + I \cdot B^\vee$$

$$\log: 1 + I \cdot B^\vee \longrightarrow I \cdot B^\vee$$

are defined and are (1.7) inverse isomorphisms. These maps are of course functorial in flat A-algebras. An element $y \in B^\vee$ is said to be <u>primitive</u> if $\epsilon^T(y) = 0$ and $\mu^T(y) = \pi_1^T \otimes \pi_2^T$ $(y \otimes 1 = 1 \otimes y) \in (B \hat{\otimes} B)^\vee$.

(2.5.2) On $I \cdot \underline{\text{Prim}}(B^\vee)$ there are defined divided powers induced from those on $I \cdot B^\vee$. Consider an element $i \cdot y$ in $I \cdot \underline{\text{Prim}}\,(B^\vee)$. Then writing $x = \exp(iy) = \sum i^{(n)} y^n$ and applying μ^T: $\mu^T(x) = \sum i^{(n)} (\mu^T(y))^n$ $= \sum i^{(n)} (\pi_1^T \otimes \pi_2^T (y \otimes 1 + 1 \otimes y))^n = \pi_1^T \otimes \pi_2^T (\sum i^{(n)} (y \otimes 1 + 1 \otimes y)^n)$ $= \pi_1^T \otimes \pi_2^T (x \otimes x)$, we find that x is a "group-like element" in the following sense:

<u>Definition</u> (2.5.3) An element x of $B^\vee$ is said to be group-like if $\epsilon^T(x) = 1$ and $\mu^T(x) = \pi_1^T \otimes \pi_2^T (x \otimes x)$.

<u>Remark</u> (2.5.4) This is an obvious generalization of the usual definition.

Notice that for β, β' in B we have $\langle \beta \cdot \beta', x \rangle = \langle \mu(\beta \otimes \beta'), x \rangle = \langle \beta \otimes \beta', \mu^T(x) \rangle = \langle \beta \otimes \beta', \pi_1^T \otimes \pi_2^T (x \otimes x) \rangle = \langle \beta, x \rangle \cdot \langle \beta', x \rangle$ by the final

remark of (2.5.1). Also $\langle 1, x\rangle = \langle \epsilon(1_A), x\rangle = \langle 1_A, \epsilon^T(x)\rangle = 1_A$. Thus x "group-like" implies $x: B \longrightarrow A$ is an algebra homomorphism.

(2.5.5) If $(B \hat{\otimes} B)^\vee$ is also flat over A then since divided powers are defined on $I \cdot B^\vee$ and $I \cdot (B \hat{\otimes} B)^\vee$ we have:

For $y \in I \cdot B^\vee \cap \underline{\mathrm{Prim}}(B^\vee)$, $\mu^T(\exp(y)) =$

$\exp(\mu^T(y)) = \exp(\pi_1^T \otimes \pi_2^T(y \otimes 1 + 1 \otimes y)) =$

$\pi_1^T \otimes \pi_2^T(\exp(y) \otimes \exp(y))$. Thus $x = \exp(y)$ is a group-like element of $B^\vee$.

In this case we can also define the log mapping and have for $1 + z \in 1 + I \cdot B^\vee$:

$$\epsilon^T \circ \log(1+z) = \log(\epsilon^T(1+z)) = 0 \quad \text{if } 1 + z \text{ is group-like.}$$

Also $\mu^T \circ \log(1+z) = \log \circ \mu^T(1+z) = \log \circ \pi_1^T \otimes \pi_2^T((1+z) \otimes (1+z))$

$= \pi_1^T \otimes \pi_2^T [\log(1+z \otimes 1) + \log(1 \otimes 1+z)]$

$= \pi_1^T \otimes \pi_2^T (\log(1+z) \otimes 1 + 1 \otimes \log(1+z))$ whenever $1 + z$ is group-like.

Thus in summary, we can state:

Lemma (2.5.6) Assume $B^\vee$ and $(B \hat{\otimes} B)^\vee$ are flat over A. Then exp and log are inverse isomorphisms:

$$I \cdot B^\vee \cap \underline{\mathrm{Prim}}(B^\vee) \underset{\log}{\overset{\exp}{\rightleftarrows}} \{\text{group-like elements in } 1 + I \cdot B^\vee\}$$

Application (2.5.7) Let G be a commutative group scheme which is locally of finite type over S. Let $\overline{G} = \varinjlim \mathrm{Inf}^k(G)$ and $\mathrm{Inf}^k(G) = \mathrm{Spec}(B_k)$ where B_k is a finite A-algebra [E.G.A. IV 16.1.7]. Also set

$B = \varprojlim B_n$, a complete adic ring whose topology is defined by the ideal $J = \mathrm{Ker}\,(B \longrightarrow B_o)$ [E.G.A. 0 I 7.2.7]. If C is any A-algebra then $\overline{G}(C) = \mathrm{Hom}_{\mathrm{cont.}}(B, C)$ where C is given the discrete topology. Let us define the hyper-algebra of G to be $B^\vee$. $B^\vee$ is, as was noted above in (2.5.1), an algebra and not in general a bi-algebra. For y in $\underline{\mathrm{Prim}}(B^\vee)$ and $\beta_1, \beta_2 \in B$, $\langle \beta_1 \cdot \beta_2, y\rangle = \langle \beta_1, y\rangle \varepsilon^T(\beta_2) + \langle \beta_2, y\rangle \varepsilon^T(\beta_1)$. Thus y kills J^2 and hence gives us an A-linear derivation of $B_1 \longrightarrow A$ (i.e., an element in $\underline{\mathrm{Lie}}\,(G)$). Conversely it is obvious that any such derivation comes from an element in $\underline{\mathrm{Prim}}(B^\vee)$. Thus $\underline{\mathrm{Prim}}(B^\vee) \xrightarrow{\sim} \underline{\mathrm{Lie}}\,(G)$. Also the set of "group-like" elements in $B^\vee$ is identical with $\overline{G}(A)$. If $B^\vee$ is flat over A, the exponential defines a map: $\exp: I \cdot \underline{\mathrm{Lie}}\,(G) \longrightarrow \mathrm{Ker}\,[G(A) \longrightarrow G(A/I)]$. If furthermore $(B \hat{\otimes} B)^\vee$ is flat over A, we have an isomorphism given by the exponential:

(2.5.7.1) $\underline{\mathrm{Lie}}\,(G) \cap I \cdot B^\vee \xrightarrow{\sim} \mathrm{Ker}\,[G(A) \longrightarrow G(A/I)]$.

(2.6) Unfortunately, what has preceded is not general enough. Thus in this section we give an ad hoc construction of the exponential in a situation which we will meet again later. Some preliminary comments are necessary.

Remark (2.6.1) In (1.8) it suffices to assume that $I \otimes B \longrightarrow IB$ is an isomorphism (i.e., $\mathrm{Tor}_1^A(A/I, B) = (0)$).

Remark (2.6.2) In the constructions of the exponential in 2.2 through 2.5 the hypothesis that the bi-algebra was flat can be replaced by the hypothesis that the divided powers on I extend to it as well as to its tensor

product with itself (obvious modification with regard to section 2.5). In effect all that was used was that it made sense to write down expressions such as $"\sum_{n \geq 0} x^{(n)}."$

Remark (2.6.3) Given a bi-algebra U it was its structure of augmented co-algebra which played the predominant role in the preceding sections. The concepts of primitive element and group-like element (or points with values in Cospec (U)) did not make use of the multiplication $\mu: U \otimes U \longrightarrow U$. Thus if the underlying augmented co-algebra of the bi-algebra U satisfies the appropriate conditions we will have the exponential defined.

(2.6.4) Let A be a ring, I an ideal of A with nilpotent divided powers, $A_o = A/I$. Let V be a locally-free of finite rank A-module and G a finite locally-free group scheme over $S = \mathrm{Spec}\,(A)$. Let $G = \mathrm{Spec}(B)$. Consider the S-group $V \underset{S}{\times} G$ whose ring is $\mathrm{Sym}\,(\check{V}) \underset{A}{\otimes} B$. Let H be an S-group which, as pointed scheme, is isomorphic to $V \underset{S}{\times} G$. We will show that there is a "theory of the exponential" for H (at least when $\underline{\mathrm{Lie}}\,(G)$ is locally-free).

(2.6.5) Set $C = \mathrm{Sym}\,(\check{V}) \otimes B$ so that $H = \mathrm{Spec}\,(C)$. C possesses two different structures of co-algebra corresponding to the two distinct group structures on Spec (C). Because $V \underset{S}{\times} G$ and H are isomorphic as pointed schemes, $\underline{\omega}_H \xrightarrow{\sim} \underline{\omega}_{V \underset{S}{\times} G}$ and hence is locally-free of finite type. Thus $\underline{\mathrm{Lie}}\,(H)$ is locally-free. Let W be a locally-free module and $\theta: W \longrightarrow I \cdot \underline{\mathrm{Lie}}\,(H)$ an A-linear map. Before defining $\exp(\theta)$, a lemma

is needed.

Lemma (2.6.6) Let $C^\vee = \mathrm{Hom}_{\mathrm{cont}}(C, A)$. The natural map $C^\vee \hat{\otimes} C^\vee \xrightarrow{\sim} (C \otimes C)^\vee$ is an isomorphism.

Proof: $C \otimes C \xrightarrow{\sim} (\mathrm{Sym}\,(\check{V}) \otimes B) \otimes (\mathrm{Sym}\,(\check{V}) \otimes B) \xrightarrow{\sim} (\mathrm{Sym}\,(\check{V}) \otimes \mathrm{Sym}(\check{V})) \otimes (B \otimes B)$. Therefore $(C \otimes C)^\vee \xrightarrow{\sim} \Gamma(V \hat{\oplus} V) \otimes (B^\vee \otimes B^\vee) \xrightarrow{\sim} \Gamma(V \oplus V)$ $\hat{\otimes} (B^\vee \otimes B^\vee)$ (since $B^\vee \otimes B^\vee$ is of finite presentation) $\xrightarrow{\sim} (\Gamma(V) \otimes \Gamma(V))$ $\hat{\otimes} (B^\vee \otimes B^\vee) \xrightarrow{\sim} (\Gamma(V) \otimes B^\vee) \hat{\otimes} (\Gamma(V) \otimes B^\vee) \xrightarrow{\sim} (\Gamma(\hat{V}) \otimes B^\vee) \hat{\otimes} (\Gamma(\hat{V}) \otimes B^\vee)$ by [E.G.A. 0 I 7.7.1] for example. This establishes the lemma.

Let $\Delta: C^\vee \longrightarrow C^\vee \hat{\otimes} C^\vee$ be the transpose of the multiplication map μ on C. If $y \in I \cdot \underline{\mathrm{Prim}}(C^\vee) = I \cdot \underline{\mathrm{Lie}}(H)$, $\Delta(y) = y \otimes 1 + 1 \otimes y$ belongs to $I \cdot \underline{\mathrm{Lie}}(H) \otimes 1 + 1 \otimes I \cdot \underline{\mathrm{Lie}}(H)$ and this last is isomorphic to $I \cdot (\underline{\mathrm{Lie}}(H) \oplus \underline{\mathrm{Lie}}(H))$.

Lemma (2.6.7) Let B_1 and B_2 be A-algebras, M_1, M_2 sub-A-modules of B_1 and B_2 respectively. Assume M_1 and M_2 are both finite and locally-free so that the divided powers on I extend to $I \cdot \mathrm{Sym}\,(M_1)$ and $I \cdot \mathrm{Sym}\,(M_2)$. Let ρ_1(resp. ρ_2): $\mathrm{Sym}\,(M_1) \longrightarrow B_1$ (resp. $\mathrm{Sym}\,(M_2) \longrightarrow B_2$) be the canonical mapping. Finally let $\varphi: B_1 \longrightarrow B_2$ be an algebra map taking M_1 to M_2. Then for $y \in I \cdot M_1$ $\varphi \circ \rho_1\,(\exp y) = \rho_2 \circ \exp(\varphi(y))$.

Proof: Obviously it suffices to verify the assertion for y of the form $i \cdot y'$, $i \in I$. Then we have $\varphi \circ \rho_1(\exp(iy')) = \varphi \circ \rho_1(\sum_{n \geq 0} i^{(n)} y'^n) = \sum i^{(n)} (\varphi(y'))^n$. Clearly this is $\rho_2 \circ \exp(\varphi(y'))$.

Applying the lemma to $B_1 = C^\vee$, $B_2 = C^\vee \hat{\otimes} C^\vee$, $M_1 = \underline{Lie}\,(H)$, $M_2 = \underline{Lie}\,(H) \otimes I + 1 \otimes \underline{Lie}\,(H)$, $\varphi = \Delta$, we find $\Delta(\exp(y)) = \exp(y \otimes 1 + 1 \otimes y)$ $= \exp(y \otimes 1) \cdot \exp(1 \otimes y) = \exp(y) \otimes \exp(y)$, where the last equality follows by applying the lemma to $B_1 = C^\vee$, $B_2 = C^\vee \hat{\otimes} C^\vee$, $\varphi =$ "inclusion along first factor," $M_1 = \underline{Lie}\,(H)$, $M_2 = \underline{Lie}\,(H) \otimes 1, \ldots$. Hence for $y \in I \cdot \underline{Lie}\,(H)$, $\exp(y)$ $(= \rho_1(\sum y^{(n)})$ in the above notation) is a "group-like" element. From (2.6.7) it is clear that $C^\vee$ is a bi-algebra and thus $\exp(y)$ is in $\mathrm{Cospec}\,(C^\vee)\,(A)$. But this is certainly $H(A)$ since $(C^\vee)^\vee = C$. Thus there is a homomorphism $I \cdot \underline{Lie}\,(H) \longrightarrow \mathrm{Ker}\,[H(A) \longrightarrow H(A_o)]$. As usual it is injective. By looking at $\exp(\theta(x))$ for $x \in W$ (notation of (2.6.5), we obtain our desired homomorphism:

(2.6.8) $\exp: \mathrm{Hom}\,(W,\ I \cdot \underline{Lie}\,(H)) \hookrightarrow \mathrm{Ker}\,[\mathrm{Hom}\,(W, H) \longrightarrow \mathrm{Hom}\,(W_o, H_o)]$ defined by $\exp(\theta)(x) = \exp(\theta(x))$.

More precisely, by looking at the mapping $\Gamma(W) \longrightarrow C^\vee$ given by $x \longmapsto \exp(\theta(x))$, and repeating the reasoning of (2.4) we obtain the above inclusion.

Remark (2.6.9) This construction is obviously functorial with respect to both arguments. If H' is a sheaf of groups and H is a group scheme as above and we assume $H \hookrightarrow H'$, $\overline{H}'$ is a formal Lie group, $\underline{Lie}\,(H) = \underline{Lie}\,(H') = \underline{Lie}\,(\overline{H}')$, then the above definition of the exponential coincides with the one given in (2.4) in the following sense: any homomorphism $u: W \longrightarrow H$ which restricts to zero over S_o must have its image contained in $\overline{H} \hookrightarrow \overline{H}'$. Then for $\theta: W \longrightarrow I \cdot \underline{Lie}\,(H)$, $\exp(\theta)$:

$W \longrightarrow \bar{H}'$ is the mapping defined in (2.4).

Remark (2.6.10) The introduction of the symmetric algebra above seems necessary because $\Gamma^{\wedge}(V)$ is not necessarily flat over A [4, Chapter 1, exercises §2, #12]. Thus although the divided powers on I will extend to $\Gamma^{\hat{}}(V)$, it is no longer clear that they will extend to $\Gamma^{\hat{}}(V) \otimes B^{\vee}$ when this module is given the non-standard algebra structure (corresponding to H as opposed to $V \underset{S}{\times} G$).

(2.7) In this section we study prolongations of homomorphisms and the relation between these and the exponential. Let S be an affine scheme, Spec (A), I an ideal of A with nilpotent divided powers, and $S_o = \mathrm{Spec}(A/I)$. Let G be a group on S. Assume that G is a filtering direct limit of sub-groups G_α each of which is representable. Also assume that $\mathrm{Inf}^1(G) = \mathrm{Inf}^1(G_\alpha)$ for some α, so that $\underline{\mathrm{Lie}}\,(G) = \underline{\mathrm{Lie}}\,(G_\alpha)$ and that the "theory of the exponential" exists for G. The last requirement means that the homomorphism

$$\exp: \mathrm{Hom}\,(V,\ I \cdot \underline{\mathrm{Lie}}\,(G)) \hookrightarrow \mathrm{Ker}\,[\mathrm{Hom}_{S\text{-gr.}}(V,G) \longrightarrow \mathrm{Hom}_{S_o\text{-gr.}}(V_o, G_o)]$$

is defined. Examples of groups which satisfy these conditions are the following:

1) smooth group scheme

2) Barsotti-Tate group, say over a base where p is nilpotent

3) a group of the type discussed in (2.6.4) or more generally a direct limit of such (provided the condition on the Lie algebra is satisfied).

Actually, we shall later use the following discussion in connection with groups of the third type.

(2.7.1) Let H be an S-group and $u_o : H_o \longrightarrow G_o$ a homomorphism. It is clear that the set of liftings of u_o to homomorphisms $u: H \longrightarrow G$ is either empty or principal homogeneous under the group $\mathrm{Ker}[\mathrm{Hom}(H,G) \longrightarrow \mathrm{Hom}(H_o, G_o)]$. Assume that $V = H$ is a vector group (i.e., the group associated to a locally free of finite rank, $\mathcal{O}_S$-module). Then the theory of the exponential permits us to make the following definitions:

Definition (2.7.2) Two liftings u', u'' of $u_o : V_o \longrightarrow G_o$ are linearly compatible if their difference is in the image of

$$\mathrm{Hom}(V, I \cdot \underline{\mathrm{Lie}}(G)) \hookrightarrow \mathrm{Ker}[\mathrm{Hom}(V,G) \longrightarrow \mathrm{Hom}(V_o, G_o)].$$

This is obviously an equivalence relation on the set of liftings of u_o to a $u: V \longrightarrow G$.

(2.7.3) Assume $u_o : V_o \longrightarrow G_o$ is a monomorphism with image $H_o \subseteq G_o$. We want to examine the set of liftings H of H_o to subgroups of G, flat over S, together with structure of locally-free module on H, lifting that defined on H_o. Let H be a solution of this problem. Then H is given by V where V is a finite locally-free $\mathcal{O}_S$-module. Any such V is determined up to (non-unique) isomorphism [S.G.A 1 III 7.1]. Let us fix once and for all such a V lifting V_o. Then, to give an H as above is equivalent to giving a monomorphism $V \longrightarrow G$ lifting u_o, modulo identifying two such u and u' if they differ by an $\mathcal{O}_S$-automorphism of V

which reduces to the identity on S_o. In fact given such a monomorphism $u: V \longrightarrow G$, it is obvious that $H = \mathrm{im}(u)$ is a solution of the problem. Conversely, let H be a solution of the problem. Via $u_o^{-1}: H_o \longrightarrow V_o$, H becomes a lifting of V_o. Thus by [S.G.A. 1 III 7.1] there is an isomorphism w between H and V which reduces to u_o^{-1}. By taking u to be the composite of w^{-1} and the inclusion of H into G, we find a $u: V \longrightarrow G$ of the desired type. Finally it is clear that if and only if u and u' differ by an $\mathcal{O}_S$-linear automorphism of V (reducing to id_{V_o}) is it the case that $H = \mathrm{im}(u)$ and $H' = \mathrm{im}(u')$ give the same solution of the problem (after all one makes H into an $\underline{\mathcal{O}}_S$-module via transport of structure).

Lemma (2.7.4) Any homomorphism $u: V \longrightarrow G$ lifting $u_o: V_o \longrightarrow G_o$ is a monomorphism.

Proof: Since V is quasi-compact and G satisfies the conditions of (2.7), $u: V \longrightarrow G$ factors through a representable sub-group G' of G. The induced morphism $u': V \longrightarrow G'$ is locally of finite type [E.G.A. IV, 1.3.4(v)], and hence $S_o \hookrightarrow S$ being a nilpotent immersion implies that $u': V \longrightarrow G'$ is a monomorphism [S.G.A. 3 VI B 2.11].

Definition (2.7.5) Two homomorphisms $u, u': V \longrightarrow G$ lifting u_o are said to be congruent if they differ by an $\mathcal{O}_S$-linear automorphism of V reducing to the identity on V_o.

Thus u and u' are congruent if and only if they define the same solution of our problem. The next lemma allows us to speak of two solutions of our problem as being linearly compatible.

Lemma (2.7.6) If u and u' are congruent, then they are linearly compatible.

Proof: Write $u' = u \circ (id_V + \eta)$ where $\eta: V \longrightarrow I \cdot V$ since η reduces to zero. $u' - u = u \circ \eta$ and hence by the functoriality of the exponential it suffices to show that η is an exponential. But V is given by the co-algebra $\hat{\Gamma}(V)$ via the identification of its "group-like" elements with elements of V given by $1 + v^{(1)} + v^{(2)} + \ldots \longmapsto v^{(1)}$. Hence under this identification we see that $\eta = \exp(\eta)$.

Thus we see that the exponential allows us to define an equivalence relation on the set of solutions H of our problem.

Let $\underline{h} \subseteq \underline{Lie}(G)$ be a locally-free sub-module lifting $\underline{h}_o = \underline{Lie}(H_o)$ (with necessarily locally free quotient by the criterion for flatness [4, Chap. III §5, Theorem 1]). The following proposition will be quite important later.

Proposition (2.7.7) In each linear equivalence class of solutions of our problem, there is exactly one H with $\underline{Lie}(H) = \underline{h}$.

Proof: Choose a particular class and let $u: V \longrightarrow G$ be a representative (lifting u_o) in it. By the previous lemma we are allowed to modify u by exactly one element in $\mathrm{Hom}(V, I \cdot \underline{Lie}(G)) / \mathrm{Aut}_{\mathcal{O}_S}(V,$ inducing $id_{V_o})$. Here the quotient has an obvious meaning. On the other hand if we look at $\underline{Lie}(u): V \longrightarrow \underline{Lie}(G)$, which lifts $\underline{Lie}(u_o): V_o \longrightarrow \underline{Lie}(G_o)$, it is clear that we are permitted to modify $\underline{Lie}(u)$ by exactly one element in $\mathrm{Hom}(V, I \cdot \underline{Lie}(G)) / \mathrm{Aut}_{\mathcal{O}_S}(V,$ inducing $id_{V_o})$ in order to get any possible

locally-free lifting of $\underline{h}_o \subseteq \underline{\mathrm{Lie}}\,(G_o)$. (Note that any such modification will give rise to a monomorphism $V \longrightarrow \underline{\mathrm{Lie}}\,(G)$ by [E.G.A. IV 11.9.18]). Hence in modifying $\underline{\mathrm{Lie}}\,(u)$ by an appropriate element so as to obtain $\underline{h}$, we obtain an element $u' : V \longrightarrow G$ such that $\mathrm{im}\,(\underline{\mathrm{Lie}}\,(u')) = \underline{h}$.

§3. (3.0) In this paragraph we define crystals and discuss the trivial "general nonsense" aspect of this theory which we will need later.

Remark (3.1) The definition of crystal which we adopt is a very naive one. The crystalline site should be defined with reference to a base scheme and a compatibility condition on the divided powers should be imposed. Also the nilpotent site must in characteristic 2 be replaced by the Berthelot site. It is essentially because we do not utilize crystalline cohomology, that the naive definition suffices. For a more detailed discussion along with example see: [2, 3, 15].

Definition (3.2) For a scheme X, its crystalline site Crys (X) consists of the category whose objects are triples $(U \hookrightarrow T, \gamma)$ where:

1) U is an open sub-scheme of X

2) $U \hookrightarrow T$ is a locally nilpotent immersion

3) $\gamma = (\gamma_n)$ are divided powers (which are locally nilpotent) on the ideal I of U in T. The morphisms from $(U \hookrightarrow T, \gamma)$ to $(U' \hookrightarrow T', \delta)$ are the commutative diagrams:

$$\begin{array}{ccc} U & \hookrightarrow & T \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ U' & \hookrightarrow & T' \end{array}$$

such that $U \longrightarrow U'$ is the inclusion and $T \xrightarrow{\bar{f}} T'$ is a divided power morphism (i.e., the sheaf of rings morphism $\bar{f}^{-1}(\mathcal{O}_{T'}) \longrightarrow \mathcal{O}_T$ is a divided power morphism).

The topology on Crys (X) is "that induced by the Zariski topology": it is defined by a pre-topology where

$$\{(U_i \hookrightarrow T_i, \gamma_i) \longrightarrow (U \hookrightarrow T, \gamma)\}$$

is a covering family when T_i is the open sub-scheme of T whose underlying set is U_i and when $\bigcup U_i = U$.

Remark (3.3) Sheaves (of sets for example) on this site admit the following description: To give a sheaf F is equivalent to giving for each object $(U \hookrightarrow T, \gamma)$ an ordinary sheaf $F_{(U \hookrightarrow T, \gamma)}$ on T together with morphisms $\bar{f}^{-1}(F_{(U' \hookrightarrow T', \delta)}) \longrightarrow F_{(U \hookrightarrow T, \gamma)}$ whenever we have a morphism:

$$\begin{array}{ccc} U & \hookrightarrow & T \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \bar{f}} \\ U' & \hookrightarrow & T' \end{array} \qquad (3.3.1)$$

These maps are to satisfy an obvious transitivity condition and $\bar{f}^{-1}(F_{(U' \hookrightarrow T', \delta)}) \longrightarrow F_{(U \hookrightarrow T, \gamma)}$ is to be an isomorphism whenever T is the open sub-scheme of T' carried by set U.

Remark (3.4) The site Crys (X) is ringed in a natural way. Namely $\mathcal{O}_{X\ \mathrm{crys}}$ corresponds, according to (3.3), to the system $\mathcal{O}_{(U \hookrightarrow T, \gamma)} = \mathcal{O}_T$.

A sheaf of modules M on Crys (X), thus is given by a family M_T of $\mathcal{O}_T$-modules, ... M is said to be special if for any diagram (3.3.1) we have $\bar{f}^*(M_{T'}) = M_T$. A module M is quasi-coherent if and only if it is special and all $M_{(U \hookrightarrow T, \gamma)}$ are quasi-coherent.

(3.5) We now turn to the definition of crystals. Let $\mathcal{F}$ be a fibered category on (Sch) which is a stack with respect to the Zariski topology. This means that both morphisms and objects can be glued together. For a precise definition see [11, I 3.2].

Definition (3.6) An $\mathcal{F}$-crystal on X is a cartesian section of the fibered category $\mathcal{F} \underset{\text{Sch}}{\times}$ Crys (X), where Crys (X) $\longrightarrow$ (Sch) is given by $(U \hookrightarrow T, \gamma) \longrightarrow T$. A morphism of $\mathcal{F}$-crystals is a morphism of cartesian sections. This means that for each object $(U \hookrightarrow T, \gamma)$ in Crys (X) we are given an object $Q_{(U \hookrightarrow T, \gamma)}$ in $\mathcal{F}_T$ and that for each morphism (3.3.1) in Crys (X) we are given an isomorphism

$$u_{\bar{f}} : Q_{(U \hookrightarrow T, \gamma)} \longrightarrow \bar{f}^*(Q_{(U' \hookrightarrow T', \delta)})$$

These isomorphisms are to satisfy $\bar{f}^*(u_{\bar{g}}) \circ u_{\bar{f}} = u_{\bar{g} \circ \bar{f}}$ where $\bar{g}$ comes from a morphism in Crys (X)

$$\begin{array}{ccc} U' & \hookrightarrow & T' \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle \bar{g}} \\ U'' & \hookrightarrow & T'' \end{array}$$

Remark (3.7) For details on the above definition see [10, §1]. We will systematically assume the fibered categories dealt with are "split," which again by [10, §5] is harmless. Finally we will in general be careless about the canonical isomorphism $u_{\bar{f}}$ and assume we have an actual identity of objects $\bar{f}^*(\mathcal{Q}_{(U' \hookrightarrow T', \delta)}) = \mathcal{Q}_{(U \hookrightarrow T, \gamma)}$. This will never lead to confusion.

(3.8) We want now to define the notion of "inverse image" for crystals. Let $Y \xrightarrow{\varphi} X$ be a morphism of schemes. Fix a fibered category $\mathcal{F}$ as above and let $\mathcal{Q}$ be an $\mathcal{F}$-crystal on X. $\varphi^*(\mathcal{Q})$ is to be an $\mathcal{F}$-crystal on Y. To define $\varphi^*(\mathcal{Q})$, observe that since $\mathcal{F}$ is a stack it suffices to give the value of $\varphi^*(\mathcal{Q})$ on "sufficiently small" objects in Crys (Y). Specifically "sufficiently small" means an object $(U \hookrightarrow T, \gamma)$ in Crys (Y) such that $\varphi(U)$ is contained in an affine open subset V of X, and where U (and hence T) is affine. To define $\varphi^*(\mathcal{Q})$ on such an object we proceed as follows: Choose $V \supseteq \varphi(U)$, an affine. Let $U = \mathrm{Spec}(A)$, $T = \mathrm{Spec}\, A'$, $A'/I = A$, $V = \mathrm{Spec}\,(B)$ and consider the diagram of rings:

(3.8.1)
$$\begin{array}{ccc} A & \longleftarrow & A' \\ \uparrow & & \uparrow \\ B & \longleftarrow & B \underset{A}{\times} A' \end{array}$$

Obviously $B \underset{A}{\times} A' \longrightarrow B$ is surjective with kernel $\{0\} \times I$. On this ideal we define divided powers via $\gamma'_n(0, i) = (0, \gamma_n(i))$. Obviously these divided powers are nilpotent and $B \underset{A}{\times} A' \longrightarrow A'$ is a divided power morphism.

Taking $W = \mathrm{Spec}\,(B \underset{A}{\times} A')$ we see that $(V \hookrightarrow W, \gamma')$ is an object of Crys (X). Furthermore we have a diagram:

$$\begin{array}{ccc} U & \hookrightarrow & T \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \bar{\varphi}} \\ V & \hookrightarrow & W = V \underset{U}{\coprod} T \end{array} \qquad (3.8.2)$$

(in the category of affine schemes).

By definition $\varphi^*(\Omega)_{(U \hookrightarrow T, \gamma)} = \bar{\varphi}^* (\Omega_{(V \hookrightarrow W, \gamma')})$.

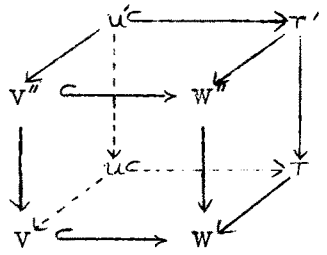
It must be shown that this object is independent of the V chosen. But if V' is a second affine open in X such that $\varphi(U) \subseteq V'$, then repeating the above construction we obtain $V' \hookrightarrow W'$ and $\bar{\varphi}' : T \longrightarrow W'$. What must be shown is that $\bar{\varphi}^*(\Omega_{V \hookrightarrow W}) = \bar{\varphi}'^*(\Omega_{V' \hookrightarrow W'})$. To do this it suffices, since $\mathcal{F}$ is a stack, to show these objects are equal locally. Thus choose $U' \hookrightarrow T'$, with T' the open sub-scheme of T induced on $U' \hookrightarrow U$, so that $\varphi(U')$ is contained in an affine $V'' \subseteq V \cap V'$, and U' is affine. For $U' \hookrightarrow T'$ the above construction can be performed to obtain

$$\begin{array}{ccc} U' & \hookrightarrow & T' \\ \downarrow & & \downarrow \\ V'' & \hookrightarrow & W'' \end{array}$$

By looking at the definitions of the various diagrams it is immediate that there are morphisms:

$$\begin{array}{ccc} V'' & \hookrightarrow & W'' \\ \downarrow & & \downarrow \\ V & \hookrightarrow & W \end{array} \qquad \begin{array}{ccc} V'' & \hookrightarrow & W'' \\ \downarrow & & \downarrow \\ V' & \hookrightarrow & W' \end{array}$$

making the following diagrams commute:



, ...

Thus $\overline{\varphi}^{*}(\Omega_{V \hookrightarrow W})\,|\,T' = \overline{\varphi}''^{*}(\Omega_{V'' \hookrightarrow W''})$

$= \overline{\varphi}'^{*}(\Omega_{V' \hookrightarrow W'})\,|\,T'$

This shows the definition above is independent of the choice of V. Having defined $\varphi^{*}(\Omega)$ for "sufficiently small" objects it is immediate (since $\mathcal{F}$ is a stack) that this partial definition can be uniquely completed so that $\varphi^{*}(\Omega)$ is a crystal.

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.

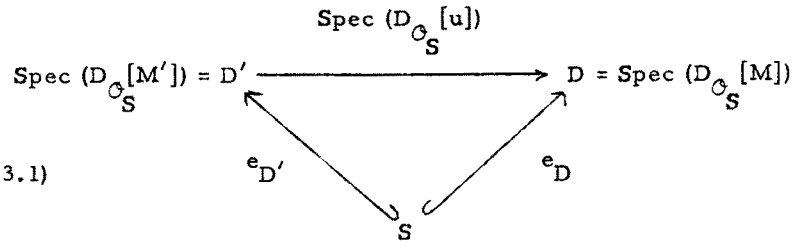
Proposition (1.3) The functor (on quasi-coherent modules) $M \longmapsto \mathrm{Hom}_{S\text{-gr.}}(G, M)$ is represented by $\underline{\omega}_{G^*}$, G^* being the Cartier dual of G.

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 $\mathcal{C}(M)$. Note that $M \longmapsto \mathcal{C}(M)$ 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:

$\mathrm{Hom}_{S\text{-gr.}}(G, M) \xrightarrow{\sim} \mathcal{C}(M)$. Let us show how the proposition follows. By definition (or by [S.G.A. 3 VII A 3.3]) $\mathcal{C}(M) = \mathrm{Ker}\,[G^*(D) \longrightarrow G^*(S)]$. 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) $\qquad \mathrm{Hom}\,(G, M) \xrightarrow{\sim} \mathfrak{a}(M).$

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 $G(T) \longrightarrow \Gamma(T, \mathcal{O}_T^*)$. 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 $\mathrm{Hom}\,(G_D, \mathbb{G}_{m_D}) \longrightarrow \mathrm{Hom}\,(G, \mathbb{G}_{m_D})$ 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 $\mathcal{A}(M) = \mathrm{Ker}[\mathrm{Hom}_{D\text{-gr.}}(G_D, \mathbb{G}_{m_D}) \longrightarrow \mathrm{Hom}_{S\text{-gr.}}(G, \mathbb{G}_m)]$.

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 $\mathrm{Hom}_{S\text{-gr.}}(G, M) \longrightarrow \mathcal{A}(M)$ 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 $D' = D \underset{S}{\times} S' = \mathrm{Spec}[\mathcal{O}_{S'} \oplus (M \underset{\mathcal{O}_S}{\otimes} \mathcal{O}_{S'})]$ 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 $\Sigma (a_i \oplus m_i) \otimes m_i'$ and hence the hypothesis that $\varphi'(D) = 0$ says that $\Sigma a_i m_i' = 0$. Notice that over this affine open U $\varphi(S)(e_D^*(x)) = \Sigma a_i m_i' = 0$. 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 $\tilde{\varphi}(D_{S'}): G(D_{S'}) \longrightarrow \mathfrak{G}_m(D_{S'})$. 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 $G(T) \hookrightarrow G(D_T) \xrightarrow{\tilde{\varphi}(D_T)} \mathfrak{G}_M(D_T)$ minus $1 = \tilde{\varphi}(T)(x) - 1$ because there is a commutative diagram

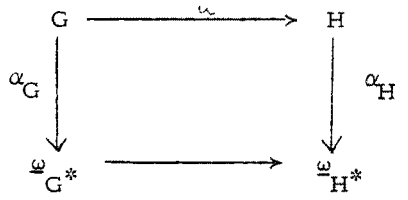
$$\begin{array}{ccc} G(D_T) & \xrightarrow{\tilde{\varphi}(D_T)} & \mathbb{G}_m(D_T) \\ \uparrow & & \uparrow \\ G(T) & \xrightarrow{\tilde{\varphi}(T)} & \mathbb{G}_m(T) \end{array}$$

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 $\dot{\alpha}: G \longrightarrow \underline{\omega}_{G^*}$, 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:



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

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

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

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

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

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

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

3) Let $G^* = \mathrm{Spec}\,(C)$, $H^* = \mathrm{Spec}\,(B)$, 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 $\mathrm{Hom}\,(\underline{\omega}_{H^*}, M)$ 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, $\mathrm{Hom}_{S\text{-gr.}}(G, M) = (0)$ 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 $\mathrm{Ext}^1(G, M)$.

Definition (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.

Remark (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

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

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

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

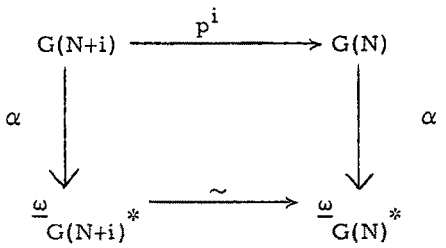
Since Ext is a bi-functor, the map $\mathrm{Ext}^1(G,M) \longrightarrow \mathrm{Ext}^1(G, M)$ comes from multiplication by p^N on M. Hence it is zero. This means there is an isomorphism induced by the coboundary map δ, δ: Hom (G(N), M) $\xrightarrow{\sim}$ $\mathrm{Ext}^1(G, M)$. This isomorphism is 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:

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

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)

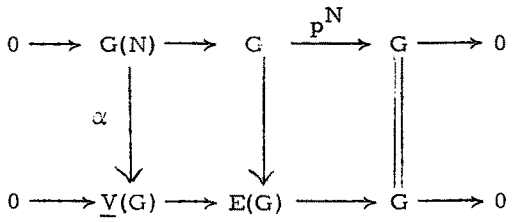


The fact that $\underline{\omega}_{G(N+i)^*} \longrightarrow \underline{\omega}_{G(N)^*}$ is an isomorphism is [II 3.3.20].

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



what must be shown is that $\alpha: G(N) \longrightarrow \underline{\omega}_{G(N)^*}$ 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 $0 \longrightarrow \underline{V}(G) \longrightarrow E(G) \longrightarrow G \longrightarrow 0$ 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 $0 \longrightarrow \underline{\omega}_{G^*} \longrightarrow E(G) \longrightarrow G \longrightarrow 0$ 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 $u: G \longrightarrow H$ a homomorphism. There is a unique homomorphism $E(u): E(G) \longrightarrow E(H)$ such that we obtain a morphism of extensions:

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

(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)

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

(II)

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

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:

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

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.

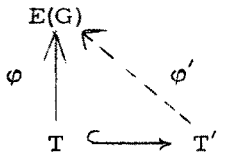
Proof: Let p^N kill S so that $\mathrm{Inf}^k(G) \subseteq G(n+N-1)$ if $k < p^n$ [II(3.3.17)]. Consider the extension

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

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 $\varphi\colon T \longrightarrow E(G)$ be given:



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 $\pi_T(\varphi)\colon T \longrightarrow G(n)$ 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 $\psi\colon T' \longrightarrow E(G) \underset{G}{\times} G(n)$. $\psi|T$ 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 $\eta\colon T' \longrightarrow \underline{V}(G)$. Thus $\eta+\psi\colon T' \longrightarrow E(G) \underset{G}{\times} G(n)$ and $\eta+\psi|T = \varphi$. This proves E(G) is formally smooth.

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

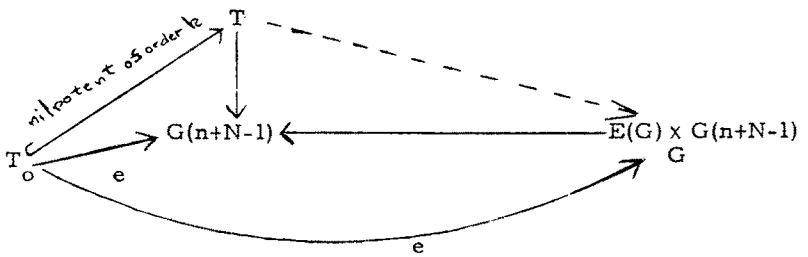
Proof: Since $\overline{E(G)}$ is by (1.18) formally smooth (locally at least) it follows immediately from [II 3.1.1] and (1.17) that $\overline{E(G)}$ is a formal Lie group. In particular $\overline{E(G)}$ is formally smooth.

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

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), $E(G) \underset{G}{\times} G(n+N-1)$ 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

$\mathrm{Inf}^k(E(G)) \longrightarrow \mathrm{Inf}^k(G)$ 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 $E(G) \underset{G}{\times} G(N) \longrightarrow G(N)$ 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 $\widehat{E(A)}$ 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 Lie. 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" $E(G)$.

Notation (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 $G|U_o = G_o|U_o$.

Remark (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 $\mathbb{E}(G)$.

Theorem (2.2) Let $S = \mathrm{Spec}(A)$, $p^N \cdot 1_S = 0$, $S_o = \mathrm{Var}(I)$ 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:

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

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 exponential (an assertion which makes sense by [III 2.4]).

Remark (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 $E(H)$) $\bar{i} \circ h(x) = \bar{i}\,(\Sigma\,(h(x))^{(n)}) = \Sigma\,(\bar{i} \circ h(x))^{(n)}$ (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:

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

By hypothesis $i' \circ w' = v' \circ i + \exp(\theta')$, where $\theta': \underline{V}(H) \longrightarrow I \cdot \underline{Lie}(E(K))$. Thus $i' \circ (w' \circ w) = v' \circ (i \circ w) + \exp(\theta') \circ w$. But $i \circ w = v | \underline{V}(G) + \exp(\theta)$, $\theta: \underline{V}(G) \longrightarrow I \cdot \underline{Lie}(E(H))$. 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.

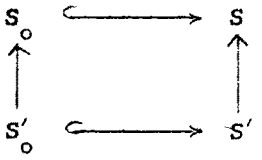
Corollary (2.4.2) If $G = H$ and $u_o = id_{G_o}$, then $E_S(u_o) = id_G$.

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:



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 $\theta: \underline{V}(G) \longrightarrow I \cdot \underline{Lie}(E(H))$, then $d_{S'}$ is (obviously) $\exp(\theta_{S'})$ where $\theta_{S'}: \underline{V}(G_{S'}) \longrightarrow J \cdot \underline{Lie}(E(H_{S'}))$ 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

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

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

$$\begin{array}{ccccc} U_o & \hookrightarrow & U & = & U_o \underset{V_o}{\amalg} V \\ {\scriptstyle f}\uparrow & & \uparrow{\scriptstyle \bar{f}} & & \\ V_o & \hookrightarrow & V & & \end{array}$$

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

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:

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

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

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

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

$\mathbb{D}$ is defined via:

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

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 $L = E(G) \underset{G}{\times} G(n)$ satisfies the hypotheses of (III 2.6.4) and hence the exponential mapping exp: $\mathrm{Hom}(M, I \cdot \underline{\mathrm{Lie}}(L)) \hookrightarrow \mathrm{Ker}[\mathrm{Hom}(M, L) \longrightarrow \mathrm{Hom}(M_o, L_o)]$ is defined for any locally-free module M.

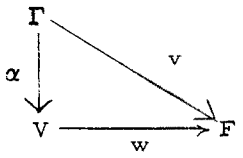
Proof: The first sentence of the proof of (1.2 2) tells us that $E(G) \underset{G}{\times} G(n) \longrightarrow G(n)$ admits a section. Since $E(G) \underset{G}{\times} G(n)$ is a group and the section is a morphism of S-schemes, by translation by an appropriate element of the kernel $\underline{V}(G)(S)$ it can be assumed that the section preserves the unit section. Consider the isomorphism of G(n)-schemes $E(G) \underset{G}{\times} G(n) \xrightarrow{\sim} \underline{V}(G) \underset{S}{\times} G(n)$ 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 $\mathrm{Hom}(V, I \cdot \underline{\mathrm{Lie}}(F)) \xleftarrow{\exp} \mathrm{Ker}[\mathrm{Hom}(V, F) \longrightarrow \mathrm{Hom}(V_o, F_o)]$ 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 $\mathcal{W}$ 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 $\mathcal{B}$ 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.

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

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

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

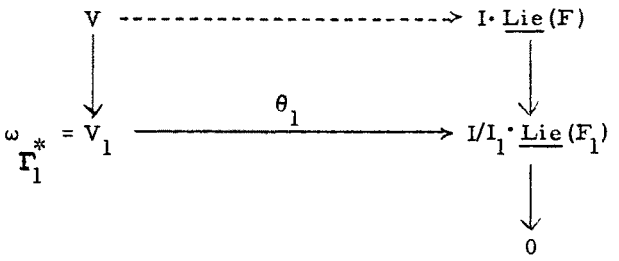
2) $h_o = 0$

3) h is an exponential.

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

2nd reduction: Take a finite filtration of S: $S = S_r \supseteq S_{r-1} \supseteq \dots \supseteq S_o$ 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 $\theta_1 : \omega_{\Gamma_1^*} \longrightarrow I/I_1 \cdot \underline{Lie}(F_1)$ 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 $\theta_2 : V \longrightarrow I \cdot \underline{Lie}(F)$ 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 $\theta_3 : V \longrightarrow I_1 \cdot \underline{Lie}(F)$ such that $\exp(\theta_2 + \theta_3) \circ \alpha = v$. This gives us the existence of a solution. To show uniqueness let $\theta' : V \longrightarrow I \cdot \underline{Lie}(F)$ 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 $\theta' = \theta_2 + \theta_3$.

Application: 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 Cospec (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 $\overline{F}$, 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)]

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

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 $\underline{\mathcal{O}}_S$-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:

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

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 $B = \hat{\Gamma}[M]$, 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 $\text{Cospec}(\hat{\Gamma}(V))$ 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 $V_o \longrightarrow \underline{Lie}(F) \otimes I$ 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 $u: V_o \longrightarrow \underline{Lie}(F_o) \otimes I$ 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 $u: V_o \longrightarrow \underline{Lie}(F_o) \otimes I$ is equivalent to giving a linear map

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

On $\underline{Prim}(B/((p)+I) \cdot B)$ 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 $\underline{Lie}(F_o) \otimes I$ 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 $\underline{Lie}(F_o) \otimes I$ 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 $\underline{Lie}(F_o) \otimes I$.

Let $u: V_o \longrightarrow \underline{Lie}(F_o) \otimes I$ 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].

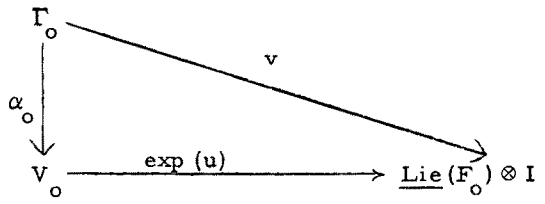
Thus $\sum_{n\geq 0} u(x)^{(p^n)} = \sum_{n\geq 1} u(x)^{(n)} = \exp(u)\,(x)$.

Thus we can state:

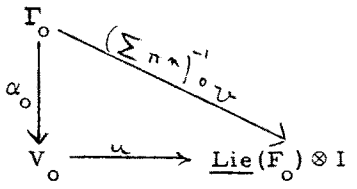
(2.6.6.3) $\qquad (\sum \pi^n) \circ u = \exp(u).$

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

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

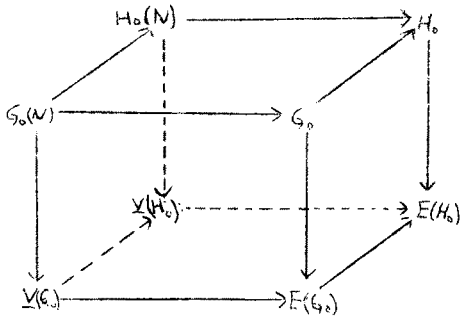
Consider the following diagram from which the universal extension E(G) is obtained (and consider the corresponding diagram for H).

(2.7.1)

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

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) $\quad v'$ lifts v'_o, v'' lifts v''_o

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

Lemma (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.

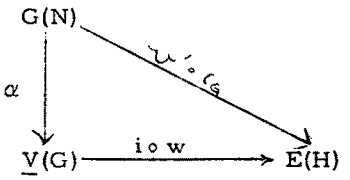
Proof: By the statement of the problem it is clear that the set of solutions is in one to one correspondence with the set of $v'': \underline{V}(G) \longrightarrow E(H)$ such that:

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:



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 $\mathrm{Ext}^1(G, M) \hookrightarrow \mathrm{Ext}^1(G(N), M)$.

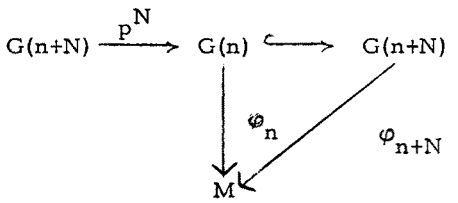
Hence we are reduced to showing that the obstruction to lifting

$v'_o | G_o(N)$ 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 Hom (G, M). But this group is zero because it can be written as $\varprojlim$ Hom (G(n), M). If (φ_n) were an element of this inverse limit, then:

(2.7.5)



$\varphi_{n+N} \circ p^N \cdot id_{G(n+N)} = 0$ 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 $G(\pi)$ is flat, w is an element in $\varprojlim \Gamma(G(\pi), (E(H))') = \varprojlim \Gamma(G(\pi), E(H)) = \operatorname{Hom}_{\widetilde{S}_{Flat}}(G, E(H))$.

Because the $G(\pi)$ 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 $G(\pi)$-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 $\mu: X \underset{A}{\otimes} X \longrightarrow X$ which lifts the subtraction map $\mu_o: X_o \underset{A_o}{\otimes} X_o \longrightarrow X_o$. 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 $U \subseteq$ 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

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

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 $B.T.'(S_o)$ the full sub-category of $B.T.(S_o)$ consisting of those G_o's which can locally (for Zariski) be lifted to a G in $B.T.(S)$.

Remark (1.2) The definition of $B.T.'(S_o)$ 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 $B.T.'(S_o)$ 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 $B.T.'(S_o)$ 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 $B.T.'(S_o)$, 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:

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

Prior to proving the theorem some preliminary remarks are necessary.

Remark (1.7) 1) Let G_o be in $B.T.'(S_o)$. On S there is defined a (Zariski) sheaf of sets $\mathscr{L}$ in the following way: For an affine open $U \subseteq S$ $\Gamma(U, \mathscr{L})$ = 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 $\underline{Lie}\,(E(u)): \underline{Lie}\,(E(G)) \longrightarrow \underline{Lie}\,(E(H))$ 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

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

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 $V \in \mathfrak{V}$, $V \hookrightarrow \mathbb{E}(G_o)_S$ 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 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

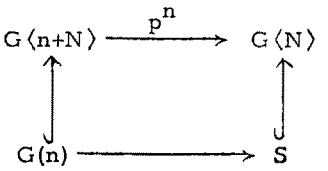
nilpotent ideal it is and is furthermore flat and of finite presentation [S.G.A. 3 VI b 9.2 xi, xiii]. Let $G\langle n\rangle = E(n)/V$ so that $G = \varinjlim G\langle n\rangle$ and $G\langle n\rangle|S_o = G_o(n)$. Let $S = \mathrm{Spec}\,(A)$, $G\langle n\rangle = \mathrm{Spec}\,(B_n)$. Since B_n/IB_n 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:



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 $B.T.'(S_o)$ 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

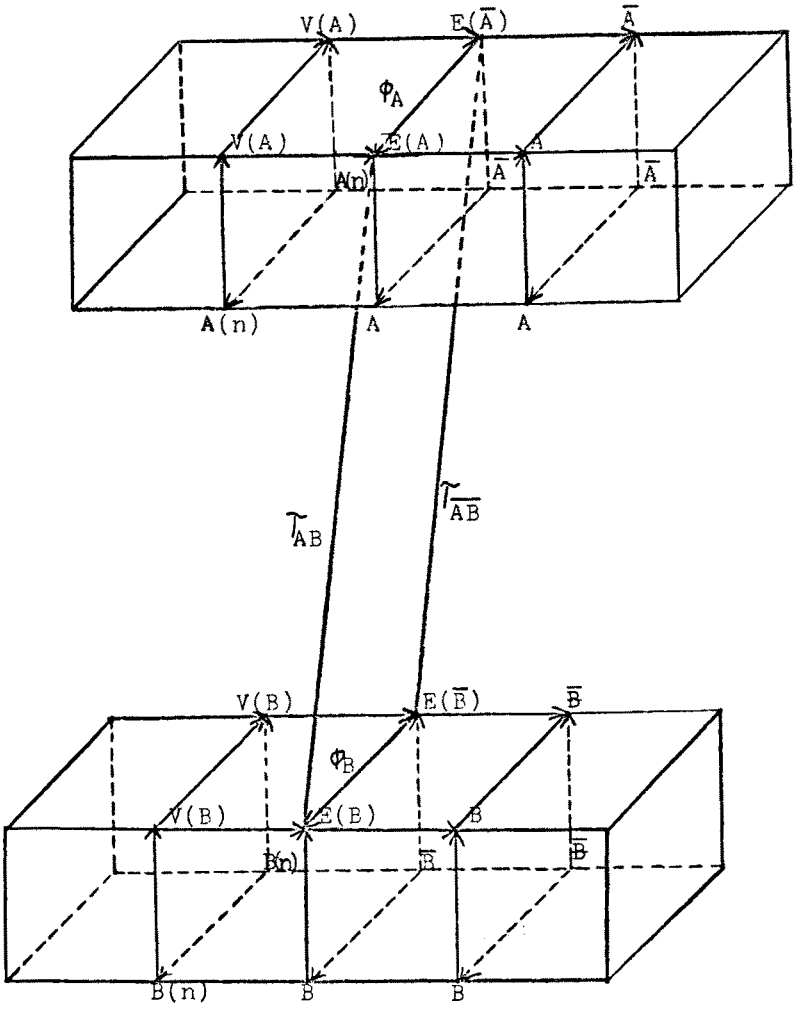
$$(2.1.2) \qquad \tau_{\bar{A}\bar{B}} : E(\bar{A}) \xrightarrow{\sim} E(\bar{B})$$

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

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)

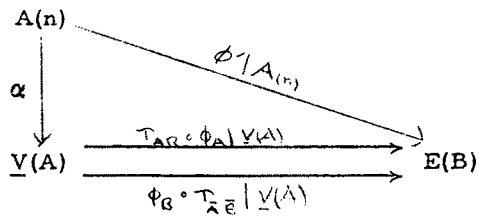
$\tau_{AB} \circ \varphi_A = \varphi_B \circ \tau_{\bar{A}\bar{B}}$ it suffices to show that both mappings have the same restriction to $\bar{A}$ and to $\underline{V}(A)$.

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 $i: S_o \hookrightarrow S$)

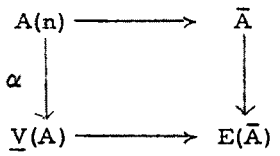
$\left(\tau_{AB} \circ \varphi_A - \varphi_B \circ \tau_{\bar{A}\bar{B}}\right) \big| \bar{A}: \bar{A} \longrightarrow$ Ker where Ker denotes the kernel of the mapping $E(B) \longrightarrow i_* i^*(E(B))$. But as has been seen in the proof of [IV 2.2] this kernel (or at least its restriction to flat 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 $\underline{V}(A_o) \xrightarrow{id.} \underline{V}(A_o)$ (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 $\tau_{AB} \circ \varphi_A | \underline{V}(A) = \tau_{AB} | \underline{V}(A)$ 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 $\varphi_B \circ \tau_{\bar{A}\bar{B}} | \underline{V}(A) = \varphi_B \circ (\underline{V}(A) \xrightarrow{g} \underline{V}(B) \hookrightarrow E(\bar{B})$ + 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 $\tau_{AB} \circ \varphi_A | \underline{V}(A)$ differs from $\varphi_B \circ \tau_{\bar{A}\bar{B}} | \underline{V}(A)$ by an exponential. Therefore applying [IV 2.6.3] it follows that

$$\tau_{AB} \circ \varphi_A | \underline{V}(A) = \varphi_B \circ \tau_{\bar{A}\bar{B}} | \underline{V}(A).$$

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):

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

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:

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

(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 $A \longmapsto (A \underset{S}{\times} S_o, \bar{A})$ 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) <u>essential surjectivity</u>: 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 $I = I_o \supseteq I_1 \supseteq \cdots \supseteq I_r = (0)$. 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 $(\underline{V}(A) \longrightarrow D(\bar{A}_o)_S) \longrightarrow (\underline{V}(B) \hookrightarrow D(\bar{B}_o)_S)$, 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 $(A \times_S S_o, \bar{A})$ 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:

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

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

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

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 $\mathrm{End}\,(A'_n \times A''_n) \longrightarrow \mathrm{End}\,(\bar{A}_o)$ is bijective for all n. Thus the map $\mathrm{End}\,(A') \longrightarrow \mathrm{End}\,(A_o)$ 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 $\left(\overline{(A'|W_n(k))}\right)^* \xrightarrow{\sim} \overline{(A'|W_n(k))^*}$.

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 $A'_n \longrightarrow A^{*\prime}_n$ (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 $\mathrm{End}\,(A) \longrightarrow \mathrm{End}\,(A_o)$ is bijective (since we already know $\mathrm{End}\,(A') \longrightarrow \mathrm{End}\,(A_o)$ 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 $\mathrm{Hom}(A, B) \to \mathrm{Hom}(A_o, B_o)$ 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 5.41] 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 [$\mathrm{EGA}_{\mathrm{II}}$ 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 [$\mathrm{EGA}_{\mathrm{IV}}$ 8.11.1]. Thus the kernel is finite, and locally-free. From (1.0) and [$\mathrm{EGA}_{\mathrm{IV}}$ 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 $n^{\underline{\text{th}}}$ 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 $\tilde{A}$ is a Barsotti-Tate group is suffices to show $\tilde{A}(i)$ is finite, locally-free. Let us show $\tilde{A}(i) = A < 1 >$. Since $\tilde{A}(i) = \varinjlim A < n > (i)$ 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 $\tilde{A} \hookrightarrow A(\infty)$. Over k, there is a map $A_o(\infty) \longrightarrow \tilde{A}_o = A_o(\infty)^{ét}$ which when composed with the inclusion is the identity on $\tilde{A}_o$ (since $A_o(\infty) = A_o(\infty)^{t.m.} \times A_o(\infty)^{ét}$). Because $\tilde{A}$ 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 $i^{\underline{th}}$ 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 $Ext^1(G'',G')$.

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 :

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

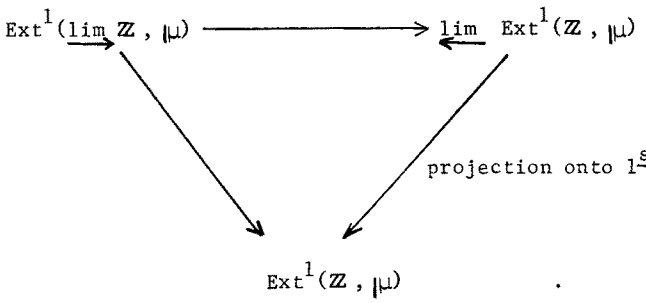
Looking at the relevant portion of the long exact sequence arising from applying the functor $\mathrm{Hom}(-,\mu)$ we obtain the sequence :

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

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 $\mathrm{Spec}(R)$.

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 $\mathrm{Spec}(R)$, 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

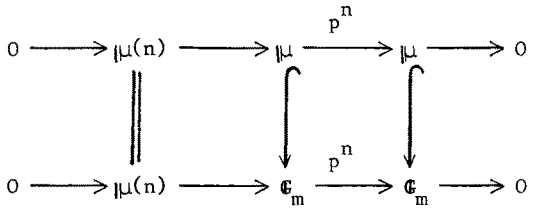
$$(2.5.2.2) \quad 0 \longrightarrow R^1\Gamma((1+\underline{m})_{i\in\mathbb{N}}) \longrightarrow \mathrm{Ext}^1(\varinjlim \mathbb{Z}, \mu) \longrightarrow \varprojlim \mathrm{Ext}^1(\mathbb{Z}, \mu) \quad .$$

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.

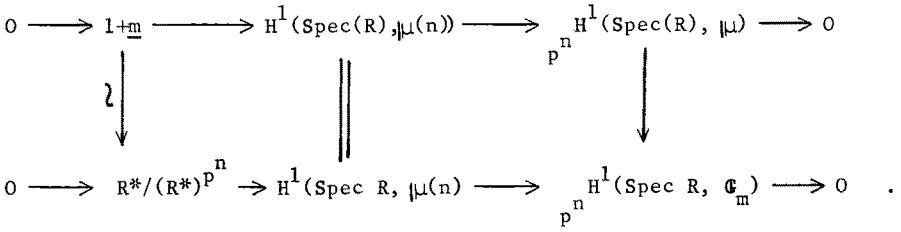
(2.5.3). The injectivity of the map $\varprojlim \mathrm{Ext}^1(\mathbb{Z}, \mu) \longrightarrow \mathrm{Ext}^1(\mathbb{Z}, \mu)$ follows from the more precise:

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 :



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:



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

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

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,

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

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) :

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

(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 $r_i : \mathbb{Q}/\mathbb{Z}_p \xrightarrow{\sim} E_i(\infty)^{\text{ét}}$. 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 $1+\underline{m} \xrightarrow{\sim} \text{Ext}^1(\mathbb{Q}_p/\mathbb{Z}_p,\mu)$ "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].

Bibliography

1. Barsotti, I: Analytical Methods for Abelian Varieties in Positive Characteristic, Coll. Théorie Groupes algébriques, C.B.R.M., Bruxelles, 1962.

2. Berthelot, P.: Cohomologie p-cristalline des schémas,... C. R. Acad. Sc. Paris, t.269, pp. 297-300, 357-360, 397-400, August , September, 1969; t. 272, pp. 42-45, 141-144, 254-257.

3. Berthelot, P. and Illusie, L.: Classes de Chern en cohomologie cristalline. C. R. Acad. Sc. Paris, t. 270, pp. 1695-1697, 1750-1752 (June, 1970).

4. Bourbaki, N.: Éléments de Mathématique Algèbre Commutative, Hermann, Paris, 1961...

4(bis) _____, Éléments de Mathématiques Algèbre, Chapter II, Hermann, Paris, 1962.

5. Cartier, P.: Hyperalgèbres et groupes de Lie formels, Seminaire Sophus Lie, 2^{e} année, Secretariat Mathématique, Paris, 1957.

6. _____,: Groupes algébriques et groupes formels, Coll. Théorie Groupes Algébriques, C.B.R.M., Bruxelles, 1962.

7. _____,: Relèvements des Groupes Formels Commutatifs. Seminaire Bourbaki, No. 359 (June 1969).

8. Demazure, M. and Gabriel, P.: Groupes Algébriques (Tome I) Mason and Cie, Paris, 1970. (cited G.A. in the text)

9. Demazure,M., and Grothendieck, A.: Schémas en Groupes, Lecture notes in Mathematics, Volumes 151-153, Springer-Verlag, Berlin, 1970. (cited S.G.A. 3 in text)

[9bis] Deuring, M. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hams. Univ. 14 (1947) p.p. 197-272.

[9ter] Dwork, B. p-adic Cycles, Publ. Math. IHES n° 37 (1969) p.p. 27-116.

10. Giraud, J.: Méthode de la Descente, Bull. Soc. Math. France, Memoire 2, 1964.

11. _____,: Cohomologie non abélienne, multigraphed, Columbia University, 1966.

12. Grothendieck, A., and Dieudonné, J.: Éléments de Géométrie Algébrique, Publ. Math. IHES, nos. 4,8,11,17,20,24,28,32. (cited E.G.A. in the text)

13. Grothendieck, A., et al.: Séminaires de Géométrie Algébrique du Bois Marie, multigraphed, IHES, Bures-sur-Yvette. (cited S.G.A. in the text)

14. Grothendieck, A.: Catégories Cofibrées Additives et Complexe Cotangent Relatif, Lecture notes in Mathematics, Vol. 79, Springer-Verlag, 1968.

15. _____,: Crystals and the De Rham Cohomology of schemes (notes by I. Coates and O. Jussila), in Dix Exposés sur la Cohomologie des Schémas, North Holland, 1968.

16. Hartshorne, R.: Residues and Duality, Lecture notes in Mathematics, Vol. 20, Springer-Verlag, 1966.

[16bis] Hasse, H. Beweis des Analogons die Riemannschen Vermutung für die Artinschen und F.K. Schmidtschen Kongruenz-zetafunktionen in gewissen elliptischen Fällen (Vorläufige Mitteilung), Nachr. Ges. d. Wiss. Math. Phys. Kl., Göttingen (1933) p.p. 253-262.

[16ter] Hasse H., Modular functions and elliptic curves over finite fields, Simposio Internazionale di Geometria Algebrica, Edizoni Cremonese, Roma 1967, p.p. 248-266.

17. Illusie, L.: Algèbre homotopique relative, C. R. Acad. Sc. Paris, t. 268, pp. 11-14, 206-209; Complexe cotangent relative d'un faisceau d'algèbres, t. 268, pp. 278-281, 323-326.

[17bis] Illusie, L. Thesis (to appear)

18. Lazard, D.: Sur les Modules plats, C. R. Acad. Sci., Paris, t. 258, pp. 6313-6316 (1964).

19. Lubin, J., Serre, J-P, Tate, J.: Elliptic Curves and Formal Groups, Woods Hole Summer Institute, 1964. (mimeographed notes)

20. Manin, Yu.: The theory of commutative formal groups over fields of finite characteristic, English trans., Russian Math. Surv., Vol. 18, 1963.

21. Mumford, D.: Geometric Invariant Theory, Ergebnisse Math., Springer-Verlag, 1965.

22. _____,: Abelian Varieties, Oxford, 1970.

23. Oda, T.: The First De Rham Cohomology Group and Dieudonné Modules, Ann. Sci. Ecole Norm. Sup., 1969.

24. Oort, F.: Commutative Group Schemes, Lecture notes in Mathematics, Vol. 15, Springer-Verlag, 1966.

25. _____,: Finite Group Schemes, local moduli for abelian varieties, and lifting problems, Nordic Summer School in Mathematics, Oslo, 1970.

26. Raynaud, M.: Faiseeaux amples sur les schémas en groupes et les espaces homogènes, Lecture notes in Mathematics, Vol. 119, Springer-Verlag, 1970.

27. Roby, N.: Lois polynomes et lois formelles en théorie des Modules, Ann. Sci. Ecole Norm. Sup., 1963.

28. _____,: Les algèbres, à puissances divisées, Bull, Sci. Math., 1965.

29. Serre, J-P.: Groupes p-divisibles (d'après J. Tate), Séminaire Bourbaki, exposé 318, 1966-67.

30. Tate, J.: p-Divisible Groups, Proceedings of a Conference on Local Fields, Nuffic Summer School at Driebergen, Springer-Verlag, 1967.