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

(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

$U \mapsto \Gamma_{\mathcal{O}_S(U)}(M(U))$. 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 $(\nu'_n)_{n \geq 1}$ 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 $\mathrm{id}_{I \otimes B}$. Assume $\gamma'_1, \dots, \gamma'_{n-1}$ have been defined so as to satisfy the above condition. Consider $I \times B$ and define a map $\varphi\colon A^{(I \times B)} \longrightarrow B$ via the formula

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

$$= \quad \Sigma\, (a_1 b_1)^{k_1} \gamma_{k_1}(i_1) \dots (a_\ell b_\ell)^{k_\ell} \gamma_{k_\ell}(i_\ell)$$

where this sum runs over the ℓ-tuples $(k_1, \dots, k_\ell)$ 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 $x = a_1(i_1, b_1) + \dots + a_\ell(i_\ell, b_\ell)$ 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

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

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

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

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

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 $I \cdot B$.

§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) x 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 <u>filtered</u> 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

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

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 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 $S' \longmapsto \Gamma(S', \text{Nil}\ (\mathcal{O}_{S'})))$.

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

Definition (2.1.7) $\exp_M : \overline{M} \longrightarrow \text{Cospec}\ (\Gamma(M))$ 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 $S = \text{Spec}\ (A)$, $S' = \text{Spec}\ (A')$. 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 $\Gamma(S', \text{Cospec}\ (\Gamma(M)))$.

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 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 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 = nil-radical 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], $\text{Cospec}(\Gamma(M)) = \varinjlim \text{Cospec}(\Pi(F_i))$ [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 $\underline{\underline{\mathcal{O}}}_S$-module and $\exp_M$ is a homomorphism of $\underline{\underline{\mathcal{O}}}_S$-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 $(\text{id}_U \otimes \eta) \circ \Delta = \text{id}_U$ 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 $\underline{\underline{\mathcal{O}}}_S$-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 $\underline{\text{Lie}}(U) = V(\underline{\omega}_X) = \underline{\text{Lie}}(X)$, 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 $\underline{\underline{\mathcal{O}}}_S$-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

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 $\exp\colon \Gamma(S, I\cdot \underline{\mathrm{Lie}}(U)) \longrightarrow \Gamma(S, \mathrm{Cospec}(U))$ defined by $\exp(x) = \Sigma\, x^{(n)}$ is a homomorphism whose image lies in $\mathrm{Ker}\,[\Gamma(S, \mathrm{Cospec}(U)) \longrightarrow \Gamma(S_o, \mathrm{Cospec}(U))]$.

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

Proof: Without hypothesis on $U/\underline{\mathrm{Lie}}\,(U)$ observe we can define a map $\log\colon \mathrm{Ker} \longrightarrow I\cdot U \cap \underline{\mathrm{Lie}}\,(U)$ 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 $\underline{\mathrm{Lie}}\,(U)$ 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 $\Gamma(S, I\cdot U \cap \underline{\mathrm{Lie}}\,(U))$ and $\mathrm{Ker}\,[\Gamma S, \mathrm{Cospec}\,(U)) \longrightarrow \Gamma(S_o, \mathrm{Cospec}\,(U))]$. But the flatness hypothesis insures that $I\cdot U \cap \underline{\mathrm{Lie}}\,(U) = I\cdot\underline{\mathrm{Lie}}\,(U)$ [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 $\underline{\mathrm{Lie}}\,(U) \cap I\cdot U \xrightarrow{\sim} \mathrm{Ker}\,[\Gamma(S, \mathrm{Cospec}\,(U)) \longrightarrow \Gamma(S_o, \mathrm{Cospec}\,(U))]$, 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 <u>augmented</u> $\mathcal{O}_S$-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 $u\colon \Gamma(M) \longrightarrow U$ be a map compatible with divided powers (so that $u(\Gamma^+(M)) \subset I \cdot U$). Let $\theta\colon M \longrightarrow I{\cdot}U$ 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 $\theta \in \mathrm{Hom}\,(M, \underline{\mathrm{Lie}}\,(U) \cap I{\cdot}U^+)$.

<u>Lemma</u> (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.

<u>Proof</u>: 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.

<u>Remark</u> (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 $\overline{M} \xrightarrow{\sim} \mathrm{Cospec}\,(\Gamma(M))$ [2.18]. Thus we have defined a monomorphism:

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

We make the map explicit as follows: Let $\theta\colon M \longrightarrow \underline{\mathrm{Lie}}(G) \cap I{\cdot}U$ 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 $u'(x) = u(\Sigma\, x^{(n)}) = \Sigma\,(\theta(x))^{(n)}$ 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 $\theta\colon M \longrightarrow \underline{\mathrm{Lie}}(G) \cap I \cdot U$ 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 $\underline{\omega}_G$ 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 $I \cdot U \cap \underline{\mathrm{Prim}}(U) = I \cdot \underline{\mathrm{Prim}}\,(U)$ 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 $U \longmapsto \underline{\mathrm{Prim}}\,(U)$ is represented by $A[\epsilon]$. Clearly this category admits a product (namely the ordinary product of two co-algebras with the obvious "pointing"). Hence:

$$\begin{aligned} \underline{\mathrm{Prim}}\,(U \otimes V) &= \mathrm{Hom}_{\text{pt.-co-algebras}}\,(A[\epsilon],\ U \otimes V) \\ &= \mathrm{Hom}\,(A[\epsilon], U) \times \mathrm{Hom}\,(A[\epsilon],\ V) \\ &= \underline{\mathrm{Prim}}\,(U) \times \underline{\mathrm{Prim}}\,(V). \end{aligned}$$

Thus the map $\underline{\mathrm{Prim}}\,(U \otimes V) \longrightarrow \underline{\mathrm{Prim}}\,(U) \times \underline{\mathrm{Prim}}\,(V)$ of components $\mathrm{id}_U \otimes \eta_V$ and $\eta_U \otimes \mathrm{id}_V$ is an isomorphism. Let $u \in \underline{\mathrm{Prim}}\,(U)$ and $v \in \underline{\mathrm{Prim}}\,(V)$. 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 $I \cdot (U \otimes V) \cap \underline{\mathrm{Prim}}\,(U \otimes V)$. This implies $u = \mathrm{id}_U \otimes \eta_V\,(x) \in I \cdot U \cap \underline{\mathrm{Prim}}\,(U)$ and hence $u = \sum i_\alpha u_\alpha$ with $u_\alpha \in \underline{\mathrm{Prim}}(U)$, $i_\alpha \in I$. 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 $\theta: M \longrightarrow I \cdot \underline{\mathrm{Lie}}(G)$ 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 <u>nilpotent</u> 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 $\mathrm{Cospec}(U)$ for a flat augmented co-algebra U and that all $\mathrm{Inf}^k(G)$ are finite and locally-free. Let $\theta: V \longrightarrow I \cdot \underline{\mathrm{Lie}}(U)$ be given. Then θ corresponds to a $u: \Gamma(V) \longrightarrow U$ given by $u(x) = \Sigma(\theta(x))^{(n)}$ for $x \in V$. Because the divided powers on I are nilpotent u will map $\underset{i \geq n}{\oplus} \Gamma^i(V)$ to zero if n is sufficiently large. Thus u can be extended to the completion $\Gamma\hat{}(V)$ 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 $u: \Gamma\hat{}(V) \longrightarrow U$ we find a bi-algebra mapping $B \longrightarrow \mathrm{Sym}(\check{V})$ and this defines a group homomorphism $V \longrightarrow \overline{G}$. Since given $u: \Gamma\hat{}(V) \longrightarrow U$, 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:

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

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 $u^T(x) = \Sigma(\theta(x))^{(n)} = \exp(\theta(x))$ 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

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

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

Remark (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 $1 + z \in 1 + I \cdot B^{\vee}$:

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

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 $\mathrm{Inf}^k(G) =$ 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 $J = \operatorname{Ker}(B \longrightarrow B_o)$ [E.G.A. 0 I 7.2.7]. If C is any A-algebra then $\overline{G}(C) = \operatorname{Hom}_{\text{cont.}}(B, C)$ 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 <u>not</u> in general a bi-algebra. For y in $\underline{\text{Prim}}(B^{\vee})$ and $\beta_1, \beta_2 \in B$, $\langle \beta_1 \cdot \beta_2, y\rangle = \langle \beta_1, y\rangle\, \epsilon^T(\beta_2) + \langle \beta_2, y\rangle\, \epsilon^T(\beta_1)$. Thus y kills J^2 and hence gives us an A-linear derivation of $B_1 \longrightarrow A$ (i.e., an element in $\underline{\text{Lie}}(G)$). Conversely it is obvious that any such derivation comes from an element in $\underline{\text{Prim}}(B^{\vee})$. Thus $\underline{\text{Prim}}(B^{\vee}) \xrightarrow{\sim} \underline{\text{Lie}}(G)$. 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: $\exp: I \cdot \underline{\text{Lie}}(G) \longrightarrow \operatorname{Ker}[G(A) \longrightarrow G(A/I)]$. If furthermore $(B \hat{\otimes} B)^{\vee}$ is flat over A, we have an isomorphism given by the exponential:

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

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

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

<u>Remark</u> (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 "$\sum_{n \geq 0} x^{(n)}$."

<u>Remark</u> (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 $S = \operatorname{Spec}(A)$. Let $G = \operatorname{Spec}(B)$. Consider the S-group $V \times_S G$ whose ring is $\operatorname{Sym}(\check{V}) \otimes_A B$. Let H be an S-group which, as pointed scheme, is isomorphic to $V \times_S G$. We will show that there is a "theory of the exponential" for H (at least when $\underline{\text{Lie}}(G)$ is locally-free).

(2.6.5) Set $C = \operatorname{Sym}(\check{V}) \otimes B$ so that $H = \operatorname{Spec}(C)$. C possesses two different structures of co-algebra corresponding to the two distinct group structures on $\operatorname{Spec}(C)$. Because $V \times_S G$ and H are isomorphic as pointed schemes, $\underline{\omega}_H \xrightarrow{\sim} \underline{\omega}_{V \times_S G}$ and hence is locally-free of finite type. Thus $\underline{\text{Lie}}(H)$ is locally-free. Let W be a locally-free module and $\theta: W \longrightarrow I \cdot \underline{\text{Lie}}(H)$ 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 $B_1 = C^\vee$, $B_2 = C^\vee \hat{\otimes} C^\vee$, $M_1 = \underline{\mathrm{Lie}}(H)$, $M_2 = \underline{\mathrm{Lie}}(H) \otimes I + 1 \otimes \underline{\mathrm{Lie}}(H)$, $\varphi = \Delta$, 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," $M_1 = \underline{\mathrm{Lie}}(H)$, $M_2 = \underline{\mathrm{Lie}}(H) \otimes 1, \ldots$. Hence for $y \in I \cdot \underline{\mathrm{Lie}}(H)$, $\exp(y)$ (= $\rho_1(\sum y^{(n)})$ 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 $I \cdot \underline{\mathrm{Lie}}(H) \longrightarrow \mathrm{Ker}[H(A) \longrightarrow H(A_o)]$. 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) $\exp: \mathrm{Hom}(W, I \cdot \underline{\mathrm{Lie}}(H)) \hookrightarrow \mathrm{Ker}[\mathrm{Hom}(W, H) \longrightarrow \mathrm{Hom}(W_o, H_o)]$

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 $H \hookrightarrow H'$, $\bar{H}'$ is a formal Lie group, $\underline{\mathrm{Lie}}(H) = \underline{\mathrm{Lie}}(H') = \underline{\mathrm{Lie}}(\bar{H}')$, 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 $\bar{H} \hookrightarrow \bar{H}'$. Then for $\theta: W \longrightarrow I \cdot \underline{\mathrm{Lie}}(H)$, $\exp(\theta)$:

$W \longrightarrow \overline{H}'$ 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 $\Gamma^{\wedge}(V)$, it is no longer clear that they will extend to $\Gamma^{\wedge}(V) \otimes B^{\vee}$ 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

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

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 $u_o\colon H_o \longrightarrow G_o$ a homomorphism. It is clear that the set of liftings of u_o to homomorphisms $u\colon H \longrightarrow G$ 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 $u_o\colon V_o \longrightarrow G_o$ 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 $u\colon V \longrightarrow G$.

(2.7.3) Assume $u_o\colon V_o \longrightarrow G_o$ 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 $u' = u \circ (\mathrm{id}_V + \eta)$ 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 $\underline{h} \subseteq \underline{\mathrm{Lie}}\,(G)$ be a locally-free sub-module lifting $\underline{h}_o = \underline{\mathrm{Lie}}(H_o)$ (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 $\underline{\mathrm{Lie}}\,(H) = \underline{h}$.

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 $\mathrm{Hom}\,(V, I \cdot \underline{\mathrm{Lie}}\,(G)) / \mathrm{Aut}_{\mathcal{O}_S}(V,$ inducing $\mathrm{id}_{V_o})$. Here the quotient has an obvious meaning. On the other hand if we look at $\underline{\mathrm{Lie}}\,(u): V \longrightarrow \underline{\mathrm{Lie}}\,(G)$, which lifts $\underline{\mathrm{Lie}}\,(u_o): V_o \longrightarrow \underline{\mathrm{Lie}}(G_o)$, it is clear that we are permitted to modify $\underline{\mathrm{Lie}}\,(u)$ by exactly one element in $\mathrm{Hom}\,(V, I \cdot \underline{\mathrm{Lie}}\,(G)) / \mathrm{Aut}_{\mathcal{O}_S}(V,$ inducing $\mathrm{id}_{V_o})$ in order to get any possible locally-free lifting of $\underline{h}_o \subset \underline{\text{Lie}}\,(G_o)$. (Note that any such modification will give rise to a monomorphism $V \longrightarrow \underline{\text{Lie}}\,(G)$ by [E.G.A. IV 11.9.18]). Hence in modifying $\underline{\text{Lie}}\,(u)$ by an appropriate element so as to obtain $\underline{h}$, we obtain an element $u' : V \longrightarrow G$ such that $\text{im}\,(\underline{\text{Lie}}\,(u')) = \underline{h}$.

§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:

$$\begin{tikzcd}
U \arrow[r, hook] \arrow[d, "f"'] & T \arrow[d, "\bar{f}"] \\
U' \arrow[r, hook] & T'
\end{tikzcd}$$

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:

(3.3.1)
$$\begin{tikzcd}
U \arrow[r, hook] \arrow[d, "f"'] & T \arrow[d, "\bar{f}"] \\
U' \arrow[r, hook] & T'
\end{tikzcd}$$

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 $\mathcal{O}_{X\ \text{crys}}$ 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 $\mathcal{F} \underset{\text{Sch}}{\times} \text{Crys}(X)$, where $\text{Crys}(X) \longrightarrow (\text{Sch})$ 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)

$$\begin{tikzcd}
U' \arrow[r, hook] \arrow[d, "g"'] & T' \arrow[d, "\bar{g}"] \\
U'' \arrow[r, hook] & T''
\end{tikzcd}$$

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 $\bar{f}^*(Q_{(U' \hookrightarrow T', \delta)}) = Q_{(U \hookrightarrow T, \gamma)}$. 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 Q be an $\mathcal{F}$-crystal on X. $\varphi^*(Q)$ is to be an $\mathcal{F}$-crystal on Y. To define $\varphi^*(Q)$, observe that since $\mathcal{F}$ is a stack it suffices to give the value of $\varphi^*(Q)$ 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 $\varphi^*(Q)$ on such an object we proceed as follows: Choose $V \supseteq \varphi(U)$, an affine. Let $U = \text{Spec}(A)$, $T = \text{Spec}\, A'$, $A'/I = A$, $V = \text{Spec}(B)$ and consider the diagram of rings:

(3.8.1)
$$\begin{tikzcd}
A & A' \arrow[l] \\
B \arrow[u] & B \underset{A}{\times} A' \arrow[l] \arrow[u]
\end{tikzcd}$$

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

$$\begin{tikzcd} U \arrow[r, hook] \arrow[d, "\varphi"'] & T \arrow[d, "\overline{\varphi}"] \\ V \arrow[r, hook] & W = V \underset{U}{\coprod} T \end{tikzcd} \quad \text{(in the category of affine schemes).} \tag{3.8.2}$$

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

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 $\overline{\varphi}' : T \longrightarrow W'$. What must be shown is that $\overline{\varphi}^*(\Omega_{V \hookrightarrow W}) = \overline{\varphi}'^*(\Omega_{V' \hookrightarrow W'})$. 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

$$\begin{tikzcd} U' \arrow[r, hook] \arrow[d] & T' \arrow[d] \\ V'' \arrow[r, hook] & W'' \end{tikzcd}$$

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

$$\begin{tikzcd} V'' \arrow[r, hook] \arrow[d] & W'' \arrow[d] \\ V \arrow[r, hook] & W \end{tikzcd} \qquad \begin{tikzcd} V'' \arrow[r, hook] \arrow[d] & W'' \arrow[d] \\ V' \arrow[r, hook] & W' \end{tikzcd}$$

making the following diagrams commute:

$$\begin{tikzcd} & U' \arrow[rr, hook] \arrow[dl] \arrow[dd, dashed] & & T' \arrow[dl] \arrow[dd] \\ V'' \arrow[rr, hook] \arrow[dd] & & W'' \arrow[dd] & \\ & U \arrow[rr, hook, dashed] \arrow[dl, dashed] & & T \arrow[dl] \\ V \arrow[rr, hook] & & W & \end{tikzcd} \quad , \ . \ . \ .$$

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.