# Geometry of $p$-jets, II

**Alexandru Buium**

Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
D-53225 Bonn

Germany

MPI / 94-128

# Geometry of $p-$jets, II

Alexandru Buium

## 0. Introduction.

This paper is a direct continuation of [B5] which we shall refer to as Part I. In Part I we started to develop a $p-$adic analogue of our differential algebraic theory in [B1-B4] and we have studied "$\delta-$formal functions" on curves of genus $g \geq 2$, and of genus $g = 0$. The present paper is devoted to the study of $\delta-$formal functions on curves of genus $g = 1$, and more generally on abelian varieties. Our main purpose is to construct an analogue, in our $p-$adic theory, of the "Manin maps of abelian varieties over fields with a derivation" [Man], [Ch], [B1], [BV], [Hr]. Recall that in the "classical case" of fields with a derivation the Manin maps are "differential algebraic" homomorphisms from the group of points of the abelian varieties into the additive group of the field; they have the property that the intersection of their kernels is "small". We shall find a similar picture here for abelian varieties with good reduction defined over $p-$adic fields. As in Part I we shall restrict our attention to the absolutely unramified case. This is only for simplicity of the exposition for most of the theory has a ramified version, as we shall explain in a forthcoming paper.

Let's briefly recall the basic objects considered in Part I. Let $R$ be an absolutely unramified complete discrete valuation ring with fraction field $K$ of charactersitic 0 and algebraically closed residue field $k$ of characteristic $p > 0$. In addition to Part I we shall assume throughout the present paper that $p \neq 2$. Consider the unique lifting $\phi : R \rightarrow R$ of the Frobenius of $k$. Define the map $\delta : R \rightarrow R$ by the formula $\delta x = (\phi(x) - x^p)/p$ and for any $x \in R$ write $x', x'', ..., x^{(n)}$ in place of $\delta x, \delta^2 x, ..., \delta^n x$. Moraly $x', x'', ...$ play the role of "derivatives" of $x$ (and will be called the *$p-$derivatives* of $x$).

Let $X/S$ be a scheme of finite type. An $R-$valued function $\varphi : X(R) \rightarrow R$ will is called a *$\delta-$formal function of order* $\leq n$ on $X(R)$ if any point in $X$ has an affine open neighbourhood $U \subset X$ where $\varphi$ can be written as

$$\varphi(P) = \Phi(u(P), u(P)', u(P)'', ..., u(P)^{(n)}), \quad P \in U(R)$$

where $u = (u_1, ..., u_N)$ is an $N-$uple of regular functions on $U$ (so $u(P) \in R^N$) and $\Phi$ is an element in the $p-$adic completion of the ring of polynomials with coefficients in $R$ in $N(n+1)$ indeterminates. Denote by $\mathcal{O}^n(X)$ the ring of $\delta-$formal functions of order $\leq n$ on $X(R)$. A function in $\mathcal{O}^n(X) \backslash \mathcal{O}^{n-1}(X)$ will be called *of order* $n$ (rather than $\leq n$).

In what follows, if $A/R$ is a commutative group scheme of finite type , by a $\delta-$character of $A(R)$ we understand a $\delta-$formal function $\psi : A(R) \rightarrow R = \mathbf{G}_a(R)$ (of some order $n \in \mathbf{N}$) which is also an (additive) group homomorphism. Consider the intersection

$$A^\sharp(R) := \bigcap_\psi Ker\ \psi \subset A(R)$$

where $\psi$ runs through the set of all $\delta-$characters of $A(R)$. Then of course $A^\sharp(R)$ contains the intersection

$$p^\infty A(R) := \bigcap_n p^n A(R) \subset A(R)$$

If for example $A = \mathbf{G}_{m,R}^N$ is a linear torus then it is easy to see that actually $A^\sharp(R) = p^\infty A(R)$; cf. Remark 4 below. Our main result will say that $A^\sharp(R)$ is still close to $p^\infty A(R)$ in case $A/R$ is an abelian scheme. To state our result recall that A(R) has a natural structure of proalgebraic group over $k$ in the sense of Serre [S2] given by the theory of Greenberg transform; cf., say, [Ray]. (Alternatively and equivalently, in the notations of Part I, section 2, this proalgebraic structure is defined by the surjective maps $\pi_n : A(R) \simeq A_0^\infty(k) \rightarrow A_0^n(k)$ where $A_0^\infty, A_0^n$ are the reduction modulo $p$ of the $p-$jet spaces of $A$). Now as we shall easily check $A^\sharp(R)$ is a proalgebraic subgroup of $A(R)$ (actually this holds for any intersection of kernels of $\delta-$characters of $A(R)$). In particular we may consider the identity component $A^\sharp(R)^\circ$ of $A^\sharp(R)$ in the sense of proalgebraic groups [S2] (defined, in our notations of Part I, as the inverse limit of the identity components of $\pi_n(A^\sharp(R))$). On the other hand it is well known [Ray] p.10 and easy to check that $p^\infty A(R)$ is a connected proalgebraic subgroup of $A(R)$ (actually all groups $\pi_n(p^\infty A(R))$ are abelian varieties isogenous to $A_0 := A \otimes k$). So we have trivially that $p^\infty A(R) \subset A^\sharp(R)^\circ$.

Here is our main result, which is an analogue of the Manin-Chai "Theorem of the kernel" [Man], [Ch]:

**Theorem A.** *Let $A/R$ be an abelian scheme. Then we have $A^\sharp(R)^\circ = p^\infty A(R)$.*

So Theorem A says that there are enough $\delta-$characters in order for the intersection of their kernels to have the minimum possible identity component. Now we address the question of how many $\delta-$characters one needs to achieve this and what is their minimum order. We succeed to answer this question in the "extreme" cases: the "most degenerate" and the "generic case" respectively; cf. assertions 1) and 2) in the Theorem below respectively:

**Theorem B.** *Assume $A/R$ is an abelian scheme of relative dimension $g$. Then the following hold:*

*1) One can find $R-$linearly independent first order $\delta-$characters $\psi_1, ..., \psi_g$ of $A(R)$ if and only if there exists a $\phi-$endomorphism of the completion $\hat{A}/R$ lifting the Frobenius of the closed fibre $A_0/k$. In this case we have $(\cap_{i=1}^g Ker\ \psi_i)^\circ = p^\infty A(R)$.*

*2) Assume $A(R)$ has no first order $\delta-$characters. Then there exist $\delta-$characters $\psi_1,...,\psi_g$ of $A(R)$ of order 2 such that $(\cap_{i=1}^g Ker\ \psi_i)^\circ = p^\infty A(R)$.*

In the case of ordinary reduction, we can be more precise about when we find ourselves in one of the situations 1) or 2) in Theorem B:

**Theorem C.** *Assume the closed fibre $A_0/k$ of the abelian scheme $A/R$ is ordinary and let $q_{ij}(A) \in 1 + pR$, $1 \leq i,j \leq g$ be its Serre-Tate parameters [Ka]. Then the following hold:*

*1) There exist $g$ linearly independent first order $\delta-$characters of $A(R)$ if and only if $q_{ij}(A) = 1$ for all $i,j$ (i.e. $\hat{A}/R$ is the canonical lifting of $A_0/k$).*

*2) Assume $det((q_{ij}(A) - 1)/p) \in R^*$. Then there exist no first order $\delta-$characters of $A(R)$.*

Finally let us discuss the "power series extensions" of our $\delta-$characters. Start with the remark that if $X/R$ is smooth then any $\delta-$formal function $\varphi : X(R) \to R$ may be canonically extended to a map $\varphi_t : X(R[[t]]) \to R[[t]]$. (Cf. (1.2) below; essetially what one does is to define $\varphi_t$ using the same local formula $\Phi(u, u', ..., u^{(n)})$ which defines $\varphi$, where we extend $\phi : R \to R$ to $\phi : R[[t]] \to R[[t]]$ by letting $\phi(t) = t^p$). If $X = A/R$ is in addition a commutative group scheme then for any $\delta-$character $\psi : A(R) \to R$ the map $\psi_t : A(R[[t]]) \to R[[t]]$ is a group homomorphism into the additive group $R[[t]]$. For $A/R$ as above we define

$$A^\sharp(R[[t]]) := \bigcap_{\psi} Ker\ \psi_t \subset A(R[[t]])$$

where $\psi$ runs through the set of all $\delta-$characters of $A(R)$. Also we set

$$A(R[[t]])_{pt} := Ker(A(R[[t]]) \to A(R[[t]]/ptR[[t]]))$$

(We have a non canonical bijection $A(R[[t]])_{pt} \simeq (ptR[[t]])^g$ where $g$ is the relative dimension of $A/R$.) Then we have the following:

**Theorem D.** *Let $A/R$ be an abelian scheme. Then $A^\sharp(R[[t]]) \cap A(R[[t]])_{pt} = 0$. Furthermore, if $\psi_1, ..., \psi_g$ are as in 1) or 2) in Theorem B then the induced homomorphism*

$$(\psi_{1t}, ..., \psi_{gt}) : A(R[[t]])_{pt} \to (tR[[t]])^g$$

*is injective.*

**Remarks.** 1) The $\delta-$characters appearing in the Theorems above are *not* analytic functions; so they are very different from, say, the "Bourbaki logarithm" and the $p-$adic abelian integrals of Coleman [Co].

2) The $g-$uple of order one maps $\psi_1, ..., \psi_g$ in assertion 1) of Theorem B should be viewed as an analogue, in our theory, of Kolchin's logarithmic derivative [K1]. The situation in assertion 1) of Theorem A should be viewed as the "most degenerate case"; cf. assertion 1) in Theorem C. On the other hand, the corresponding $g-$uple of order two maps in assertion 2) of Theorem B should be viewed as a $p-$adic analogue of the "Manin map" [Man] [B1]. This situation should be viewed as the "generic one"; cf. assertion 2) in Theorem C.

3) In the case of elliptic curves ($g = 1$) assertions 1) and 2) in Theorem B provide a complete picture of the story: either there exists a $\delta-$character $\psi$ of order one (which happens if and only the Frobenius of $A_0/k$ lifts to $\hat{A}$) or, if not, there exists a $\delta-$character $\psi$ of order two. In both cases $(ker\ \psi)^\circ = p^\infty A(R)$.

4) By the way, it is instructive to note that the whole theory above has an analogue in the case of linear tori, which is already quite interesting, although easy to check. Here the whole story takes place at the level of order one $\delta-$characters (which is not surprising since linear tori should be viewed as analogues of canonically lifted abelian schemes). Indeed for $A = \mathbf{G}_m$ the map $\psi : \mathbf{G}_m(R) = R^* \to \mathbf{G}_a(R) = R$:

$$\psi(x) = \frac{1}{p} log(\phi(x)/x^p) = x'x^{-p} - \frac{p}{2}(x'x^{-p})^2 + \frac{p^2}{3}(x'x^{-p})^3 - \dots$$

is a $\delta-$character of order one. Its kernel is precisely the image of the Teichmuller character $\theta : k^* \to R^*$ and the latter is known to be equal to $\cap(R^*)^{p^n}$. So in this case we see that $A^{\sharp}(R) = p^\infty A(R)$. Note also that the induced homomorphism $\psi_t : (R[[t]])^* \to R[[t]]$ is the so called $p-$adic logarithm [FV] p.169 (taken actually with a minus sign); this map and its inverse defined on $tR[[t]]$ (called in [FV] the Artine-Hasse-Shafarevich map) play an interesting role in "explicit local class field theory"; in some of these class field theoretic applications, these functions are usefully combined with the 'usual" logarithmic derivative $(R[[t]])^* \to R[[t]], f \mapsto f^{-1}(df/dt)$.

All this suggests a number of intriguing questions in the case of abelian schemes $A/R$. What is the structure of the group $A^{\sharp}(R)/A^{\sharp}(R)^\circ$ in this case ? Is this group always finite ? What is the image of the injective map $(\psi_{1t}, ..., \psi_{gt}) : A(R[[t]])_{pt} \to (tR[[t]])^g$ in Theorem D ? The inverse of this map (defined on the image) would be an analogue of the Artine-Hasse-Shafarevich map. These maps should also have a class field theoretic relevance. Even more intriguing is the question of "putting together" the $\delta-$characters $\psi_t : A(R[[t]]) \to R[[t]]$ constructed in the present paper and the "classical Manin maps" $A(R[[t]]) \to R[[t]]$ as defined, say, in [B1] using the "usual" derivation $d/dt$.

Finally the above considerations suggest that much of the Cassidy-Kolchin theory of differential algebraic groups [C1,C2], [K2] and much of our theory in [B4] has a $p-$adic analogue.

5) Assertion 1) in Theorem C is just a reformulation of part of assertion 1) in Theorem B, because it is well known that, under the assumption $A_0/k$ is ordinary, the condition that the Frobenius of $A_0/k$ lifts to a $\phi-$endomorphism of $\hat{A}/R$ is equivalent to $\hat{A}/R$ being the canonical lifting; cf. [Me]. As for assertion 2) in Theorem C note that the

condition $det((q_{ij}(A) - 1)/p) \in R^*$ is satisfied for a generic choice of the Serre-Tate parameters and is actually a condition which can be checked modulo $p^2$. By the way, this condition is equivalent to $det(\delta q_{ij}(A)) \in R^*$ because $det(\delta q_{ij}(A))$ is congruent modulo $p$ to $(det((q_{ij}(A) - 1)/p))^p$.

The paper is organized as follows. The first section will contain some complements to the material of Part I. Section 2 is devoted to the description of the interaction between $p-$jets and formal groups. In Section 3 we complete the proof of Theorems A and B. Section 4 is devoted to the proof of Theorem C.

**Acknowledgement.** The author would like to thank the Max Planck Institut fur Mathematik in Bonn for support and hospitality during 1994/95. He is also endebted to I.B.Fesenko and F.Voloch for useful conversations.

## 1. Complements to Part I.

(1.1) It is convenient to introduce the following ad hoc terminology. By a *$p-$formal scheme* we shall understand a noetherian formal scheme $X/R$ such that $p\mathcal{O}_X$ is an ideal of definition for $X$. The fibre product of two objects $X$ and $Y$ over a third $Z$ in the category of $p-$formal schemes will be denoted by $X\hat{\times}_Z Y$. By a *$p-$formal group scheme* we shall understand a group object in the category of $p-$formal schemes. So a $p-$formal scheme is *not* a formal group. By the way, the upper $\hat{}$ will always denote the $p-$adic completion; so for instance if $G/R$ is a group scheme then $\hat{G}/R$ will denote the associated $p-$formal group scheme (i.e. the $p-$adic completion) and *not* the associated formal group (i.e. the $m-$adic completion, where $m$ is the ideal of the closed point of the zero section). This distinction is important because we shall encounter, in what follows, both $p-$formal group schemes *and* formal groups.

Let $B$ be a ring and $x$ a finite family of indeterminates. Then we shall identify the completion $B[x]\hat{}$ with the subring of $\hat{B}[[x]]$ whose elements are the restricted power series (recall that *restricted* means "whose coefficients tend $p-$adically to 0"). Note also that $R[x]\hat{} \otimes_R K$ identifies with the ring of restricted power series in $K[[x]]$.

Finally, as a general notational convention, the letter $F$ will always denote the absolute Frobenius of a scheme over $\mathbf{F}_p$ whereas the letter $\phi$ will be systematically used to denote endomorphisms of schemes $X/R$ which lift the absolute Frobenius $F$ of the closed fibre $X_0$.

(1.2) Let us quickly review the main construction in Part I. Recall that a $p-$derivation of a ring homomorphism $f : A \rightarrow B$ is a map of sets $\delta : A \rightarrow B$ such that the induced map $(f, \delta) : A \rightarrow B \times B = W_2(B)$, $x \mapsto (f(x), \delta(x))$ is a ring homomorphism. Here $W_2(-)$ is the "ring of Witt vectors of length 2" over a given ring. (E.g. the map $\delta : R \rightarrow R$ from the Introduction is a $p-$derivation of the identity.)

For any finitely generated $R$–algebra $B$ we defined in Part I a sequence of algebras

$$R = B^{-1} \xrightarrow{f^0} B = B^0 \xrightarrow{f^1} B^1 \to \dots \to B^{n-1} \xrightarrow{f^n} B^n \to \dots$$

together with $p$–derivations $\delta : B^{n-1} \to B^n$ ($n \geq 1$) of $f^n$ where $f^n \circ \delta = \delta \circ f^{n-1}$, satisfying the following universality property ($UP$): for any ring homomorphism $g : B^{n-1} \to C$ and any $p$–derivation $\partial : B^{n-1} \to C$ such that $\partial \circ f^{n-1} = g \circ \delta : B^{n-2} \to C$, there exists a unique ring homomorphism $u : B^n \to C$ such that $g = u \circ f^n$ and $\partial = u \circ \delta$. The $p$–derivations $\delta$ extend to $p$–derivations still denoted by $\delta : (B^{n-1})\hat{} \to (B^n)\hat{}$ of $\hat{f} : (B^{n-1})\hat{} \to (B^n)\hat{}$ which have the following universality property ($UP\hat{}$): for any ring homomorphism $g : (B^{n-1})\hat{} \to C$ into a $p$–adically complete ring $C$ and for any $p$–derivation $\partial : (B^{n-1})\hat{} \to C$ such that $\partial \circ \hat{f}^{n-1} = g \circ \delta : (B^{n-2})\hat{} \to C$, there exists a unique ring homomorphism $u : (B^n)\hat{} \to C$ such that $g = u \circ \hat{f}^n$ and $\partial = u \circ \delta$.

Using this universality property one sees that for any element $s \in B$ the natural homomorphisms $((B^n)_s)\hat{} \to ((B_s)^n)\hat{}$ are isomorphisms. This allows one to globalize the construction: for any scheme of finite type $X/R$ we have a projective system

$$\dots \to X^n \to X^{n-1} \to \dots \to X^1 \to X^0 = \hat{X}$$

of $p$–formal schemes with $p$–derivations $\delta$ of $\mathcal{O}_{X_{n-1}}$ into the direct image of $\mathcal{O}_{X_n}$ satisfying the obvious analogue universality property ($UP\hat{}$). The $p$–formal scheme $X^n$ is called the $p$–jet space of $X$ order $n$. It follows from Part I, (2.12), that one has natural homomorphisms $\mathcal{O}(X^n) \to \mathcal{O}^n(X)$, which is actually an isomorphism, in case $X/R$ is smooth. So in particular, for $X/R$ smooth, and $U \subset X$ an affine open subset, the ring $\mathcal{O}^n(U) \otimes K$ is an affinoid algebra in the sense of [FvP]. Also note that if $X/R$ is smooth, for any $\varphi \in \mathcal{O}^n(X)$ we have an induced map $\varphi_t : X(R[[t]]) \to R[[t]]$. Indeed consider the unique $p$–derivation $\delta : R[[t]] \to R[[t]]$ extending $\delta : R \to R$ such that $\delta t = 0$. By the above $f$ is given by a morphism of $p$–formal schemes $\tilde{f} : X^n \to (\mathbf{A}^1)\hat{}$. By the universality property ($UP\hat{}$) any morphism $Spec\ R[[t]] \to X$ lifts to a morphism $Spf\ R[[t]] \to X^n$ which by composition with $\tilde{f}$ gives a morphism $Spf\ R[[t]] \to (\mathbf{A}^1)\hat{}$ hence an element of $R[[t]]$. This provides us with the desired map $\varphi_t : X(R[[t]]) \to R[[t]]$.

We will need the following

**Lemma (1.3).** *Let $u : A \to B$ be an etale ring homomorphism and $v : B \to C$ a ring homomorphism into a $p$–adically complete ring $C$. Then any $p$–derivation of $v \circ u$ lifts uniquely to a $p$–derivation of $v$.*

*Proof.* We may assume $p^n C = 0$ for some $n$. Set $f = v \circ u$, let $\delta$ be a $p$–derivation of $f$, and consider the commutative diagram

$$\begin{tikzcd} A \arrow[r, "u"] \arrow[d, "{(f,\delta)}"'] & B \arrow[d, "v"] \\ W_2(C) \arrow[r, "p_1"] & C \end{tikzcd}$$

where $p_1$ is the first projection. Since $u$ is etale and $(Ker\ p_1)^{n-1} = 0$, there exists a unique ring homomorphism $\sigma : B \to W_2(C)$ such that $p_1 \circ \sigma = v$ and $\sigma \circ u = (f, \delta)$ which means exactly that $\delta$ extends uniquely to a $p-$derivation of $v$.

**Proposition (1.4).** *Let $u : R[x] \to B$ be an etale morphism, where $x$ is a finite family of indeterminates. Let $x', x'', ..., x^{(n)}$ be $n$ families of new indeterminates indexed by the same set as $x$. Then the natural homomorphism*

$$B[x', x'', ..., x^{(n)}]\hat{} \to (B^n)\hat{}$$

*(sending $x^{(i)}$ into $u(x)^{(i)}$) is an isomorphism*

**Corollary (1.5) (Local product property).** *Let $X/R$ be a smooth scheme of finite type of relative dimension $g$. Then each point in $X$ has an affine open neighbourhood $U$ such that the $p-$jet spaces of $U$ have the following product decomposition (as $p-$formal schemes):*

$$U^n \simeq \hat{U} \hat{\times} (\mathbf{A}^{gn})\hat{}$$

*Moreover the projections $U^{n+1} \to U^n$ correspond, under the above isomorphisms, to the projections $(\mathbf{A}^{g(n+1)})\hat{} = (\mathbf{A}^{gn})\hat{}\hat{\times}(\mathbf{A}^g)\hat{} \to (\mathbf{A}^{gn})\hat{}$.*

**Corollary (1.6).** *Let $X/R$ be a smooth scheme of finite type such that the closed fibre $X_0/k$ is connected. Then the rings $\mathcal{O}^n(X)$ are integral domains for all $n \geq 0$.*

(1.7) *Proof of (1.4).* Consider the unique $p-$derivations of the inclusions

$$R[x] \xrightarrow{\delta} R[x, x'] \xrightarrow{\delta} R[x, x', x''] \to ...$$

sending $x$ into $x'$, $x'$ into $x''$ a.s.o. By the existence statement in Lemma (1.3) these $p-$derivations lift to $p-$derivations

$$. \qquad B \xrightarrow{\delta} B[x']\hat{}, B[x'] \xrightarrow{\delta} B[x', x'']\hat{}, ...$$

The latter $p-$derivations induce $p-$derivations

$$\hat{B} \xrightarrow{\delta} B[x']\hat{} \xrightarrow{\delta} B[x', x'']\hat{} \xrightarrow{\delta} ...$$

By the uniqueness statement in Lemma (1.3) each $p-$derivation in this sequence prolongs the preceeding one. To conclude it is enough to check that the last sequence of $p-$derivations satisfy the universality property of the sequence

$$\hat{B} \xrightarrow{\delta} (B^1)\hat{} \xrightarrow{\delta} (B^2)\hat{} \xrightarrow{\delta} ...$$

cf. $(UP\hat{})$ in (1.2); but this is a trivial exercise using the unicity in Lemma (1.3).

## 2. $p$−jets of group schemes and formal groups.

(2.1) Let $f = f(x_1, x_2) \in R[[x_1, x_2]]^g$ be a (not necessarily commutative) formal group law in $g$ variables (so $x_1, x_2$ are $g$−uples of variables). Then for each integer $n \geq 1$ the $g$−uple of power series $p^{-n} f^{\phi^n}(p^n x_1, p^n x_2)$ is actually a $g$−uple of restricted power series (so it belongs to $(R[x_1, x_2]\hat{})^g$) hence it defines a structure of $p$−formal group scheme on the $p$−adic completion of the affine space of dimension $g$; we denote this $p$−formal group scheme by $((\mathbf{A}^g)\hat{}, p^{-n} f^{\phi^n}(p^n x_1, p^n x_2))$. Here of course $f^{\phi^n}$ is the $g$−uple of series $f$ with coefficients acted by $\phi^n$.

**Proposition (2.2).** *Let $G/R$ be a smooth group scheme of finite type of relative dimension $g$. Let $f \in R[[x_1, x_2]]^g$ be the formal group law associated to $G/R$. Then the kernel of $G^n \to G^{n-1}$ is isomorphic as a $p$−formal group scheme to $((\mathbf{A}^g)\hat{}, p^{-n} f^{\phi^n}(p^n x_1, p^n x_2))$.*

In defining $f$ above one starts of course with a regular system of parameters $x$ of the local ring $\mathcal{O}_{G,e}$ of $G$ at the generic point of the zero section (we may assume $x$ is contained in the local ring $\mathcal{O}_{G,0}$ of $G$ at the closed point 0 of the zero section). Fixing such a $g$−uple $x$ provides inclusions $R[x] \subset \mathcal{O}_{G,0} \subset R[[x]]$ where $R[[x]]$ identifies with the completion of $\mathcal{O}_{G,0}$ in the $m$−adic topology, and then $f$ is defined as the image of $x$ under the comultiplication $R[[x]] \to R[[x_1, x_2]]$.

*Proof.* In notations above, the compatibility of $\delta$ with the "counits" $e : \mathcal{O}_{G^n,0} \to R$ shows that the $p$−derivatives $x', x'', ..., x^{(n)}$ belong to the maximal ideal of the local ring $\mathcal{O}_{G^n,e}$ of $G^n$ at the generic point of the zero section, and hence to the maximal ideal of $\mathcal{O}_{G^n,0}$. So we get inclusions $R[x, x', ..., x^{(n)}] \subset \mathcal{O}_{G^n,0} \subset R[[x, x', ..., x^{(n)}]]$, where $R[[x, x', ..., x^{(n)}]]$ identifies with the $m$−adic completion of $\mathcal{O}_{G^n,0}$ (due to the Local product property (1.5)). The Proposition will be proved if we can construct, for any $p$−adically complete ring $C$ a group isomorphism

$$Hom(Spf\ C, Ker(G^n \to G^{n-1})) \simeq Hom(Spf\ C, ((\mathbf{A}^g)\hat{}, p^{-n} f^{\phi^n}(p^n x_1, p^n x_2))$$

which behaves functorially in $C$. Here of course $Hom$ stands for "morphisms in the category of $p$−formal schemes". We have a functorial bijection of sets

$$Hom(Spf\ C, (\mathbf{A}^g)\hat{}) \simeq C^g$$

defined by associating to each morphism $Spf\ C \to (\mathbf{A}^g)\hat{} = Spf\ R[t]\hat{}$ , $t = \{t_1, ..., t_g\}$ the images of $t_1, ..., t_g$ via the corresponding map $R[t]\hat{} \to C$. Also, we may define a map

$$Hom(Spf\ C, Ker(G^n \to G^{n-1})) \to C^g$$

as follows. By the universality property $(UP^{\hat{}})$ in (1.2), morphisms

$$Spf\ C \to Ker(G^n \to G^{n-1})$$

are in bijection with $p-$derivations $\partial : \mathcal{O}_{G^{n-1},0} \to C$ of the homomorphism $e : \mathcal{O}_{G^{n-1},0} \to R \to C$ (where $e(x) = e(x') = ... = e(x^{(n-1)}) = 0$) with the property that $\partial$ restricted to $\mathcal{O}_{G^{n-2},0}$ is equal to the composition $\mathcal{O}_{G^{n-2},0} \xrightarrow{\delta} \mathcal{O}_{G^{n-1},0} \xrightarrow{e} C$. Then we attach to each morphism $Spf\ C \to Ker(G^n \to G^{n-1})$ the $g-$uple $\partial x^{(n-1)} \in C^g$. We claim that the map $\partial \mapsto \partial x^{(n-1)}$ is bijective. It is certainly injective because $\partial$ is uniquely determined by its values at $x, x', ..., x^{(n-1)}$ (due to Lemma (1.3)). To check it is surjective pick up any $g-$uple $c \in C^g$ and consider the $p-$derivation $\partial_c : R[x, x', ..., x^{(n-1)}] \to C$ defined by the formula

$$\partial_c h = (\delta h)(0, ..., 0, c) = (h^{\phi}(0, ..., 0, pc) - (h(0, ..., 0, 0))^p)/p, \ \ h \in R[x, x', ..., x^{(n-1)}]$$

where $\delta : R[x, x', ..., x^{(n-1)}] \to R[x, x', ..., x^{(n)}]$ is the unique $p-$derivation sending $x$ into $x'$, $x'$ into $x''$, a.s.o. Note that $\partial$ and $\partial_c$ agree on $R[x, x', ..., x^{(n-1)}]$. But now the formula defining $\partial_c$ makes sense for any power series $h$ rather than any polynomial (because $C$ is $p-$adically complete) so $\partial_c$ can be prolonged to a $p-$derivation (still denoted by) $\partial_c : R[[x, x', ..., x^{(n-1)}]] \to C$ of the homomorphism $R[[x, x', ..., x^{(n-1)}]] \to C$, $x \mapsto 0, ..., x^{(n-1)} \mapsto 0$. Restricting $\partial_c$ back to $\mathcal{O}_{G^{n-1},0}$ we get a $p-$derivation (still denoted by) $\partial_c : \mathcal{O}_{G^{n-1},0} \to C$ of $e$, which must be equal to $\partial$ in view of the unicity statement in Lemma (1.3).

Composing the bijections constructed above we get a bijection

$$Hom(Spf\ C, Ker(G^n \to G^{n-1})) \simeq C^g \simeq Hom(Spf\ C, (\mathbf{A}^g)^{\hat{}})$$

Let us check that this is a group homomorphism. Start with two elements in

$$Hom(Spf\ C, Ker(G^n \to G^{n-1}))$$

As noted above they correspond to two $p-$derivations $\partial_1, \partial_2 : \mathcal{O}_{G^{n-1},0} \to C$. The product, under the group law, of the two elements we have choosen corresponds to the $p-$derivation:

$$\partial_1 \cdot \partial_2 : \mathcal{O}_{G^{n-1},0} \xrightarrow{\mu} \mathcal{O}_{G^{n-1} \hat{\times} G^{n-1},(0,0)} \xrightarrow{(\partial_1,\partial_2)} C$$

where $\mu$ is the comultiplication and $(\partial_1, \partial_2)$ is the unique $p-$derivation inducing $\partial_1$ and $\partial_2$ when restricted to the two factors. Set $c_1 = \partial_1 x^{(n-1)} \in C^g$ and $c_2 = \partial_2 x^{(n-1)} \in C^g$. Now $\partial_1 \cdot \partial_2$ is the restriction of the following $p-$derivation:

$$R[[x, x', ..., x^{(n-1)}]] \xrightarrow{M} R[[x_1, x_1', ..., x_1^{(n-1)}, x_2, x_2', ..., x_2^{(n-1)}]] \xrightarrow{(\partial_{c_1},\partial_{c_2})} C$$

where $M(x) = f, ..., M(x^{(n-1)}) = f^{(n-1)}$. We get

$$(\partial_1 \cdot \partial_2)(x^{(n-1)}) = (\partial_{c_1}, \partial_{c_2})(f^{(n-1)}) = f^{(n)}(0, ..., 0, c_1, 0, ..., 0, c_2) = p^{-n} f^{\phi^n}(p^n c_1, p^n c_2)$$

which closes the proof of the Proposition.

In the commutative case one can be more specific due to the following Lemma (this is the only place where we use our assumption that $p \neq 2$) :

**Lemma (2.3).** *In notations of (2.1) assume $f$ is commutative. Then we have an isomorphism of $p-$formal group schemes*

$$((\mathbf{A}^g)^\wedge, p^{-n} f^{\phi^n}(p^n x_1, p^n x_2)) \simeq (\mathbf{G}_a^g)^\wedge := ((\mathbf{A}^g)^\wedge, x_1 + x_2)$$

*Proof.* Of course we may assume $n = 1$. It is enough to prove that the power series (with coefficients in $K$) defining the logarithm $log_{f_1}$ and the exponential $exp_{f_1}$ of the formal group law $f_1(x_1, x_2) := p^{-1} f^{\phi}(px_1, px_2)$ have actually coefficients in $R$ and are restricted. By [Haz] p.31, Remark (5.4.8) together with Remark (11.1.6) at p. 64, for each $n \geq 1$ there exist $g-$uples $b_{n0}(x), ..., b_{nn}(x) \in R[[x]]^g$, $b_{n0}(x) = x+$(terms of degree $\geq 2$), $b_{ni}(0) = 0$, such that

$$[p^n]_{f^\phi}(x) = p^n b_{n0}(x) + p^{n-1} b_{n1}(x^p) + ... + p b_{n,n-1}(x^{p^{n-1}}) + b_{nn}(x^{p^n})$$

where $[p^n]_{f^\phi}$ is the "multiplication by $p^n$ with respect to the formal group $f^\phi$. On the other hand by [Haz] p. 64, formula (11.1.7), we have

$$log_{f_1}(x) = lim_{n \to \infty} p^{-n} [p^n]_{f_1}(x)$$

Now

$$p^{-n}[p^n]_{f_1}(x) = p^{-(n+1)}[p^n]_{f^\phi}(px) = \sum_{i=0}^{n} p^{-(i+1)} b_{ni}(p^{p^i} x^{p^i})$$

Let $\alpha = (\alpha_1, ..., \alpha_g) \in \mathbf{N}^g$ be a multiindex with $|\alpha| := \alpha_1 + ... + \alpha_g \geq 2$. Then the coefficient $l_{\alpha,n,i}$ of $x^\alpha$ in $p^{-(i+1)} b_{ni}(p^{p^i} x^{p^i})$ has valuation $v_p(l_{\alpha,n,i}) \geq |\alpha| - i - 1$. Now if $l_{\alpha,n,i} \neq 0$ we must have $|\alpha| \geq p^i$ hence we get $i \leq log_p|\alpha|$ and $|\alpha| - i - 1 \geq 1$ (here we used the fact that $p \geq 3$). Consequently we have

$$v_p(l_{\alpha,n,i}) \geq M(\alpha) := max\{1, |\alpha| - log_p|\alpha| - 1\}$$

and hence if we denote by $l_\alpha$ the coefficient of $x^\alpha$ in $log_{f_1}(x)$ we will still have $v_p(l_\alpha) \geq M(\alpha)$. Since $M(\alpha)$ is $\geq 1$ and goes to $\infty$ as $|\alpha| \to \infty$ we may write $log_{f_1}(x) = x - ph(x)$ where $h \in (R[x]^\wedge)^g$ is restricted. In particular $log_{f_1}(x) \in (R[x]^\wedge)^g$ is also restricted. To get $e(x) := exp_{f_1}(x)$ we have to solve the equation $e(x) - ph(e(x)) = x$. As usual one finds $e(x)$ as a limit $e(x) = lim_{n \to \infty} e_n(x)$ where $e_1(x) := x$ and $e_{n+1}(x) := x + ph(e_n(x))$; note that $e_n(x)$ converge $p-$adically and are restricted, with $R-$coefficients (being compositions of restricted series with $R-$coefficients) so $e(x)$ exists and is restricted, with $R-$coefficients, which closes the proof of the Lemma.

**Remark.** In the case of characteristic $p = 2$, $log_{f_1}(x)$ is still with $R-$coefficients and restricted, but $exp_{f_1}(x)$ may fail to be restricted. For instance in case $g = 1$ and $f = x_1 + x_2 + x_1 x_2$, $log_{f_1}(x)$ is congruent to $x - x^2$ modulo 2 while $exp_{f_1}(x)$ is congruent to $x + x^2 + x^4 + x^8 + ...$ modulo 2.

To state the next Corollary it is convenient to make the following definition. Let $B_1, B_2, B$ be $p-$formal group schemes. We say that $B$ is a regular (respectively locally regular) extension of $B_2$ by $B_1$ if there exists a homomorphism $B \to B_2$ admitting a section in the category of $p-$formal schemes (respectively admitting such sections locally in the Zariski topology) such that $B_1 \simeq Ker(B \to B_2)$ as $p-$formal group schemes.

Putting together (2.2), (2.3) and the Local product property (1.5) we get:

**Corollary (2.4).** *Let $G/R$ be a smooth commutative group scheme of finite type of relative dimension $g$. Set $B_n = Ker(G^n \to G^0)$. Then $B_n$ is obtained as $n$ succesive regular extensions of $p-$formal group schemes of the form $(\mathbf{G}_a^g)^{\wedge}$; moreover $G^n$ is a locally regular extension of $G^0$ by $B_n$.*

To state the next lemma let us make a definition. Let $B$ be a $p-$formal group scheme whose undelying $p-$formal scheme is isomorphic to the $p-$adic completion of an affine space of dimension $N$. By a *system of coordinates* in $\mathcal{O}(B)$ we will understand an $N-$uple of elements $z = (z_1, ..., z_N)$, $z_i \in \mathcal{O}(B)$ such that $\mathcal{O}(B) = R[z]^{\wedge}$.

**Lemma (2.5).** *Let $B$ be a $p-$formal group scheme obtained by $N$ successive regular extensions of $p-$formal group schemes of the form $(\mathbf{G}_a)^{\wedge}$. Then there exists a homomorphism $\chi : B \to (\mathbf{G}_a^N)^{\wedge}$ and a system of coordinates $z$ in $\mathcal{O}(B)$ such that if $\xi$ is the canonical system of coordinates in $\mathcal{O}((\mathbf{G}_a^N)^{\wedge})$ then $det(\partial\chi^*\xi/\partial z) \in R\backslash\{0\}$.*

*Proof.* We proceed by induction on $N$. If $N = 1$ there is nothing to prove. Assume $B$ is a regular extension of $(\mathbf{G}_a)^{\wedge}$ by $B_1$ where $B_1$ is obtained by $N$ successive regular extensions of groups $(\mathbf{G}_a)^{\wedge}$. By the induction hypothesis there exists a homomorphism $\chi_1 : B_1 \to (\mathbf{G}_a^N)^{\wedge}$ and a system of coordinates $z = (z_1, ..., z_N)$ in $\mathcal{O}(B_1)$ such that $det(\partial\chi_1^*\xi/\partial z) \in R\backslash\{0\}$. If $s : (\mathbf{G}_a)^{\wedge} \to B$ is a section of the projection then we may identify as usual $B$ with $(\mathbf{G}_a)^{\wedge}\hat{\times}B_1$, with group law defined (at the level of points with values in $p-$adically complete $R-$algebras) by

$$(u_1, v_1) + (u_2, v_2) = (u_1 + u_2, v_1 + v_2 + f_1(u_1, u_2))$$

where $f_1 : (\mathbf{G}_a)^{\wedge}\hat{\times}(\mathbf{G}_a)^{\wedge} \to B_1$, $f_1(u_1, u_2) := s(u_1 + u_2) - s(u_1) - s(u_2)$. Consider the composition

$$f := \chi_1 \circ f_1 : (\mathbf{G}_a)^{\wedge}\hat{\times}(\mathbf{G}_a)^{\wedge} \to (\mathbf{G}_a^N)^{\wedge}$$

The components $f_\alpha$ of $f$ are symmetric cocycles so $f_\alpha \in R[u_1, u_2]^{\wedge}$. Then each homogenous component $f_{\alpha m}$ of degree $m$ of $f_\alpha$ will be a symmetric cocycle. By a fundamental lemma of Lazard [Laz], Lemma 3, p.257 , we must have $f_{\alpha m} = r_{\alpha m}C_m$ where $C_m$ is either $C_m := (u_1 + u_2)^m - u_1^m - u_2^m$ if $m$ is not a power of $p$ or $C_m = C_{p^n} := ((u_1 + u_2)^{p^n} - u_1^{p^n} - u_2^{p^n})/p$ if $m = p^n$. So we must have $r_{\alpha m} \to \infty$ as $m \to \infty$. So replacing $f_\alpha$ by the coboundary of some restricted power series with $R-$coefficients we may write

$$f = \sum_n r_n C_{p^n}(u_1, u_2)$$

where the sum is finite, $f$ is viewed as a $g \times 1$ matrix and $r_n$ are $g \times 1$ matrices with entries in $R$. Define

$$\chi : B = (\mathbf{G}_a)^{\wedge}\hat{\times}B_1 \to (\mathbf{G}_a)^{\wedge}\hat{\times}(\mathbf{G}_a^N)^{\wedge}$$

by the formula

$$\chi(u,v) = (u, \sum_n r_n u^{p^n} - p\chi_1(v))$$

Let $z_0 = \xi_0$ be the canonical system of coordinates on $(\mathbf{G}_a)^{\wedge}$ and consider the system of coordinates $z_0, z_1, ..., z_N$ on $\mathcal{O}(B)$. Then the condition on the Jacobian of $\chi$ follows trivially from the condition on the Jacobian of $\chi_1$.

## 3. Construction of $\delta$–characters.

(3.1) Let's prove Theorem A. Set $B_n := Ker(A^n \to A^0)$ and let $U_i$ be a Zariski open covering of $A$ over which $A^n \to A^0$ admits sections. By the usual yoga of extensions of groups which locally admit a section [S1] $A^n$ is obtained by gluing $p$–formal schemes $U_i^n = (U_i)^{\wedge}\hat{\times}B_n$ via maps $(U_{ij})^{\wedge}\hat{\times}B_n \to (U_{ij})^{\wedge}\hat{\times}B_n$ given at the level of points by

$$(u,v) \mapsto (u, v + \gamma_{ij}(u))$$

where $\gamma_{ij} : (U_{ij})^{\wedge} \to B_n$ form a cocycle with respect to addition in $B_n$. By Lemma (2.5) we may find a homomorphism $\chi : B_n \to (\mathbf{G}_a^{ng})^{\wedge}$ and a system of coordinates $z$ on $\mathcal{O}(B_n)$ such that if $\xi$ is the canonical system of coordinates on $(\mathbf{G}_a^{ng})^{\wedge}$ then $det(\partial\chi^*\xi/\partial z) \in K^*$. Then the maps

$$\chi \circ \gamma_{ij} : (U_{ij})^{\wedge} \to (\mathbf{G}_a^{ng})^{\wedge}$$

define an $ng$–uple of classes $[\chi \circ \gamma_{ij}] \in H^1(A, \mathcal{O}_A)^{ng} \simeq H^1(\hat{A}, \mathcal{O}_{\hat{A}})^{ng}$. Since the latter is a free $R$–module of rank $g$ there exists a $(n-1)g \times ng$ matrix $m$ with entries in $R$ such that $m[\chi \circ \gamma_{ij}] = 0$. So we may write

$$m(\chi \circ \gamma_{ij}) = a_i - a_j$$

where $a_i$ are $(n-1)g \times 1$ matrices with entries in $C_i := \mathcal{O}((U_i)^{\wedge})$. Now consider the maps

$$\Psi_i : U_i^n = (U_i)^{\wedge}\hat{\times}B_n \to (\mathbf{G}_a^{(n-1)g})^{\wedge}$$

defined by the formula

$$\Psi_i(u,v) = m \cdot \chi(v) + a_i(u)$$

Clearly $\Psi_i$ glue together to give a map $\Psi : A^n \to (\mathbf{G}_a^{(n-1)g})^{\wedge}$. We claim this map is a homomorphism. Indeed its components $\Psi^{\alpha} : A^n \to (\mathbf{G}_a)^{\wedge}$ are "affine" on the fibres of $A^n \to A^0$ (i.e. $\Psi^{\alpha}(u+v) = \Psi^{\alpha}(u) + \Psi^{\alpha}(v)$ for $u \in A^n$ and $v \in B_n$); this plus the fact that $H^0(\hat{A}, \mathcal{O}_{\hat{A}}) = R$ formally imply that $\Psi^{\alpha}$ are group homomorphisms. Then the maps $\Psi_i$ correspond to elements (still denoted by)

$$\Psi_i := m \cdot \chi^*\xi + a_i \in C_i[z]^{\wedge}$$

Then the matrix

$$(\partial\Psi^{\alpha}/\partial z_{\beta}) = m\cdot(\partial\chi^{*}\xi/\partial z)$$

must contain a $(n-1)g \times (n-1)g$ minor belonging to $K^{*}$. We get that

$$dim((\mathcal{O}^{n}(U_i^n)/(\Psi))\otimes K) = dim(C_i[\xi]^{\hat{}}\otimes K/(\Psi)) \leq dim\ C_i + ng - (n-1)g = 2g$$

To establish the last inequality use the fact that the rings $C_i\otimes K$ and $C_i[\xi]^{\hat{}}\otimes K$ are affinoid algebras and one may simply use the description of the Krull dimension of affinoid algebras in terms of the finite module of Kahler differentials, and hence in terms of Jacobian matrices [FvP].

Consider the $p-$formal group scheme $\mathcal{G}^n := Ker(\Psi : A^n \to (\mathbf{G}_a^{(n-1)g})^{\hat{}})$; so $\mathcal{G}^n$ is covered by $p-$formal schemes $Spf\ \mathcal{O}(U_i^n)/(\Psi)^{cl}$ where the upper $cl$ stands for "closure of an ideal in the $p-$adic topology". Consider the $p-$formal scheme $\mathcal{G}_f^n$ obtained by gluing the $p-$formal schemes $Spf\ \mathcal{O}(U_i^n)/((\Psi)^{cl} : p^{\infty})$; clearly $\mathcal{G}_f^n$ is then flat over $R$. Since the $p-$adic completion of the tensor product of two flat $R-$algebras is still flat over $R$, it follows that there is an induced structure of $p-$formal group scheme on $\mathcal{G}_f^n$. Hence $\mathcal{G}_f^n\otimes k$ has an induced structure of $k-$group scheme of finite type. Set

$$H_n := ((\mathcal{G}_f^n\otimes k)\cap Ker(A_0^n \to A_0))_{red}$$

Then $H_n$ is a unipotent algebraic subgroup of $A_0^n$; let $H_n^{\circ}$ be its connected component. Furthermore set

$$H_n^{stab} := Im(H_m \to H_n),\quad m \gg 0$$

$$H_n^{\circ,stab} := Im(H_m^{\circ} \to H_n^{\circ}),\quad m \gg 0$$

Then of course, for any point $P \in A^{\sharp}(R)\cap Ker(A(R) \to A_0(k))$, $P : Spec\ R \to A$, the induced point $Spec\ k \to A_0^{\infty} \to A_0^n$ factors through a morphism $Spec\ k \to H_n^{stab}$.

Now it is a consequence of general facts of commutative algebras that the rings $\mathcal{O}(U_i^n)/((\Psi)^{cl} : p^{\infty})$ are catenary (they are quotients of regular rings; use [Mat] pp. 137 and 157). Also, since

$$R \to \mathcal{O}(U_i^n)/((\Psi)^{cl} : p^{\infty})$$

is flat, it has "going down" [Mat] p. 68. Due to catenarity and going down we have (by [Mat] p. 117):

$$dim\ (\mathcal{O}(U_i^n)/((\Psi)^{cl} : p^{\infty}))\otimes K \geq dim\ (\mathcal{O}(U_i^n)/((\Psi)^{cl} : p^{\infty}))\otimes k$$

Since the left hand side of the above inequality is $\leq 2g$ we get that $dim\ H_n \leq 2g$. (Actually one can immediately show that $dim\ H_n \leq g$; but the only important thing here is that $dim\ H_n$ is bounded by a constant which is independent of $n$.)

**Claim 1.** *$H_n^{\circ,stab} = 0$ for all $n$.*

Indeed assume that for some $n$ the group $H_n^{\circ,stab}(k)$ contains infinitely many elements $x_{n1}, x_{n2}, \dots$ Since the maps $H_{m+1}^{\circ,stab}(k) \to H_m^{\circ,stab}(k)$ are surjective for all $m$ we may lift $x_{n1}, x_{n2}, \dots$ to elements $x_1, x_2, \dots \in$ *inv lim* $H_m^{\circ,stab}(k) \subset A_0^\infty(k) \simeq A(R)$. Since $H_m^{\circ,stab}$ is unipotent connected of dimension $\leq 2g$ we must have $0 = p^{2g}x_1 = p^{2g}x_2 = \dots$ so we end up with infinitely many points of order $p^{2g}$ in $A(R)$, a contradiction. Our Claim 1 is proved.

**Claim 2.** *$A^\sharp(R)$ is a proalgebraic subgroup of $A(R)$.*

Recall that the proalgebraic structure is defined by the maps $\pi_n : A(R) \simeq A_0^\infty(k) \to A_0^n(k)$. Let $S \subset \mathcal{O}^\infty(A) = \mathcal{O}(A^\infty)$ denote the set of $\delta-$characters of $A(R)$. Then by Part I section 2, $A^\sharp(R)$ is the subset of $A(R) \simeq A_0^\infty(k)$ defined by the image in $\mathcal{O}_{A_0^\infty}$ of the ideal $(S, S', S'', \dots)^{cl} \subset \mathcal{O}_{A^\infty}$ where the upper $cl$ means "$p-$adic closure of an ideal". Clearly the ideal $(S, \phi S, \phi^2 S, \dots)^{cl}$ defines a $p-$formal subgroup scheme of $A^\infty$ hence, exactly as above, the same holds for $(S, \phi S, \phi^2 S, \dots)^{cl} : p^\infty$. But the latter ideal clearly equals $(S, S', S'', \dots)^{cl}$. So the image of this ideal in $\mathcal{O}_{A_0^\infty}$ will define a $k-$subgroup scheme of $A_0^\infty$, which proves Claim 2. Note the above argument holds for $S$ any set of $\delta-$characters.

**Claim 3.** *$p^\infty A(R)$ is a connected proalgebraic subgroup of $A(R)$.*

This is well known [Ray] p.10 and easy to check. Indeed one immediately checks that $\pi_n(p^\infty A(R)) = p^n A_0^n(k)$ =maximal abelian subvariety of $A_0^n(k)$ and and $p^\infty A(R)$ is the inverse limit of the $\pi_n(p^\infty A(R))$'s.

Now Claim 1 implies that $H_n^{stab}$ is finite for all $n$. Hence by Claim 2 $\pi_n(A^\sharp(R))$ is an algebraic subgroup of $A_0^n(k)$ mapping onto $A_0(k)$ with finite kernel. Hence $\pi_n(p^\infty A(R)) = \pi_n(A^\sharp(R))^\circ$. Taking inverse limits (and using Claims 2 and 3) we get $p^\infty A(R) = A^\sharp(R)^\circ$ and Theorem A is proved.

(3.2) Let us pass to the proof of Theorem B. We shall redo what we did in (2.5) and (3.1) in the special case $n = 2$, taking into account the special features of this case.

Denote by $B$ the $p-$formal group scheme $Ker(A^2 \to A^0)$. If $s : (\mathbf{G}_a^g)^\wedge \to B$ is any section of the second projection, then consider the section $\tilde{s} : (\mathbf{G}_a^g)^\wedge \to B$ defined as

$$\tilde{s}(x) = \tilde{s}(x_1, \dots, x_g) = s(x_1, \dots, 0) + \dots + s(0, \dots, x_g)$$

This latter section defines a symmetric cocycle $f : (\mathbf{G}_a^g)^\wedge \hat{\times} (\mathbf{G}_a^g)^\wedge \to (\mathbf{G}_a^g)^\wedge$ $f(x^1, x^2) = \tilde{s}(x^1 + x^2) - \tilde{s}(x^1) - \tilde{s}(x^2)$ which, of course, will have components of the form $f_\alpha(x^1, x^2) = f_{\alpha 1}(x_1^1, x_1^2) + \dots + f_{\alpha g}(x_g^1, x_g^2)$ where $f_{\alpha\beta} : (\mathbf{G}_a)^\wedge \hat{\times} (\mathbf{G}_a)^\wedge \to (\mathbf{G}_a)^\wedge$ are symmetric cocycles, hence are given by series $f_{\alpha\beta} \in R[x_\beta^1, x_\beta^2]^\wedge$. Reasoning as in (2.5) we may assume

$$f = \sum_n r_n C_{p^n}(x^1, x^2)$$

where the sum above is finite, $f$ is the $g \times 1$ matrix with entries $f_\alpha$, $r_n$ are $g \times g$ matrices with entries in $R$, and $C_{p^n}(x^1, x^2)$ is the $g \times 1$ matrix with entries $C_{p^n}(x^1_\beta, x^2_\beta)$.

As in (3.1) $A^2$ is obtained by gluing products $(U_i)\hat{\ }\hat{\times}B = Spf\ C_i[x,y]\hat{\ }$ where $U_i$ is a Zariski open covering of $A$, $C_i = \mathcal{O}(U_i)\hat{\ }$, $x, y$ are $g$-uples of indeterminates (sometimes viewed as $g \times 1$ matrices) giving "the coordinates" on $(\mathbf{G}^g_a)\hat{\ } = ker(A^1 \to A^0)$ and $(\mathbf{G}^g_a)\hat{\ } = ker(A^2 \to A^1)$ respectively, and the gluing isomorphisms $\sigma_{ij} : C_{ij}[x,y]\hat{\ } \to C_{ij}[x,y]\hat{\ }$, $(C_{ij} = \mathcal{O}(U_{ij})\hat{\ }$, $U_{ij} = U_i \cap U_j)$ are given by formulae

$$\sigma_{ij}(x) = x + a_{ij}$$

$$\sigma_{ij}(y) = y + b_{ij} + \sum_n r_n C_{p^n}(x, a_{ij})$$

where $a_{ij}, b_{ij}$ are $g \times 1$ matrices with entries in $C_{ij}$ such that $(a_{ij}, b_{ij})$ form a cocycle with respect to addition in $B$; in other words:

$$(a_{ij}, b_{ij}) = (a_{ik} + a_{kj}, b_{ik} + b_{kj} + \sum_n r_n C_{p^n}(a_{ik}, a_{kj}))$$

Now $C_{p^n}(a_{ik}, a_{kj}) = (a_{ij}^{p^n} - a_{ik}^{p^n} - a_{kj}^{p^n})/p$ so, upon letting

$$c_{ij} := \sum_n r_n a_{ij}^{p^n} - pb_{ij} \in C_{ij}$$

we see that $c_{ij}$ defines a $g$-uple of cocycles in $\mathcal{O}_{\hat{A}}$.

Let us prove assertion 2) in Theorem B. We claim that the $g$-uple of classes $[a_{ij}] \in H^1(\hat{A}, \mathcal{O}_{\hat{A}})^g$ generates a rank $g$ submodule of $H^1(\hat{A}, \mathcal{O}_{\hat{A}})$. Indeed if we had a relation of the form $h[a_{ij}] = 0$ where $h \neq 0$ is a $1 \times g$ matrix with entries in $R$ we would have $ha_{ij} = b_i - b_j$ for some $b_i \in C_i^g$. Then the expressions $hx - b_i$ would glue together to give a non zero $\delta$-character of order one, which proves our claim.

By the claim we may write $ma_{ij} + p^\nu c_{ij} = a_i - a_j$ where $m$ is a $g \times g$ matrix with entries in $R$. Set

$$\Psi_i = p^\nu(\sum_n r_n x^{p^n} - py) + mx - a_i \in (C_i[x,y]\hat{\ })^g$$

As in (3.1) $\sigma_{ij}(\Psi_i) = \Psi_j$ so the $\Psi_i$'s glue together to give a $g$-uple $\Psi \in \mathcal{O}(A^2)^g$ of homomorphisms.

By the Local product property, if $t$ are etale coordinates on $U_i$ then we must have compatible isomorphisms $C_i[x]\hat{\ } \simeq C_i[t']\hat{\ }$ and $C_i[x,y]\hat{\ } \simeq C_i[t', t'']\hat{\ }$. This immediately implies that for $n \geq 0$ we have

$$\mathcal{O}(U_i^{n+2}) \simeq C_i[t', t'', ..., t^{(n+2)}]\hat{\ } \simeq C_i[x, y, y', ..., y^{(n)}]\hat{\ }$$

In the rings above we may write

$$\Psi = -p^{\nu+1}y + g_0(x),\ \Psi' = -p^{\nu+1}y' + g_1(x,y),\ \Psi'' = -p^{\nu+1}y'' + g_2(x,y,y'), ...$$

Note that

$$det(\partial\Psi^{(r)}/\partial y^{(s)})_{0\leq r,s,\leq n} \in K^*$$

We get

$$dim\ (C_i[x,y,y',...,y^{(n)}]\hat{}/(\Psi,\Psi',...,\Psi^{(n)})\otimes_R K) \leq dim\ (C_i[x]\hat{}\otimes_R K) = 2g$$

and the proof of assertion 2) can be concluded exactly as in (3.1).

(3.3) Let's check assertion 1) in Theorem B. Assume there exist $g$ linearly independent homomorphisms $A^1 \to (\mathbf{G}_a)\hat{}$. They give rise to $g-$uples $\Psi_i \in (C_i[x]\hat{})^g$. Since $\Psi_i$ must be "affine" on the fibres of $A^1 \to A^0$ they must be of the form $\Psi_i = u_i x + v_i$ where $u_i, v_i$ are $g \times g$ (respectively $g \times 1$) matrices with entries in $C_i$. The gluing condition $u_j x + v_j = \sigma_{ij}(u_i x + v_i) = u_i x + u_i a_{ij} + v_i$ shows that the $u_i$'s glue together to give an matrix $u$ with entries in $R$, with $det\ u \neq 0$. We also get $u a_{ij} = v_i - v_j$ which imples that the $g-$uple of classes $[a_{ij}]$ is zero in $H^1(\hat{A}, \mathcal{O}_{\hat{A}})^g$. This means that the projection $A^1 \to A^0$ has a section. This section defines, by the universality property $(UP\hat{})$ a lifting of $\delta : R \to R$ to a $p-$derivation of the identity of $A^0 = \hat{A}$, and hence a $\phi-$lifting of the Frobenius, as desired in assertion 1). Conversely, if such a lifting exists, the reversed argument leads to $g$ linearly independent $\delta-$characters of order one. The assertion about profiniteness can be proved in a way similar to the argument for assertion 2).

(3.4) Let us prove Theorem D. We will only check its first assertion; the second one may be proved similarly. We use notations from (3.1). Assume we have a point $P \in A^\sharp(R[[t]]) \cap A(R[[t]])_{pt}$, $P : Spec\ R[[t]] \to A$, consider its lifting $\nabla P : Spf\ R[[t]] \to A^\infty$ and the point obtained by reduction modulo $p$, $(\nabla P)_0 : Spec\ k[[t]] \to A_0^\infty$. Since $P \in A^\sharp(R[[t]]) \cap Ker(A(R[[t]]) \to A_0(k[[t]]))$ the morphism $(\nabla P)_0$ factors through a morphism

$$Spec\ k[[t]] \to inv\ lim\ H_n^{stab}$$

Since by (3.1) $H_n^{stab}$ are finite over $k$ for all $n$ the morphism $(\nabla P)_0$ factors through a morphism $Q : Spec\ k \to A_0^\infty$. Then we may write $Q = (\nabla\tilde{Q})_0$ for a unique $\tilde{Q} : Spec\ R \to A$. Let

$$\tilde{P} : Spec\ R[[t]] \to Spec\ R \xrightarrow{\tilde{Q}} A$$

be the composition. Then $(\nabla(P - \tilde{P}))_0 = 0 \in A_0^\infty(k[[t]])$. By Lemma (3.5) below the map $A(R[[t]]) \to A_0^\infty(k[[t]])$, $S \mapsto (\nabla S)_0$ is injective. We get $P = \tilde{P}$, hence $P \in A(R)$. Since $P$ also belongs to $Ker(A(R[[t]]) \to A(R[[t]]/tR[[t]]) = A(R))$ it follows that $P = 0$ and we are done.

We are left to prove the following:

**Lemma (3.5).** *The map $R[[t]] \to k[[t]]^{\mathbf{N}}$, $f \mapsto (\pi_t f, \pi_t \delta f, \pi_t \delta^2 f, ...)$ is injective. (Here $\pi_t : R[[t]] \to k[[t]]$ is the reduction modulo $p$ map.)*

*Proof.* Let $f_1, f_2 \in R[[t]]$ be distinct. Write $f_1 = f_2 + p^n f$ with $\pi_t f \neq 0$. We get

$$\delta^n f_1 \equiv \delta^n f_2 + f^{p^n} \quad mod \quad (p)$$

so $\pi_t \delta^n f_1 \neq \pi_t \delta^n f_2$ and we are done.

## 4. Serre-Tate parameters and $\delta$–characters.

The aim of this section is to prove Theorem C in the Introduction.

(4.1) We start by defining a certain cohomology class which already appeared in the literature in various incarnations. We do it for abelian schemes but everything makes sense for any smooth projective scheme. So let $A/R$ be an abelian scheme with closed fibre $A_0/k$. Define its *internal* Kodaira-Spencer class $\rho^{int}(A/R) \in H^1(A_0, F^* T_{A_0/k})$ as follows. Cover $A$ with affine open subsets $U_i$, lift $\pi \circ \delta : R \to k$ (where $\pi : R \to k$ is the canonical surjection) to a $p$–derivation $\delta_i : \mathcal{O}(U_i) \to \mathcal{O}(U_{i0})$ of the canonical surjection, and consider the differences $\delta_j - \delta_i$; they define a class $[\delta_j - \delta_i] \in H^1(A_0, F^* T_{A_0/k})$ which we call $\rho^{int}(A/R)$. (Actually it is enough to do this construction modulo $p^2$.) We shall sometimes make the identification

$$H^1(A_0, F^* T_{A_0/k}) \simeq Hom_k(H^0(A_0, F^* \Omega^1_{A_0/k}), H^1(A_0, \mathcal{O}_{A_0}))$$

and view $\rho^{int}(A/R)$ as map $H^0(A_0, F^* \Omega^1_{A_0/k}) \to H^1(A_0, \mathcal{O}_{A_0})$

**Lemma (4.2).** *The class of the extension*

$$0 \to \mathbf{G}^g_{a,k} \to A^1_0 \to A_0 \to 0$$

*in the group*

$$Ext^1(A_0, \mathbf{G}^g_{a,k}) \simeq Hom_k(H^0(A_0, F^* \Omega^1_{A_0/k}), H^1(A_0, \mathcal{O}_{A_0})) \simeq H^1(A_0, F^* T_{A_0/k})$$

*equals $\rho^{int}(A/R)$.*

*Proof.* Let $v_1, ..., v_g$ be a basis of $H^0(A_0, T_{A_0/k})$ coming from an $R$–basis $V_1, ..., V_g$ of $H^0(A, T_{A/R})$. We view $v_i$ as derivations of $\mathcal{O}_{A_0}$. Then composing these with the absolute Frobenius $F$ of $A_0$ we get a basis $Fv_1, ..., Fv_g$ of $H^0(A_0, F^* T_{A_0/k})$. Using notations above, we may write $\delta_j - \delta_i = \sum_n \alpha_{ijn} F v_n$ where $\alpha_{ijn} \in \mathcal{O}(U_{i0})$. Then of course $\rho^{int}(A/R)$ is represented by the map $(Fv_n)^\circ \mapsto [\alpha_{ijn}] \in H^1(A_0, \mathcal{O}_{A_0})$, where $\{(Fv_n)^\circ\} \subset H^0(A_0, F^* \Omega^1_{A_0/k})$ is the dual basis of $\{Fv_n\}$. Now glue the schemes $Spec\ \mathcal{O}(U_{i0})[x]$, where $x$ is a $g$–uple of indeterminates, by $x_n \mapsto x_n + \alpha_{ijn}$. The resulting scheme is the extension $E$ of $A_0^1$ by $\mathbf{G}_{a,k}^g$ corresponding to $\rho^{int}(A/R)$. Consider now the $p-$derivations $\theta_i : \mathcal{O}(U_i) \to \mathcal{O}(U_{i0})[x]$ defined by $\theta_i a := \delta_i a + \sum_n F(V_n a \ mod \ p)x_n$. There $p-$derivations glue together to give a $p-$derivation $\theta : \mathcal{O}_A \to \mathcal{O}_E$. It is easy to check that $E$ together with this $p-$derivation satisfies the universality property of $A_0^1$ (just interpret correctly the Local product property).

(4.3) Assume from now on that $A_0/k$ is ordinary. Let $\mathcal{A}/\mathcal{M}$ be the universal formal deformation of $A_0/k$. By Serre-Tate $\mathcal{M}$ has a structure of toroidal formal group so we may write $\mathcal{M} = Spf \ R[[t]]$ where $t = (t_{ij})$ are indeterminates: the expressions $q_{ij} = 1 + t_{ij}$ are the "universal" Serre-Tate parameters. Then $A/R$ defines a classifying map $R[[t]] \to R$. The images of $t_{ij}$ respectively $q_{ij}$ in $R$ will be denoted by $t_{ij}(A)$, $q_{ij}(A)$; cf. [Ka].

One may define two Kodaira-Spencer maps (which we may call *external* Kodaira-Spencer maps)

$$\rho^{ext} : k^{g^2} \to H^1(A_0, T_{A_0/k})$$

and

$$\rho^{ext,Frob} : k^{g^2} \to H^1(A_0, F^*T_{A_0/k})$$

as follows. For any matrix $r = (r_{ij}) \in k^{g^2}$ let $\partial_r : k[[t]] \to k[[t]]$ be the $k-$derivation of the identity of $k[[t]]$ defined by the formula $\partial_r := \sum_{ij} r_{ij}(\partial/\partial t_{ij})$. Consider an affine open covering $\mathcal{A}_i$ of $\mathcal{A}$ and lift $\partial_r$ to derivations of the identity $\partial_{r,i} : \mathcal{O}(\mathcal{A}_{i,0}) \to \mathcal{O}(\mathcal{A}_{i,0})$. Recall that the index 0 stands for "taking the closed fibre" (equivalently "tensorizing with $k$"). Then consider the differences $\partial_{r,j} - \partial_{r,i}$ and reduce them modulo $t$ to get a class $\rho^{ext}(r) \in H^1(A_0, T_{A_0/k})$. Similarly to define $\rho^{ext,Frob}$ start with any matrix $r$ as above, consider the $k-$derivation of Frobenius $\sum_{ij} r_{ij} F \circ (\partial/\partial t_{ij})$, lift it to derivations of the Frobenius $\mathcal{O}(\mathcal{A}_{i,0}) \to \mathcal{O}(\mathcal{A}_{i,0})$ and consider the class in $H^1(A_0, F^*T_{A_0/k})$ represented by the differences of these liftings. We have then a commutative diagram

$$\begin{tikzcd}
k^{g^2} \arrow[r, "\rho^{ext}"] \arrow[d, "F"'] & H^1(A_0, T_{A_0/k}) \arrow[d, "F^*"] \\
k^{g^2} \arrow[r, "\rho^{ext,Frob}"] & H^1(A_0, F^*T_{A_0/k})
\end{tikzcd}$$

It is also useful to note that $\rho^{ext}(r)$ viewed as a map $H^0(A_0, \Omega^1_{A_0/k}) \to H^1(A_0, \mathcal{O}_{A_0})$ can be represented (in suitable basis) as the matrix $r$ itself. Indeed, by "Katz' formula" [Ka], there exists a basis $\omega_1, ..., \omega_g, \eta_1, ..., \eta_g$ of $H := H^1_{DR}(\mathcal{A}/\mathcal{M})$ compatible with the Hodge filtration such that the Gauss-Manin connection

$$\nabla : H \to \sum R[[t]]dt_{ij} \otimes H$$

satisfies $\nabla \eta_i = 0$ and

$$\nabla \omega_i = \sum_{j=1}^{g} \frac{dt_{ij}}{1 + t_{ij}} \otimes \eta_j$$

So $\rho^{ext}(r)$ corresponds to the matrix with entries

$$< \sum_{u,v} r_{uv}(\partial/\partial t_{uv}), \frac{dt_{ij}}{1+t_{ij}}|_{t=0} >= r_{ij}$$

**Lemma (4.4).** $\rho^{int}(A/R) = F^*\rho^{ext}((\pi(\delta t(A)))^{1/p})$

**Remark.** The above is an analogue of "Katz' formula" [Ka] which says something similar for "usual" derivations (rather than $p-$derivations).

*Proof.* Recall that $\pi : R \to k$ is the canonical projection. Let us give names to some of the maps which we are going to consider. Call $\pi_t : R[[t]] \to k[[t]]$ the "reduction modulo $p$" map, call $f_0 : R[[t]] \to k$ the $R-$algebra map which sends $t \mapsto 0$ and call $f_{00} : k[[t]] \to k$ be the $k-$algebra map sending $t \mapsto 0$. Also call $f_A : R[[t]] \to R$ the classifying map of $A/R$; i.e. $f_A(t) = (t_{ij}(A))$. Of course we have $\pi \circ f_A = f_0$.

By [Ka] pp.170-171 there is a commutative diagram of schemes

$$\begin{tikzcd}
\mathcal{A} \arrow[r, "\phi"] \arrow[d] & \mathcal{A} \arrow[d] \\
\mathcal{M} \arrow[r, "\phi"] \arrow[d] & \mathcal{M} \arrow[d] \\
Spf\ R \arrow[r, "\phi"] & Spf\ R
\end{tikzcd}$$

where $\mathcal{M} \xrightarrow{\phi} \mathcal{M}$ has the property that $\phi^* t_{ij} = t_{ij}^p$. So we get $p-$derivations of the identity on $R[[t]]$ and on the structure sheaf $\mathcal{O}_{\mathcal{A}}$, both to be denoted in what follows by $\delta$. Of course $\delta t_{ij} = 0$. Consider the map

$$\bar{\partial} : R[[t]] \to k, \ \bar{\partial} = \pi \circ \delta \circ f_A - f_0 \circ \delta$$

Since both $\pi \circ \delta \circ f_A$ and $f_0 \circ \delta$ are $p-$derivations of $f_0$ it follows that $\bar{\partial}$ is an $R-$derivation of $F \circ f_0 : R[[t]] \to k \to k$. So $\bar{\partial}$ has necessarly the form

$$\bar{\partial}(h) = \sum_{ij} r_{ij} \left( \pi \left( \frac{\partial h}{\partial t_{ij}}(0) \right) \right)^p, \quad h \in R[[t]]$$

where $r_{ij} \in k$. Consider the map $\partial : R[[t]] \to k[[t]]$ defined by

$$\partial(h) = \sum_{ij} r_{ij} \left( \pi_t \left( \frac{\partial h}{\partial t_{ij}} \right) \right)^p, \quad h \in R[[t]]$$

It is an $R-$derivation of $F \circ \pi_t : R[[t]] \to k[[t]] \to k[[t]]$. Of course we have $\bar{\partial} = f_{00} \circ \partial$. Note that

$$r_{ij} = \partial t_{ij} = \bar{\partial} t_{ij} = \pi \circ \delta \circ f_A(t_{ij}) - f_0 \circ \delta t_{ij} = \pi(\delta t_{ij}(A))$$

Now let $\mathcal{A}_i$ be an affine covering of $\mathcal{A}$ and lift $\partial$ to $R-$derivations $\partial_i : \mathcal{O}_{\mathcal{A}_i} \to \mathcal{O}_{\mathcal{A}_{i,0}}$ of $F \circ \pi_i : \mathcal{O}_{\mathcal{A}_i} \to \mathcal{O}_{\mathcal{A}_{i,0}}$, where $\pi_i : \mathcal{O}_{\mathcal{A}_i} \to \mathcal{O}_{\mathcal{A}_{i,0}}$ are the reduction modulo $p$ homomorphisms. Finally consider the maps

$$D_i := \pi_i \circ \delta + \partial_i : \mathcal{O}_{\mathcal{A}_i} \to \mathcal{O}_{\mathcal{A}_{i,0}}$$

They are $p-$derivations of $\pi_i$ whose restriction to $R$ is of course $\pi \circ \delta : R \to R \to k$. Let us examine the differences

$$D_j - D_i = \partial_j - \partial_i : \mathcal{O}_{\mathcal{A}_{ij}} \to \mathcal{O}_{\mathcal{A}_{ij,0}}$$

$(\mathcal{A}_{ij} := \mathcal{A}_i \cap \mathcal{A}_j)$. These differences vanish on $p$ so they induce a cocycle

$$\partial_i - \partial_j : \mathcal{O}_{\mathcal{A}_{ij,0}} \to \mathcal{O}_{\mathcal{A}_{ij,0}}$$

which represents

$$\rho^{ext,Frob}(r) = \rho^{ext,Frob}(\pi(\delta t(A))) = F^*\rho^{ext}((\pi(\delta t(A)))^{1/p})$$

Now we claim that each $D_i$ maps $Ker(f_A)$ into $Ker(f_{00}) = tk[[t]]$. Indeed the restriction of $D_i$ to $R[[t]]$ equals $\pi_t \circ \delta + \partial$ and we have

$$f_{00} \circ (\pi_t \circ \delta + \partial) = f_0 \circ \delta + \bar{\partial} = \pi \circ \delta \circ f_A$$

This shows that each $D_i$ induces a $p-$derivation $\delta_i : \mathcal{O}_{\hat{A}_i} \to \mathcal{O}_{\hat{A}_{i,0}}$ of the canonical surjection $\mathcal{O}_{\hat{A}_i} \to \mathcal{O}_{A_{i,0}}$ (where $\hat{A}_i \subset \hat{A}$ is the pull back of $\mathcal{A}_i$ via $f_A$). The induced cocyle

$$\delta_j - \delta_i : \mathcal{O}_{A_{ij,0}} \to \mathcal{O}_{A_{ij,0}}$$

represents $\rho^{int}(A/R)$ and the Lemma is proved.

(4.5) Let us conclude the proof of Theorem C. Only assertion 2) of it requires a proof. So assume we are in the hypothesis of Theorem C and use freely the notations from section 3 and from the discussion in the present section. As remarked in the Introduction, our hypothesis $det((q_{ij}(A) - 1)/p) \in R^*$ is equivalent to the fact that $det(\pi(\delta t_{ij}(A))) \neq 0$. By (4.3) the class $\rho^{ext}((\pi(\delta t(A)))^{1/p})$, viewed as a map $H^0(A_0, \Omega^1_{A_0/k}) \to H^1(A_0, \mathcal{O}_{A_0})$, is represented (in suitable bases) by the matrix $((\pi(\delta t_{ij}(A)))^{1/p})$ itself; so by our hypothesis, this map is invertible. By Lemma (4.4) the class $\rho^{int}(A/R)$, viewed as a map $H^0(A_0, F^*\Omega^1_{A_0/k}) \to H^1(A_0, \mathcal{O}_{A_0})$, must be invertible. By Lemma (4.2) the class of the extension

$$0 \to \mathbb{G}^g_{a,k} \to A^1_0 \to A_0 \to 0$$

corresponds to an invertible map $H^0(A_0, F^*\Omega^1_{A_0/k}) \to H^1(A_0, \mathcal{O}_{A_0})$. This shows that the $g-$uple of classes $[a_{ij}] \in H^1(A, \mathcal{O}_A)^g$ appearing in (3.2) generate $H^1(A_0, \mathcal{O}_{A_0})$. By Nakayama this $g-$uple must generate $H^1(A, \mathcal{O}_A)^g$ itself. Assume there is a $\delta-$character of order one on $A(R)$ and look for a contradiction. This $\delta$-character produces non zero elements $\Psi_i \in C_i[x]^{\hat{}}$ of the form $\Psi_i = u_i x + v_i$ where $u_i$ are $1 \times g$ matrices with entries in $C_i$ and $v_i \in C_i$. The gluing condition for $\Psi_i$ forces $u_i$ to glue together to give an $u \in R^g$. If $u = (0, ..., 0)$ then the $v_i$'s glue together to give a $v \in R$, which of course must be 0, a contradiction. If $u \neq (0, ..., 0)$ then, since the gluing condition for the $\Psi_i$'s also gives $ua_{ij} = v_j - v_i$, we get $u[a_{ij}] = 0$, contradicting the linear independence of the $g$-uple $[a_{ij}]$. Theorem B is proved.

## References

[B1] A.Buium, Geometry of differential polynomial functions I: algebraic groups, Amer. J. Math. 115, 6 (1993), 1385-1444.

[B2] A.Buium, Geometry of differential polynomial functions II: algebraic curves, Amer. J. Math. 116, 4 (1994), 785-818.

[B3] A.Buium, Intersections in jet spaces and a conjecture of S.Lang, Annals of Math. 136 (1992) 557-567.

[B4] A.Buium, Differential Algebraic Groups of Finite Dimension, Lecture Notes in Math. 1506, Springer 1992.

[B5] A.Buium, Geometry of $p$-jets I, Preprint Max Planck Inst. Math. Bonn, 1994.

[BV] A.Buium, F.Voloch, Reduction of the Manin map modulo $p$, to appear in Crelle J.

[Ca1] P.Cassidy, Differential algebraic groups, Amer.J.Math.94(1972), 891-954.

[Ca2] P.Cassidy, The classification of the semisimple differential algebraic groups and the linear differential algebraic Lie algebras, J.Algebra.

[Ch] Ching-Li Chai, A note on Manin's Theorem of the Kernel, Amer. J. Math., 113 (1991), 387-389.

[Co] R.Coleman, Torsion points on curves and $p$-adic abelian integrals, Ann.Math. 121 (1985), 111-168.

[FV] I.B.Fesenko, S.V.Vostokov, Local Fields and their Extensions: a Constructive Approach, Translations of Math. Monographs, vol 121, Amer. Math. Soc. 1993.

[FvP] J.Fresnel, M. van der Put, Geometrie Analytique Rigide et Applications, Progress in Math, Birkhauser, 1981.

[Haz] M.Hazewinkel, Formal Groups and Applications, Academic Press, New York, 1978.

[Hr] E.Hrushovski, The Lang-Mordell conjecture over function fields, preprint.

[Ka] N.Katz, Serre-Tate local moduli, Springer LNM 868 (1981), 138-202

[K1] E.Kolchin, Differential Algebra and Algebraic Groups, Academic Press, New York 1973.

[K2] E,Kolchin, Differential Algebraic Groups, Academic Press, New York 1985.

[Laz] M.Lazard, Sur les groupes de Lie formels a un parametre, Bull. Soc. Math. France, 83 (1955), 251-274.

[Mat] H.Matsumura, Commutative ring theory, Cambridge Univ. Press, 1986.

[Man] Yu.I.Manin, Algebraic curves over fields with differentiation, Izv. Akad. Nauk SSSR, Ser. Mat. 22 (1958), 737-756 = AMS translations Series 2, 37 (1964), 59-78.

[Me] W.Messing, The Crystalls Associated to Barsotti-Tate Groups, LNM 264, Springer 1972.

[Ray] M.Raynaud, Around the Mordell conjecture for function fields and a conjecture of S.Lang, LNM 1016 (1983), 1-20.

[R] J.F.Ritt, Differential Algebra, Amer.Math.Soc.1950.

[S1] J.P.Serre, Groupes Algebriques et Corps de Classes, Hermann, Paris 1959.

[S2] J.P.Serre, Groupes proalgebriques, Publ. Math. IHES 7 (1962).

Max Planck Institut für Mathematik, Bonn.