Inventiones math. 5, 317–334 (1968)

Deformations and Liftings of Finite, Commutative Group Schemes*

Frans Oort (Amsterdam) and David Mumford (Cambridge, Mass.)

1. Introduction

Consider the following problems:

(A) Given a field k, a finite k-group scheme N_0, and a ring R with a surjective ringhomomorphism $R \to k$. Does there exist a finite, flat R-group scheme N such that $N_0 \cong N \otimes_R k$? (If so, we say that N_0 is obtained from N by reduction mod $\mathfrak{m}$, where $\mathfrak{m} = \operatorname{Ker}(R \to k)$, or, we say that N is a lifting of N_0 to R.)

(B) Given a field k (of characteristic $p > 0$), and a finite k-group scheme N_0. Does there exist a ring R (integral domain of characteristic zero) with a reduction $R \to k$, and a finite, flat R-group scheme N such that $N_0 \cong N \otimes_R k$?

The answers to (A) and to the weaker question (B) are negative in general. However if in (B) moreover is given that N_0 is a *commutative* finite group scheme, the answer is affirmative; it is the aim of this paper to give a proof of this fact via deformation theory of finite group schemes in characteristic $p > 0$. As a byproduct we obtain a proof for the fact that any finite, local group scheme can be embedded into a formal Lie group with coefficients in the same field, on the same number of parameters.

Example (−A). Let k be a field of characteristic $p > 0$ (e.g. the prime field $k = \mathbf{F}_p$), and let R be a ring with a reduction $R \to k = R/\mathfrak{m}$, such that $p \cdot 1 \notin \mathfrak{m}^2$ (an "unramified" situation) (e.g. $R = W_\infty(k)$, so $W_\infty(\mathbf{F}_p) = \mathbf{Z}_p$, the ring of p-adic integers, or $R = W_\infty(k)/p^2$). Let $N_0 = \alpha_{p,k}$, i.e. $N_0 = \operatorname{Spec}(k[\tau])$, $\tau^p = 0$, and the group law is defined by $s_0 \colon E_0 \to E_0 \otimes_k E_0$, $E_0 = k[\tau]$, with $s_0(\tau) = \tau \otimes 1 + 1 \otimes \tau$; we claim that in this case the answer to problem (A) is negative. Suppose R to be local (localize if necessary), and suppose N as indicated could be found; then $N = \operatorname{Spec}(E)$, $E = R[\sigma]$, where $\sigma^p = a_1 \sigma + \cdots + a_{p-1} \sigma^{p-1}$ with $a_i \in \mathfrak{m}$; the group law would be given by some ringhomomorphism $s \colon E \to E \otimes_R E$, so

$$s(\sigma) = \sigma \otimes 1 + 1 \otimes \sigma + \sum b_{ij} \sigma^i \otimes \sigma^j, \qquad b_{ij} \in \mathfrak{m};$$

* This work was partially supported by NSF grant GP 3512.

as $(s\sigma)^p = s(\sigma^p)$, we obtain:

$$p \cdot (\sigma \otimes \sigma^{p-1} + \cdots + \sigma^{p-1} \otimes \sigma) \equiv 0 \qquad (\mathrm{mod}\, \mathfrak{m}^2 \cdot E \otimes E),$$

which is a contradiction.

Remark. In the previous situation, by a result of Tate (cf. [13]), we know that α_p can be lifted to R (e.g. R is a complete local ring) if and only if $p \in R$ admits a factorization $p = ab$, with $a \in \mathfrak{m}$, and $b \in \mathfrak{m}$.

Example (−B). Let R be an integral domain of characteristic zero, and let $N = \mathrm{Spec}(E)$ be a finite R-group scheme such that E is a free R-module of rank p^2 (where p is a prime number). Then N is commutative. This can be seen as follows: let L be an algebraic closure of the field of fractions of R; we know that $N \otimes_R L$ is reduced (cf. [1], footnote on p. 109; cf. [9], lecture 25, theorem 1; cf. [11]), so by group theory it follows that $N \otimes L$, and hence that N is commutative. This shows that any non-commutative group scheme of rank p^2 cannot be lifted to characteristic zero. It is easy to give an example: take the kernel of the Frobenius homomorphism of a suitable non-commutative linear group. For example, let N_0 be given by: k is a field of characteristic p, and for any k-algebra B,

$$N_0(B) = \left\{ \text{the multiplicative group of matrices } \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}, \quad \alpha \in B,\ \beta \in B,\ \alpha^p = 1,\ \beta^p = 0 \right\};$$

so $N_0 = \mathrm{Spec}(E_0)$, $E_0 = k[\tau, \rho]$ with $\tau^p = 1$, $\rho^p = 0$, with $s_0(\tau) = \tau \otimes \tau$ and $s_0(\rho) = \rho \otimes 1 + \tau \otimes \rho$.

2. Liftings of Deformations

The first example makes it clear that in order to lift a finite (local, unipotent) group scheme to characteristic zero, in general one has to allow ramification at p; but it is difficult to obtain directly from N_0 the information "how much ramification" is needed. Therefore we solve the problem B in the commutative case via deformation theory in characteristic $p > 0$. The following lemma is a special case of a general principle: that specializations of liftable "objects" are liftable.

Lemma (2.1). *Assume we are given rings: $A \subset K \xleftarrow{\pi} R$, where R is a characteristic zero local domain, $\pi: R \to R/\mathfrak{m} = K$ its residue class map, and A a subring of K, and that we are given finite free group schemes over these rings*

$$\begin{array}{ccccc} N_0 & \longleftarrow & M_0 & \longrightarrow & M \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Spec}(A) & \longleftarrow & \mathrm{Spec}(K) & \longrightarrow & \mathrm{Spec}(R), \end{array}$$

where $M_0 \cong N_0 \otimes_A K \cong M \otimes_R K$. *Write* $R' = \{x \in R \mid \pi(x) \in A\}$*; there is a finite free group scheme* $N \to \operatorname{Spec}(R')$ *such that* $N_0 \cong N \otimes_{R'} A$ *and* $M \cong N \otimes_{R'} R$.

Proof. Let $N_0 = \operatorname{Spec}(E_0)$, $M_0 = \operatorname{Spec}(F_0)$, $M = \operatorname{Spec}(F)$. Then $F_0 \cong E_0 \otimes_A K \cong F \otimes_R K$. Identify E_0 with the corresponding subset of F_0, and identify F_0 with the corresponding quotient of F, so $E_0 \subset F_0 \xleftarrow{\pi'} F$. Each of these three is a free module of rank d, say, over either A, K or R, and has the structure of a bialgebra. Let $E = \{x \in F \mid \pi'(x) \in E_0\}$, and choose a basis $\{b_1, \ldots, b_d\}$ of E_0 over k; let $a_i \in F$ satisfy $\pi'(a_i) = b_i$; one checks easily that E is a free R'-module with basis $\{a_1, \ldots, a_d\}$. Moreover, one can also check

i) that the identity 1 of F is in E,

ii) E is closed under multiplication in the ring F,

iii) the comultiplication $F \to F \otimes_R F$ carries E in $E \otimes_{R'} E$,

iv) the augmentation $F \to R$ carries E in R',

v) the inverse $F \to F$ carries E to E.

Therefore $N = \operatorname{Spec}(E)$ is a finite free group scheme over R' with all the required properties.

Actually, what we need:

Corollary (2.2). *Let* $A = k$ *be a field, and let* N_0 *be a finite k-group scheme; this group scheme can be lifted to characteristic zero if and only if for some field extension* $k \subset K$ *(or for every field extension* $k \subset K$*),* $N_0 \otimes_k K$ *can be lifted to characteristic zero.*

The "if" part follows from (2.1). The "only if" part for example is an easy consequence of the place extension theorem (cf. EGA 0_{III}, 10.3.1).

Corollary (2.3). *Let* $k \leftarrow A \hookrightarrow K$ *be ringhomomorphisms, and let* $N_0 = \operatorname{Spec}(E_0)$ *be a finite free A-group scheme such that* $N_0 \otimes_A K$ *can be lifted to characteristic zero. Then* $N_0 \otimes_A k$ *can be lifted to characteristic zero.*

If $N_0 \cong N \otimes_{R'} A$, then $N \otimes_A k \cong N \otimes_{R'} A \otimes_A k \cong N \otimes_{R'} k$.

3. Moduli of Rigidified Local Group Schemes

It is clear that in general the moduli functor for finite group schemes is not representable.

Example. Let $\operatorname{char}(k) = p > 0$, take $B = k[T]$, and define a B-bialgebra by $E = B[\tau]$ with $\tau^p = T\tau$ and $s(\tau) = \tau \otimes 1 + 1 \otimes \tau$; for any field $K \supset k$ and for any $t \in \operatorname{Spec}(B)(K)$ with $t \neq 0$ (i.e. for any k-algebra homomorphism φ: $B \to K$ such that $\varphi(T) \neq 0$) E_t is the bialgebra of a reduced group scheme, isomorphic to $\mathbf{Z}/p$ in case K is algebraically closed, while E_0 is the bialgebra of the group scheme α_p.

However by an obvious rigidification of the underlying scheme of the group schemes we can obtain a moduli space. In order to see that any finite group scheme admits a nice deformation we would like to know that this moduli space is irreducible. It is easy to see it is connected, and by imposing extra conditions we can actually obtain a variety.

First we recall the following fact, due to Dieudonné and Cartier. Let N be a finite local k-group scheme, where k is a *perfect* field; $N=\operatorname{Spec}(E)$. Then there exist integers $v_1, \ldots, v_m$ and an isomorphism

$$E \cong k[X_1, \ldots, X_m]/(X_1^{p\exp(v_1)}, \ldots, X_m^{p\exp(v_m)})$$

(cf. SGAD, Exp. VII_B, 5.4; we are writing $p\exp(a)=p^a$ for typographical reasons); in this case we say that E admits a *truncation type* $v=(v_1, \ldots, v_m)$.

By the way, the following example shows that in general a finite local group scheme over an imperfect field does not admit a truncation type: let $a \in k$, $a \notin k^p$, $E=k[X,Y]/(X^{p^2}, X^p - aY)$, and $s(X)=X\otimes 1+1\otimes X$, $s(Y)=Y\otimes 1+1\otimes Y$.

Notation. Let $\alpha=(\alpha_1, \ldots, \alpha_m)$ be a set of non-negative integers; we write X^α for

$$X^\alpha = X_1^{\alpha_1} \times \cdots \times X_m^{\alpha_m}$$

(with $X_i^0=1$), and we denote by $|\alpha|=\alpha_1+\cdots+\alpha_m$.

Definition. Let p be a prime number, $v=(v_1, \ldots, v_m)$ a set of positive integers, and $\mu=X^\alpha$ a monomial in m variables, where $\alpha=(\alpha_1, \ldots, \alpha_m)$. We say that μ satisfies the condition $(P\,v)_i$ for $1\leqq i\leqq m$, if there exists an index j such that

$$\alpha_j \cdot p^{v_i} \geqq p^{v_j}$$

or, equivalently $(X^\alpha)^{p\exp(v_i)}$ is in the ideal generated by $X_1^{p\exp(v_1)}, \ldots, X_m^{p\exp(v_m)}$. We say that a polynomial in $X_1, \ldots, X_m$ satisfies $(P\,v)_i$ if is can be written as a sum of monomials which all satisfy condition $(P\,v)_i$. We say that a polynomial in the variables $X_j\otimes X_k$, $1\leqq j\leqq m$, $1\leqq k\leqq m$, satisfies condition $(P\,v)_i$ if it can be written as a sum

$$\sum_t \mu_{1t}\otimes\mu_{2t}$$

where μ_{1t} and μ_{2t} are monomials such that for each index t either μ_{1t} or μ_{2t} satisfies $(P\,v)_i$. Analogous definition for a polynomial in the variables $X_j\otimes X_k\otimes X_l$.

Remark. Let B be an *integral* domain of characteristic p, and let $N=\operatorname{Spec}(E)$ be a finite B-group scheme, $E=B[\tau_1, \ldots, \tau_m]$ with $\tau_i^{p\exp(v_i)}=0$,

$1 \leqq i \leqq m$; the comultiplication is denoted by $s\colon E \to E \otimes E$. As s is a ringhomomorphism it follows that $(s\,\tau_i)^{p\exp(v_i)} = 0$, so $s(\tau_i)$ is a polynomial in $\tau_j \otimes \tau_k$ which satisfies condition $(P\,v)_i$. The same for the polynomials $\gamma(\tau_i)$, where $\gamma\colon E \to E$ defines the inverse.

We fix k, a field of characteristic $p>0$, and $v=(v_1, \ldots, v_m)$, a set of positive integers; $\mathbf{C} = \mathbf{C}_k$ denotes the category of k-algebras. Define a functor $\Sigma_v = \Sigma\colon \mathbf{C} \to \mathbf{Ens}$ by:

$\Sigma(B) = \{$all cocommutative B-bialgebra structures on $B[\tau_1, \ldots, \tau_m] = E$, such that $s(\tau_i)$ are polynomials satisfying condition $(P\,v)_i$ for $1 \leqq i \leqq m\}$,

where $\tau_i^{p\exp(v_i)} = 0$ for $1 \leqq i \leqq m$, and where the augmentation ideal of E is generated by $\tau_1, \ldots, \tau_m$. Note that a B-bialgebra F can correspond to various elements of $\Sigma(B)$, as there may exist several isomorphisms $F \cong B[\tau_1, \ldots, \tau_m]$.

Theorem (3.1). *We fix k, and $v=(v_1, \ldots, v_m)$ as before; the functor $\Sigma\colon \mathbf{C} \to \mathbf{Ens}$ is represented by a k-algebra U, and there exists an integer n such that $U \cong k[T_1, \ldots, T_n]$.*

It is easy to see that Σ is representable; however the first step of the proof will be more complicated as we want to obtain information for late use.

Proof, first step: Σ is representable. Consider all combinations $(i,\ \alpha=(\alpha_1, \ldots, \alpha_m),\ \beta=(\beta_1, \ldots, \beta_m))$ such that $1 \leqq i \leqq m$, $0 \leqq \alpha_j < p\exp(v_j)$, $0 \leqq \beta_j < p\exp(v_j)$, and such that the monomial $\tau^\alpha \otimes \tau^\beta$ satisfies condition $(P\,v)_i$ (i.e. either $(\tau^\alpha)^{p\exp(v_i)} = 0$, or $(\tau^\beta)^{p\exp(v_i)} = 0$), and such that $|\alpha| > 0$ and $|\beta| > 0$; let $A = k[\ldots, Y_{i,\alpha,\beta}, \ldots]$, and let $F = A[\tau_1, \ldots, \tau_m]$ with $\tau_i^{p\exp(v_i)} = 0$, $1 \leqq i \leqq m$. Then we are given an A-algebra homomorphism

$$s\colon F \to F \otimes_A F$$

by

$$s(\tau_i) = \tau_i \otimes 1 + 1 \otimes \tau_i + \sum_{\alpha, \beta} Y_{i,\alpha,\beta}\, \tau^\alpha \otimes \tau^\beta$$

(s is a ringhomomorphism because of the conditions $(P\,v)_i$, but this is not the point where these conditions are used essentially). Let $\mu_1, \mu_2, \ldots$ be all non-zero monomials of the form $\tau^\alpha \otimes \tau^\beta \otimes \tau^\gamma$; we write $\Gamma s = (s \otimes 1) \cdot s - (1 \otimes s) \cdot s$, and

$$(\Gamma s)(\tau_i) = \sum_j H_{ij}\, \mu_j, \qquad 1 \leqq i \leqq m,$$

with $H_{ij} \in A$; let $\mathfrak{p} \subset A$ be the ideal generated by these polynomials, and by the symmetry relations:

$$\mathfrak{p} = (\ldots, H_{ij}, \ldots, \ldots, Y_{i,\alpha,\beta} - Y_{i,\beta,\alpha}, \ldots) \cdot A.$$

We define $U=A/\mathfrak{p}$, and $E=U[\tau_1, \dots, \tau_m]$. It is clear that s induces a coassociative comultiplication

$$s\colon E \to E \otimes_U E,$$

defined by

$$s(\tau_i)=\tau_i \otimes 1 + 1 \otimes \tau_i + \sum_{\alpha,\beta} y_{i,\alpha,\beta}\, \tau^\alpha \otimes \tau^\beta,$$

where $y_{i,\alpha,\beta}=Y_{i,\alpha,\beta} \bmod \mathfrak{p}$. Clearly the pair (U,E) represents the functor $\Omega_{m,v}=\Omega$ defined by:

$\Omega(B)=\{$all cocommutative coassociative B-algebra homomorphisms $s\colon E \to E \otimes_B E$, where $E=B[\tau_1, \dots, \tau_m]$, such that $s(x) \equiv x \otimes 1 + 1 \otimes x \pmod{\mathfrak{a} \otimes \mathfrak{a}}$, $\mathfrak{a}=(\tau_1, \dots, \tau_m)\cdot E$, and such that $s(\tau_i)$ satisfies condition $(P\,v)_i$ for $1 \leqq i \leqq m\}$.

The following lemma asserts that $\Sigma(B) \twoheadrightarrow \Omega(B)$:

Lemma (3.2). *Let B be a ring in which $p \cdot 1=0$, let $E=B[\tau_1, \dots, \tau_m]$ with $\tau_i^{p^{\exp(v_i)}}=0$, $1 \leqq i \leqq m$, and with augmentation ideal $\mathfrak{a}=(\tau_1, \dots, \tau_m)\cdot E$. Let $s\colon E \to E \otimes_B E$ be a B-algebra homomorphism such that*

$$s(x) \equiv x \otimes 1 + 1 \otimes x \qquad (\operatorname{mod} \mathfrak{a} \otimes \mathfrak{a})$$

for all $x \in \mathfrak{a}$ (i.e. the augmentation is a left- and a right-coidentity), and such that $s(\tau_i)$ satisfies condition $(P\,v)_i$ for $1 \leqq i \leqq m$. Then there exists a unique B-algebra homomorphism $\gamma\colon E \to E$ such that $m(\gamma \otimes 1)\, s(x)=0$ for all $x \in \mathfrak{a}$ (where $m\colon E \otimes_B E \to E$ is the multiplication).

Proof. We define $\gamma_1(\tau_i)=-\tau_i$; thus we have defined a B-algebra homomorphism $\gamma_1\colon E \to E$ having the property

$$m(\gamma_1 \otimes 1)\, s(x) \in \mathfrak{a}^2 \qquad \text{for all } x \in \mathfrak{a},$$

and it is unique modulo $\mathfrak{a}^2$ among all having this property. Suppose for some $N \geqq 1$ there is given a B-algebra homomorphism $\gamma_N\colon E \to E$ such that

$$m(\gamma_N \otimes 1)\, s(x)=\rho_N(x) \in \mathfrak{a}^{N+1} \qquad \text{for all } x \in \mathfrak{a},$$

and such that $\gamma_N(\tau_i)$ satisfies condition $(P\,v)_i$ for $1 \leqq i \leqq m$. It is easy to see that $\rho_N(\tau_i)$ satisfies condition $(P\,v)_i$; thus

$$\gamma_{N+1}(\tau_i)=\gamma_N(\tau_i)-\rho_N(\tau_i), \qquad 1 \leqq i \leqq m,$$

defines a B-algebra homomorphism $\gamma_{N+1}\colon E \to E$; it is clear that

$$m(\gamma_{N+1} \otimes 1)\, s(\tau_i) \in \mathfrak{a}^{N+2} \qquad \text{for } 1 \leqq i \leqq m,$$

and it is readily verified that if γ' also has the property $m(\gamma' \otimes 1)\, s(x) \in \mathfrak{a}^{N+2}$ for all $x \in \mathfrak{a}$, and $\gamma'(\tau_i)-\gamma_{N+1}(\tau_i) \in \mathfrak{a}^{N+1}$ for all i, then $\gamma'(x) \equiv \gamma_{N+1}(x)$ (mod

$\mathfrak{a}^{N+2}$) for all $x \in \mathfrak{a}$. Thus the construction of γ and its uniqueness follow by induction as $\mathfrak{a}^{|\gamma|}=0$.

Thus the ring U and the bialgebra structure on E represent the functor $\Sigma \cong \Omega$, and the first step of the proof is concluded. Let $W=\operatorname{Spec}(U)$; consider the point $0 \in W(k)$ defined by $y_{i,\alpha,\beta} \mapsto 0$, i.e. $s(\tau_i)=\tau_i \otimes 1 + 1 \otimes \tau_i$ and $\gamma(\tau_i)=-\tau_i$; that is the point corresponding to the rigidified group scheme $\alpha_{p\exp(v_1)} \times \cdots \times \alpha_{p\exp(v_m)}$.

The crucial part of the proof of the theorem is: $0 \in W(k)$ is a *non-singular* point of W (note that this is false if W were the moduli space of all rigidified group schemes, say of a fixed rank, not necessarily local; note that this is also false if W were the moduli space of all rigidified local group schemes, not all the v_i equal, and not imposing the extra conditions $(P\,v)_i$). This we can show in two ways. It can be deduced from results of Lazard about formal group laws; this will be done in the next section. We could also have used the group-cohomology as described in SGAD, Exp. III, especially p. III. 42/43, Theorem 3.5 (also cf. [8]), and using a result of G. Efroymson, which says that $H^3_{\text{symm}}(N, \mathbf{G}_a)=0$ (trivial action of the commutative finite group scheme N on the additive linear group $\mathbf{G}_a$) (proved in his Harvard thesis, 1966, later generalized into a structure theorem about the cohomology ring $H^{\cdot}(N, \mathbf{G}_a)$, not yet published).

4. Finite Group Schemes and Buds

First we recall some definitions and results to be found in a paper by Lazard, cf. [5]. Let m and r be positive integers, R a ring (commutative, and $1 \in R$), and

$$f\colon\ R[X_1, \ldots, X_m]=E \to E \otimes_R E$$

an R-algebra homomorphism; we say that f defines an r-bud ("r-bourgeon") on m parameters, with coefficients in R if (we write $(f\otimes 1)\cdot f - (1\otimes f)\cdot f = \Gamma f$):

$$(\Gamma f)(X_i) \equiv 0 \qquad (\text{mod degree } r+1) \text{ for } 1 \leqq i \leqq m$$

(degree means total degree in the variables $X_1 \otimes 1, \ldots, 1 \otimes X_m$); f and g define the same r-bud if and only if $f(X_i) \equiv g(X_i)$ (mod degree $r+1$) for $1 \leqq i \leqq m$ (cf. [5], p. 381, Definition 13.1); a system $f_1, f_2, \ldots$ such that f_r is an r-bud on m parameters, and such that f_r and f_{r+1} define the same r-bud is called a formal Lie group on m parameters. We write

$$\Lambda_{m,r}(R)=\Lambda(R)=\{\text{all cocommutative } r\text{-buds ("}r\text{-bourgeons abéliens") on } m \text{ parameters with coefficients in } R\};$$

clearly we have thus obtained a covariant functor $\Lambda_{m,r}$ defined on the category of commutative rings with identity; if $f \in \Lambda_{m,r}(E)$ and $\varphi\colon E \to R$

is a ring homomorphism we write $(\Lambda\varphi)(f) \in \Lambda_{m,r}(R)$ for the r-bud over R obtained from f, applying φ. Lazard has proved:

(i) (cf. [5], pp. 394–399, and previous pages). Let

$$N(m,r) = N = m\left(\binom{r+m}{m} - m - 1\right);$$

there exists a universal

$$F_r \in \Lambda_{m,r}(A_r), \qquad A_r = \mathbf{Z}[T_1, \ldots, T_{N(m,r)}],$$

i.e. (A_r, F_r) represents the functor $\Lambda_{m,r}$, or: the map

$$\mathrm{RHom}(A_r, \mathrm{R}) \twoheadrightarrow \Lambda_{m,r}(R)$$

defined by $\varphi \mapsto (\Lambda\varphi)(F_r)$ is bijective for every R.

(ii) The natural restriction map $\Lambda_{m,r+1}(R) \to \Lambda_{m,r}(R)$ is surjective if R is without integral torsion (cf. [5], p. 396, Lemma 15.2), hence, by (i), this map is surjective for every R; it corresponds to the inclusion map

$$A_r = \mathbf{Z}[T_1, \ldots, T_{N(m,r)}] \hookrightarrow A_{r+1} = \mathbf{Z}[T_1, \ldots, T_{N(m,r+1)}],$$

such that $F_r \in \Lambda_r(A_r) \subset \Lambda_r(A_{r+1})$ and $F_{r+1} \in \Lambda_{r+1}(A_{r+1})$ define the same r-bud.

(iii) Suppose f_r and f_{r+1} define the same r-bud on m parameters with coefficients in R; $(\Lambda\varphi_r)(F_r) = f_r$ and $(\Lambda\varphi_{r+1})(F_{r+1}) = f_{r+1}$; then the diagram

$$\begin{array}{ccc} A_r & \hookrightarrow & A_{r+1} \\ & {}_{\varphi_r}\searrow & \downarrow{\scriptstyle \varphi_{r+1}} \\ & & R \end{array}$$

commutes. Hence

$$A = \bigcup A_r = \mathbf{Z}[T_1, T_2, \ldots]$$

represents the functor of all formal Lie groups on m parameters (cf. [5], p. 397, Theorem 15.1); in particular, any r-bud on m parameters can be extended to a formal Lie group on m parameters with coefficients in the same ring.

Suppose we fix k, a field of characteristic $p > 0$, a positive integer m, and positive integers $v_1, \ldots, v_m$. We choose an integer r so that

$$r \geqq 3 \cdot \sum_{i=1}^{m} (p \exp(v_i) - 1).$$

We consider only rings R containing k, in particular $p \cdot 1 = 0$ in R. We restrict the functor Λ to the category of k-algebras; for such rings we define a functor Δ by:

$$\Delta_{m,r,v} = \Delta \subset \Lambda_{m,r}$$

$\Delta(R) = \{f \in \Lambda_{m,r}(R)$ such that $f(X_i)$ satisfies condition $(Pv)_i$ for $1 \leqq i \leqq m\}$.

For $f \in \Delta(R)$, we define $\rho(f)$ by

$$\rho(f)(\tau_i) = f(X_i) \bmod (X_1^{p\exp(v_1)}, \ldots, X_m^{p\exp(v_m)});$$

because of the conditions $(Pv)_i$ we thus obtain an R-algebra homomorphism (!)

$$\rho(f)\colon E \to E \otimes_R E, \quad E = R[\tau_1, \ldots, \tau_m],$$

where $\tau_i^{p\exp(v_i)} = 0$, $1 \leqq i \leqq m$, and because of the choice of r it follows that

$$(\Gamma s)(\tau_i) = 0, \qquad 1 \leqq i \leqq m,$$

so $\rho(f) \in \Omega(R)$ (in the notation introduced in Section 3). So we have the following morphisms of functors (defined on k-algebras):

$$\Sigma \cong \Omega_{m,v} = \Omega \leftarrow \Delta_{m,r,v} \subset \Lambda_{m,r}.$$

Proposition (4.1). *We fix k, m, $v_1, \ldots, v_m$, and $r \geqq 3 \cdot \sum (p\exp(v_i) - 1)$ as before. The functors*

$$\Lambda, \Delta, \Omega\colon \mathbf{C} \to \mathbf{Ens}$$

are representable, say by L, D, and W. The schemes D and W (and also L) are isomorphic to affine spaces over k. In suitable coordinates the morphism $\rho\colon D \to W$ is given by a projection

$$D \cong \operatorname{Spec}(k[T_1, \ldots, T_n, T_1', \ldots, T_m']) \to \operatorname{Spec}(k[T_1, \ldots, T_n]) \cong W;$$

in particular, for every $R \supset k$ the map $\rho\colon D(R) \to W(R)$ is surjective.

In order to deduce these facts from Lazard's results, we need the following tools:

Lemma (4.2). *Let*

$$f(X_i) = \sum_{\alpha,\beta} a_{i,\alpha,\beta} X^\alpha \otimes X^\beta$$

be polynomials with coefficients in a ring R with $p \cdot 1 = 0$, such that $f(X_i)$ satisfies condition $(Pv)_i$, $1 \leqq i \leqq m$; then $(f \otimes 1) f(X_i)$, and also $(1 \otimes f)$ $f(X_i)$, can be written as a sum of monomials satisfying condition $(Pv)_i$.

Proof.

$$(f \otimes 1) f(X_i) = \sum_{\alpha,\beta} a_{i,\alpha,\beta} \{\prod_j [\sum a_{j,\gamma,\delta} X^\gamma \otimes X^\delta]^{\alpha_j}\} \otimes X^\beta = \sum_{\alpha,\beta} a_{i,\alpha,\beta} Q_{i,\alpha,\beta}.$$

It suffices to consider each $Q_{i,\alpha,\beta}$ separately; either X^β satisfies condition $(Pv)_i$, and we are done, or there exists an index e such that $\alpha_e \cdot p\exp(v_i) \geqq p\exp(v_e)$, so $p\exp(n + v_i) \geqq p\exp(v_e)$ with $\alpha_e \geqq p^n$, and $n \geqq 0$; in that case

$$\begin{aligned} Q_{i,\alpha,\beta} &= \{[\sum a_{e,\gamma,\delta} X^\gamma \otimes X^\delta]^{p^n} \times (\cdots)\} \otimes X^\beta \\ &= \{\{\sum [a_{e,\gamma,\delta} X^\gamma \otimes X^\delta]^{p^n}\} \times (\cdots)\} \otimes X^\beta; \end{aligned}$$

for each (e, γ, δ) there exists an index d such that $\gamma_d \cdot p\exp(v_e) \geqq p\exp(v_d)$, or $\delta_d \cdot p\exp(v_e) \geqq p\exp(v_d)$, hence

$$p^n \cdot \gamma_d \cdot p\exp(v_i) \geqq \gamma_d \cdot p\exp(v_e) \geqq p\exp(v_d),$$

or the same with δ_d, and $(Q_{i,\alpha,\beta})^{p\exp(v_i)}$ is divisable by $(X_d \otimes 1 \otimes 1)^{p\exp(v_d)}$, respectively divisable by $(1 \otimes X_\alpha \otimes 1)^{p\exp(\gamma_d)}$, and the lemma is proved.

Lemma (4.3). *Let R be a ring, M an ideal in R, and $b \in R$ so that $M \cdot b = 0$. Let $E = R[X_1, \ldots, X_m]$, and $g\colon E \to E \otimes E$ so that*

$$g(X_i) \equiv X_i \otimes 1 + 1 \otimes X_i \qquad (\operatorname{mod} M \cdot E \otimes E).$$

Let $P = b X^\alpha \otimes X^\beta$ be a monomial such that X^α and X^β do not satisfy condition $(P\,v)_i$ (for some fixed index i); then $(g \otimes 1)(P)$, and also $(1 \otimes g)(P)$, can be written as a sum of monomials none of which satisfy condition $(P\,v)_i$.

Proof.

$$(g \otimes 1)(P) = b \cdot g(X^\alpha) \otimes X^\beta = b \cdot \{\prod_j (X_j \otimes 1 + 1 \otimes X_j)^{\alpha_j}\} \otimes X^\beta$$

as $M \cdot b = 0$, and the lemma is proved.

Let k be a field, W a k-algebraic scheme, and $w \in W(k)$. The following statements are known to be equivalent:

(i) w is a non-singular point on W;

(ii) the local ring $\mathcal{O}$ of w on W is a regular local ring, i.e. its completion $\hat{\mathcal{O}}$ is a formal power series ring $\hat{\mathcal{O}} \cong k[[e_1, \ldots, e_n]]$;

(iii) (Grothendieck's criterion, cf. SGA, III.3.1 and II.5.10) for every local artinian k-algebra R, maximal ideal M, and any ideal $I \subset R$ so that $M \cdot I = 0$, the map $W(R)_w \to W(R/I)_w$ is surjective (we write $W(R)_w$ for the set of morphisms $W \to \operatorname{Spec}(R)$ with $(W \to \operatorname{Spec}(R) \to \operatorname{Spec}(k)) = w$).

Lemma (4.4). *Let $\rho\colon D \to W$ be a morphism of k-algebraic schemes, and $d \in D(k)$ a non-singular point on D; suppose the tangential map*

$$\rho_*\colon t_{D,d} \to t_{W,\rho(d)}$$

to be surjective. Then $\rho(d) = w \in W(k)$ is a non-singular point on W.

Proof. Let $e_1, \ldots, e_n \in \mathcal{O}_{W,w}$ be choosen in such a way that their residues modulo $\mathfrak{m}^2$ form a k-base for $\mathfrak{m}/\mathfrak{m}^2$, where $\mathfrak{m}$ is the maximal ideal of $\mathcal{O}_{W,w}$. We obtain:

$$k[[e_1, \ldots, e_n]] \xrightarrow{\pi} \hat{\mathcal{O}}_{W,w} \xrightarrow{\varphi} \hat{\mathcal{O}}_{D,d};$$

as the tangential map ρ_* is surjective, the images of the e_i's are linearly independent modulo the square of the maximal ideal of $\mathcal{O}_{D,d}$; as d is a non-singular point this implies that the composition $\varphi \cdot \pi$ is injective; thus π is injective (and it is also surjective), so $\hat{\mathcal{O}}_{W,w}$ is a formal power series ring, hence $w \in W(k)$ is a non-singular point, and the lemma is proved.

Elimination Lemma (4.5). *Let* $A = k[T_1, \dots, T_N]$, *and* $H_1, \dots, H_d \in A$. *Suppose given positive integers* $w(T_1), \dots, w(T_N)$ *such that* $H_1, \dots, H_d$ *are homogeneous polynomials in the weighed variables* $T_1, \dots, T_n$ *(i.e. we write* $w(\prod T_{n_i}) = \sum w(T_{n_i})$; *if* μ_1 *and* μ_2 *are monomials occuring with non-zero coefficients in some* H_j, *then* $w(\mu_1) = w(\mu_2)$). *Suppose* $H_1(0) = 0 = H_2(0) = \dots = H_d(0)$, *such that* 0 *is a non-singular point of* $V = \operatorname{Spec}(A/(H_1, \dots, H_d)A)$. *Then we can renumber the variables, and we can choose* $0 \leqq n \leqq N$ *so that*

$$A/(H_1, \dots, H_d)A \cong k[T_1, \dots, T_n].$$

Proof. Suppose $(H_1, \dots, H_d)A \neq 0$ (otherwise the conclusion is obvious); in that case at least one of these polynomials has a linear term: if not, we would have

$$(H_1, \dots, H_d)A \subset (T_1^2, \dots, T_i T_j, \dots, T_N^2)A = \mathfrak{b},$$

so

$$\operatorname{Spec}(A/\mathfrak{b}) \subset V \subsetneqq \mathbf{A}_k^N = \operatorname{Spec}(k[T_1, \dots, T_N]),$$

a contradiction with the fact that $0 \in V(k)$ is non-singular. So let

$$H_d = c\,T_N + G, \qquad c \in k, \ c \neq 0$$

so that T_N does not appear in the linear term of G (renumber the variables and the polynomials if necessary); as $w(T_i)$ are positive integers for all i, it follows that $G \in k[T_1, \dots, T_{N-1}]$. We write

$$G_i = H_i\left(T_1, \dots, T_{N-1}, -\frac{1}{c} G(T_1, \dots, T_{N-1})\right), \qquad 1 \leqq i < d,$$

and clearly

$$A/(H_1, \dots, H_d) \cong k[T_1, \dots, T_{N-1}]/(G_1, \dots, G_{d-1})$$

(the variable T_N is eliminated); moreover it is clear that the polynomials $G_1, \dots, G_{d-1}$ are homogeneous in the weighed variables $T_1, \dots, T_{N-1}$; thus the lemma is proved by induction on d.

Proof of Proposition (4.1). We proved that Ω is represented by W in Section 3, by the results of Lazard we know Λ is representable, and it is easy to see that Δ is representable (cf. below). The point $0 \in D(k)$ is defined by $f \in \Delta(k)$, $f(X_i) = X_i \otimes 1 + 1 \otimes X_i$; first we show that this is a non-singular point on D. Let R be a local artinian k-algebra, with maximal ideal M, and let $I \subset R$ be an ideal such that $M \cdot I = 0$; we write

$R'=R/I$. By Grothendieck's criterion it suffices to show that

$$D(R)_0 \to D(R')_0$$

is a surjective map. Thus given $f' \in \Delta(R')_0 = D(R')_0$, we would like to construct $f \in \Delta(R)_0$ so that $f' \equiv f(\mathrm{mod}(I \cdot E \otimes E))$ (where $E = k[X_1, \ldots, X_m]$); by the result of Lazard we know that Λ is represented by a non-singular scheme (in fact affine space of dimension $N(m,r)$), so for $f' \in \Delta(R')_0 \subset \Lambda(R')_0$ there exists a $g \in \Lambda(R)_0$ so that

$$f' \equiv g \qquad (\mathrm{mod}\, I \cdot E \otimes E).$$

We know that

$$g(X_i) \equiv X_i \otimes 1 + 1 \otimes X_i \qquad (\mathrm{mod}\, M \cdot E \otimes E),$$

as we work in the point $0 \in D(k) \subset L(k)$; we write

$$g(X_i) = f(X_i) + c(X_i),$$

where $c(X_i)$ consists of monomials none of which satisfy condition $(P\nu)_i$, and $f(X_i)$ consists of monomials which satisfy condition $(P\nu)_i$. We claim that

$$(\Gamma f) \equiv 0 \qquad (\mathrm{mod\ degree}\ r+1),$$

i.e. $f \in \Delta(R)_0$; in fact let

$$f(X_i) = X_i \otimes 1 + 1 \otimes X_i + \sum_{\alpha,\beta} a_{i,\alpha,\beta} X^\alpha \otimes X^\beta,$$

$$c(X_i) = \sum_{\alpha,\beta} b_{i,\alpha,\beta} X^\alpha \otimes X^\beta;$$

then $a_{i,\alpha,\beta} \in M$ and $b_{i,\alpha,\beta} \in I$. Using $M \cdot I = 0$, we obtain:

$$(g \otimes 1)\, g(X_i) = [(f \otimes 1)\, f(X_i)]$$
$$+ \Big[\sum_{\alpha,\beta} b_{i,\alpha,\beta} X^\alpha \otimes X^\beta \otimes 1 + (g \otimes 1)\Big(\sum_{\alpha,\beta} b_{i,\alpha,\beta} X^\alpha \otimes X^\beta\Big)\Big].$$

By (4.2) the first term in square brackets can be written as a sum of monomials all satisfying condition $(P\nu)_i$; by (4.3) the second term can be written as a sum of monomials none of which satisfy condition $(P\nu)_i$. Thus the equation $(\Gamma g)(X_i) \equiv 0$ (mod degree $r+1$) proves, by sorting out all $(P\nu)_i$-monomials, that

$$(\Gamma f)(X_i) \equiv 0 \qquad (\mathrm{mod\ degree}\ r+1),$$

thus $f \in \Delta(R)_0$, and we have proved that $0 \in D(k)$ is a nonsingular point on D.

Next we show that $0 \in W$ is a non-singular point on W. Let $R = k[\varepsilon]$, with $\varepsilon^2 = 0$. We know that $t_{D,0} = \Delta(k[\varepsilon])_0$, hence by (4.4) it suffices to show that

$$\rho_*: \Delta(k[\varepsilon])_0 \to \Omega(k[\varepsilon])_0$$

is a surjective map. Hence we are given

$$s: E \to E \otimes E, \quad E = R[\tau_1, \dots, \tau_m],$$

with

$$s(\tau_i) = \tau_i \otimes 1 + 1 \otimes \tau_i + \varepsilon \cdot \sum c_{i,\alpha,\beta}\, \tau^\alpha \otimes \tau^\beta, \qquad c_{i,\alpha,\beta} \in k,$$

satisfying $(P\,v)_i$ and $(\Gamma\, s) = 0$, and we have to construct an r-bud f satisfying again the conditions $(P\,v)_i$ extending s. We choose

$$f(X_i) = X_i \otimes 1 + 1 \otimes X_i + \varepsilon \cdot \sum c_{i,\alpha,\beta}\, X^\alpha \otimes X^\beta;$$

as $\varepsilon^2 = 0$, we obtain

$$\begin{aligned}(f \otimes 1)\, f(X_i) = {} & X_i \otimes 1 \otimes 1 + 1 \otimes X_i \otimes 1 + 1 \otimes 1 \otimes X_i \\ & + \varepsilon \cdot \sum c_{i,\alpha,\beta}\, X^\alpha \otimes X^\beta \otimes 1 \\ & + \varepsilon \cdot \sum c_{i,\alpha,\beta} \{\prod_j (X_j \otimes 1 + 1 \otimes X_j)^{\alpha_j}\} \otimes X^\beta;\end{aligned}$$

in each of these terms the exponent of X_j is smaller than $p \exp(v_j)$, thus $\Gamma s = 0$ proves that $(\Gamma f)(X_i) = 0$. Thus $f \in \Delta(R)_0$, and certainly $\rho(f) = s$, and we have shown the tangential map ρ_* to be surjective; as $0 \in D$ is a non-singular point we conclude by (4.4) that $0 \in W$ is non-singular.

Now we prove that D and W are isomorphic to affine spaces over k. Let Δ' be the set of pairs (α, β) with $\alpha = (\alpha_1, \dots, \alpha_m)$, $\beta = (\beta_1, \dots, \beta_m)$ so that $1 \leqq |\alpha|$ and $1 \leqq |\beta|$ and $|\alpha| + |\beta| \leqq r$; let Δ'' be the set of triples (α, β, γ) with $1 \leqq |\alpha|$, $1 \leqq |\beta|$, $1 \leqq |\gamma|$, and $|\alpha| + |\beta| + |\gamma| \leqq r$. Let Ω' be the set of pairs (α, β) with $1 \leqq |\alpha|$ and $0 \leqq \alpha_j < p \exp(v_j)$ for $1 \leqq j \leqq m$, and $1 \leqq |\beta|$ and $0 \leqq \beta_k < p \exp(v_k)$ for $1 \leqq k \leqq m$; let Ω'' be the set of triples (α, β, γ) with $1 \leqq |\alpha|$ and $0 \leqq \alpha_j < p \exp(v_j)$, etc. Consider

$$F(X_i) = X_i \otimes 1 + 1 \otimes X_i + \sum_{\alpha,\beta} T_{i,\alpha,\beta}\, X^\alpha \otimes X^\beta,$$

summation taken over all $(\alpha, \beta) \in \Delta'$, respectively summation taken over all $(\alpha, \beta) \in \Omega'$; we write $k[\Delta']$, resp. $k[\Omega']$, for the polynomial ring $k[\dots, T_{i,\alpha,\beta}, \dots]$, $1 \leqq i \leqq m$ and $(\alpha, \beta) \in \Delta'$, resp. $1 \leqq i \leqq m$ and $(\alpha, \beta) \in \Omega'$. We define polynomials $H_{i,\alpha,\beta,\gamma} \in k[\Delta']$, resp. $H_{i,\alpha,\beta,\gamma} \in k[\Omega']$ by

$$(\Gamma F)(X_i) = \sum_{\alpha,\beta,\gamma} H_{i,\alpha,\beta,\gamma}\, X^\alpha \otimes X^\beta \otimes X^\gamma.$$

Clearly the scheme D, resp. W, is defined by the equations

$T_{i,\alpha,\beta} = T_{i,\beta,\alpha}$,	all $1 \leqq i \leqq m$ and $(\alpha, \beta) \in \Delta'$, resp. $(\alpha, \beta) \in \Omega'$;
$T_{i,\alpha,\beta} = 0$	if $X^\alpha \otimes X^\beta$ does not satisfy $(P\,v)_i$;
$H_{i,\alpha,\beta,\gamma} = 0$,	all $1 \leqq i \leqq m$, and $(\alpha, \beta, \gamma) \in \Delta''$, resp. $(\alpha, \beta, \gamma) \in \Omega''$.

Consider $(F\otimes 1)F(X_i)$; part of this has the form

$$\sum T_{i,\alpha,\beta}\{\prod_j (X_j\otimes 1+1\otimes X_j+\sum T_{j,\gamma,\delta}X^\gamma\otimes X^\delta)^{\alpha_j}\}\otimes X^\beta;$$

each term of this sum is of the form

$$T_{i,\alpha,\beta}\cdot \prod_{1\leqq t\leqq|\alpha|}(T_{?,\lambda_t,\mu_t}X^{\lambda_t}\otimes X^{\mu_t})\otimes X^\beta$$

(where the question mark indicates some integer, $1\leqq ?\leqq m$, and where $T_{?,1,0}=1=T_{?,0,1}$); the monomial in the T's obtained thus has weight

$$|\alpha|+|\beta|-1+\sum_t(|\lambda_t|+|\mu_t|-1)=a,$$

while the corresponding term in the X's has total degree

$$\sum_t|\lambda_t|+\sum_t|\mu_t|+|\beta|=a+1;$$

so each term in the polynomial $H_{i,\alpha,\beta,\gamma}$ has weight $|\alpha|+|\beta|+|\gamma|-1$.

Thus both D and W are defined by homogeneous equations in the weighed variables $T_{i,\alpha,\beta}$ and as $0\in D(k)$, resp. $0\in W(k)$ are non-singular points we deduce from the elimination lemma that both D and W are isomorphic to affine space over k. This finishes the proof of the first statement of (4.1). Hence Theorem (3.1) is proved, as we have seen (3.2) that $\Sigma\cong\Omega$.

Let $\mathfrak{a}\subset k[\Delta']$, respectively $\mathfrak{b}\subset k[\Omega']$ be the ideal defining D, resp. W. Renaming the variables we obtain: $k[\Omega']=k[T_1,\dots,T_N]$ and $k[\Delta']=k[T_1,\dots,T_N,T_{N+1},\dots,T_{N+M}]$. We have proved already that there exists a number n, with $0\leqq n\leqq N$, so that

$$\begin{array}{ccc} k[T_1,\dots,T_n] & \hookrightarrow & k[T_1,\dots,T_N] \\ & \searrow^{\sim} & \downarrow \\ & & k[T_1,\dots,T_N]/\mathfrak{b}. \end{array}$$

The morphism $\rho\colon D\to W$ comes from the ringhomomorphism φ:

$$\begin{array}{ccc} k[T_1,\dots,T_N] & \hookrightarrow & k[T_1,\dots,T_{N+M}] \\ \downarrow & & \downarrow \\ k[T_1,\dots,T_n]\cong U=k[T_1,\dots,T_N]/\mathfrak{b} & \xrightarrow{\varphi} & k[T_1,\dots,T_{N+M}]/\mathfrak{a}=B, \end{array}$$

$$\mathrm{Spec}(U)=W\xleftarrow{\rho}D=\mathrm{Spec}(B),\qquad \rho={}^a\varphi;$$

we are done if we can prove that if we apply the elimination lemma to $\mathfrak{a}\subset k[\mathrm{T}_1,\dots,T_{N+M}]$, none of the variables $T_1,\dots,T_n$ is eliminated: in that case

$$k[T_1,\dots,T_n]\cong U\to B\cong k[T_1,\dots,T_n,T_{N+1},\dots,T_{N+m}]$$

for some m with $0 \leqq m \leqq M$ (renumber the variables if necessary); of course in that case every R-point of W comes from an R-point of D. So we have to show: if $T_{i,\alpha,\beta}$ with $(\alpha,\beta)\in\Omega'$ appears in the linear term of some $H_{j,\gamma,\delta,\varepsilon}$, with $(\gamma,\delta,\varepsilon)\in\Delta''$, then $(\gamma,\delta,\varepsilon)\in\Omega''$; but this is clear: computing $(\Gamma F)(X_i)$ we obtain:

$$\begin{aligned}\sum T_{i,\alpha,\beta} X^\alpha \otimes X^\beta \otimes 1 - \sum T_{i,\alpha,\beta} 1 \otimes X^\alpha \otimes X^\beta \\ + \sum T_{i,\alpha,\beta} \{\prod_j (X_j \otimes 1 + 1 \otimes X_j + \sum T_{j,\gamma,\delta} X^\gamma \otimes X^\delta)^{\alpha_j}\} \otimes X^\beta \\ - \sum T_{i,\alpha,\beta} X^\alpha \otimes \{\prod_j (X_j \otimes 1 + 1 \otimes X_j + \sum T_{j,\gamma,\delta} X^\gamma \otimes X^\delta)^{\beta_j}\};\end{aligned}$$

so "$T_{i,\alpha,\beta}$ appears in the linear term of $H_{j,\gamma,\delta,\varepsilon}$" and $(\alpha,\beta)\in\Omega'$ imply that $(\gamma,\delta,\varepsilon)\in\Omega''$. Thus we have shown that the variables $T_{n+1},\dots,T_N$ can be expressed in the variables $T_1,\dots,T_n$, that $T_{N+1},\dots,T_{N+M}$ depend on $T_1,\dots,T_n$, $T_{N+1},\dots,T_{N+m}$, and that the variables $T_1,\dots,T_n$ cannot be eliminated. Thus the proof of the proposition is concluded.

Remark. The multiplicative semi-group scheme $\mathbf{A}_1^\times = \operatorname{Spec}(k[T])$ acts on $k[\Delta']$ and on $k[\Omega']$ (use the weights of the variables). Under this action D and W are stable, as their defining equations are homogeneous in weight. In this way we originally proved W to be connected; as $D-\{0\}/\mathbf{G}_m$ and $W-\{0\}/\mathbf{G}_m$ are projective schemes, it easily follows that $\rho\colon D(k)\to W(k)$ is surjective in case k is an algebraically closed field.

Remark. One could ask for the dimension of W. It is easy to compute directly the equations for the tangent space at $W(k)$. However we do not see a formula expressing $\dim W$ in terms of m and $(\nu_1,\dots,\nu_m)$.

Remark. Let V be the k-algebraic scheme such that for every $B\supset k$, $V(B)=\{$all commutative B-bialgebra structures on $B[\tau_1,\dots,\tau_m]=E\}$; then $V_{\text{red}}=W$, and $V=W$ if and only if $\nu_1=\dots=\nu_m$.

5. Conclusions

Corollary (5.1). *Let k be a field of characteristic $p>0$, and let N be a finite commutative k-group scheme; N can be lifted to characteristic zero (in the sense of problem* (B) *of Section 1).*

Proof. By (2.2) it suffices to show the result for some $K\supset k$; so we can suppose k to be an algebraically closed field. Then $N=N_{\text{loc}}\times N_{\text{sep}}$ (cf. CGS, 2.14). As a reduced finite group scheme over an algebraically closed field corresponds uniquely to a finite group (cf. CGS, 2.16), it is clear that any separable group scheme can be lifted to characteristic zero (we know $N_{\text{sep}}=\operatorname{Spec}(k\times\dots\times k)$, take any characteristic zero domain R with a reduction $R\to k$, choose $M=\operatorname{Spec}(R\times\dots\times R)$, etc.). As k is supposed to be algebraically closed, hence perfect, N_{loc} admits a truncation type $\nu=(\nu_1,\dots,\nu_m)$, hence by (3.1) there exists a point

$w \in W(k)$, where W is an irreducible, smooth k-algebraic scheme, and a finite, free group scheme $M \to W$, such that $N_{loc} \cong M_w$ (i.e. the fibre of M at the point w is isomorphic, as a group scheme, with N_{loc}). Next we note there exists a point $u \in W(k)$ such that

$$\mu_{p\exp(v_1)} \times \cdots \times \mu_{p\exp(v_m)} \cong M_u;$$

thus the fibre of the morphism $M^D \to W$ over the point $u \in W(k)$ is reduced (by D we denote the dualizing functor associating with each finite flat commutative group scheme its linear, or: Cartier, dual; e.g. compare CGS, p. 3). Let L be an algebraic closure of the field of fractions of U, where $W = \mathrm{Spec}(U)$. It follows that the group scheme M_L^D is reduced, so M_L^D can be lifted to characteristic zero by what is said before, so M_L can be lifted to characteristic zero as D commutes with base extension, so by (2.3) it follows that $M \otimes_U k \cong M_w \cong N_{loc}$ can be lifted to characteristic zero, and the corollary is proved.

Question. Let R_0 be a local, artinian ring, and let N_0 be a finite flat, commutative R_0-group scheme. Can we lift N_0 to characteristic zero? In case the rank of N_0 is prime we can, cf. [13]. However it seems that the methods developed above do not work if R_0 is not a field.

Corollary (5.2). *Let R be a ring in which $p \cdot 1 = 0$, and let $N = \mathrm{Spec}(E)$ be a commutative R-group scheme such that E admits a truncation type $E \cong R[\tau_1, \ldots, \tau_m]$, $\tau_i^{p\exp(v_i)} = 0$, $1 \leq i \leq m$ (e.g. N is any finite, commutative, local group scheme over a perfect field $k = R$). There exists a commutative formal Lie group on m parameters with coefficients in R, having N as a subgroup scheme (i.e. there exists a commutative formal group*

$$f\colon\ R[[X_1, \ldots, X_m]] \to R[[X_1, \ldots, X_m, Y_1, \ldots, Y_m]]$$

inducing the given comultiplication on $R[\tau_1, \ldots, \tau_m]$).

Proof. We take $k = \mathbf{F}_p \subset R$; the R-bialgebra E with its truncation type defines a point $e \in W(R)$. We choose a big integer r; by (4.1) there exists a point $d \in D(R)$ such that $\rho(d) = e$; by the results of Lazard (cf. the beginning of section 4) any commutative r-bud on m parameters $e \in D(R) = \Delta_{m,r}(R) \subset \Lambda_{m,r}(R)$ can be extended to a formal Lie group on the same number of parameters, with coefficients in the same ring. Thus the corollary is proved.

Example (constructed by M. Hazewinkel). There exist non-commutative finite local group schemes on m parameters which cannot be embedded into a formal Lie group on m parameters. Let $\mathrm{char}(k) = p$, n and m are positive integers, and $a, b \in k$. We define

$$E = k[\tau]/(\tau^{p\exp(n+m)}),$$

$$s(\tau) = \tau \otimes 1 + 1 \otimes \tau + a\,\tau^{p^n} \otimes \tau^{p^m} + b\,\tau^{p^m} \otimes \tau^{p^n}.$$

The s thus defined is associative; it is not cocommutative if we choose $n \neq m$ and $a \neq b$; in that case we have a local bialgebra on one parameter, which cannot be extended to a formal Lie group on one parameter if k is a field, because every one-parameter formal Lie group over k is commutative, cf. [6], and [7], Theorem 1, p. 253.

Remark. By different methods it was proved that any finite commutative group scheme over any field k can be embedded into an irreducible smooth k-algebraic group scheme G (cf. CGS, 15.4; cf. [12], in that case we can even take for k a complete local noetherian ring); however in general the dimension of G is much bigger than the number of parameters of N (suppose N to be local); in fact, if the rank of N is p^d, and k is algebraically closed, an imbedding of N into a d-dimensional group variety was constructed. In general a local finite, commutative group scheme on m parameters cannot be embedded into a group variety of dimension m (i.e. N being fixed, none of the formal Lie groups constructed in 5.2 need to be algebraizable), as is shown by the following

Example. Let k be a perfect field of characteristic p, and let N be the k-group scheme having as Dieudonné-module $W_\infty(k)[F, V]/(V-F^2, F^i)$, with $i \geqq 3$; this is a local group scheme on one parameter; it has rank p^i, the rank of $\operatorname{Ker}(p \cdot 1_N)$ is p^3 and the rank of $\operatorname{Ker}(V_N)$ is p^2. If G is an abelian variety of dimension one, the rank of $\operatorname{Ker}(p \cdot 1_G)$ is p^2, so $N \subset G$ is excluded. As $0 \neq \operatorname{Ker}(V_N)$, the case $N \subset \mathbf{G}_m$ is not possible. As $\operatorname{Ker}(V_N) \neq N$, we cannot embed N into a one-dimensional unipotent group-variety G (because any one-dimensional unipotent group variety is killed by V). Thus the N we have choosen cannot be embedded into a one-dimensional group variety.

Remark. Let $\nu_1 \leqq \nu_2 \leqq \cdots \leqq \nu_m$, $\mu_1 \leqq \mu_2 \leqq \cdots \leqq \mu_m$, with $\mu_i \geqq \nu_i$ for $1 \leqq i \leqq m$, and $\nu_j - \nu_i \geqq \mu_j - \mu_i$ for $1 \leqq i < j \leqq m$; using the methods exposed above, one can show that any $s \in \Omega_\nu(R)$ can be extended to an element $t \in \Omega_\mu(R)$; taking $\mu_1 = a = \mu_2 = \cdots = \mu_m$, and letting a grow, we obtain again (5.2).

References

1. Cartier, P.: Groupes algébriques et groupes formels. Coll. CBRM, Brussels 1962, 87–111.
2. Demazure, M., et A. Grothendieck: Schémas en groupes. Sém. géom. algébrique, IHES, 1963–1964. Referred to as SGAD.
3. Grothendieck, A., et J. Dieudonné: Éléments de géométrie algébrique. Publ. Math., IHES. Referred to as EGA.
4. Grothendieck, A.: Séminaire de géométrie algébrique. IHES, 1960. Referred to as SGA.
5. Lazard, M.: Lois de groupes et analyseurs. Ann. Sc. Éc. norm. sup. **72**, 299–400 (1955).
6. — La non-existence des groupes de Lie formels non abéliens à un paramètre. C. R. Acad. Sci. **239**, 942–945 (1954).

7. Lazard, M.: Sur les groupes de Lie formels à un paramètre. Bull. Soc. Math. France **83**, 251–274 (1955).
8. Lubin, J., and J. Tate: Formal moduli for one-parameter Lie groups. Bull. Soc. Math. France **94**, 49–60 (1966).
9. Mumford, D.: Lectures on curves on an algebraic surface (lecture notes Harvard University, 1964). Princeton Math. Notes 59.
10. Oort, F.: Commutative group schemes. Lecture Notes in Math. 15. Berlin-Heidelberg-New York: Springer 1966. Referred to as CGS.
11. – Algebraic group schemes in characteristic zero are reduced. Inv. Math. **2**, 79–80 (1966).
12. – Embedding of finite group schemes into abelian schemes. Mimeographed notes from the advanced science seminar in algebraic geometry, Bowdoin college, summer 1967.
13. Tate, J., and F. Oort: Finite group schemes of prime rank (to appear).

Frans Oort
Mathematisch Instituut
Nieuwe Achtergracht 121
Amsterdam
The Netherlands

David Mumford
Department Mathematics
Harvard University
2 Divinity Avenue
Cambridge, Mass., USA

(Received February 22, 1968)