Deformations and Liftings of Finite, Commutative Group Scheme

The Harvard community has made this article openly available. Please share how this access benefits you. Your story matters

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Published Version</td>
<td>doi:10.1007/BF01389779</td>
</tr>
<tr>
<td>Citable link</td>
<td><a href="http://nrs.harvard.edu/urn-3:HUL.InstRepos:3597249">http://nrs.harvard.edu/urn-3:HUL.InstRepos:3597249</a></td>
</tr>
<tr>
<td>Terms of Use</td>
<td>This article was downloaded from Harvard University’s DASH repository, and is made available under the terms and conditions applicable to Other Posted Material, as set forth at <a href="http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#LAA">http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#LAA</a></td>
</tr>
</tbody>
</table>
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 \( m \), where \( m = \operatorname{Ker}(R \to k) \), 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 \( k = \mathbb{F}_p \)) and let \( R \) be a ring with a reduction \( R \to k = R/m \), such that \( p \cdot 1 \notin m^2 \) (an "unramified" situation) (e.g. \( R = W_{\infty}(k) \), so \( W_{\infty}(\mathbb{F}_p) = \mathbb{Z}_p \), the ring of \( p \)-adic integers, or \( R = W_{\infty}(k)/p^2 \)). Let \( N_0 = \mathbb{G}_a, \) i.e. \( N_0 = \operatorname{Spec}(k[\tau]) \), \( \tau^p = 0 \), and the group law is defined by \( s_0 : E_0 \to E_0 \otimes_k E_0, E_0 = k[\tau] \), 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 \( a_i \in m \); the group law would be given by some ringhomomorphism \( s : E \to E \otimes_R E \), so

\[
s(\sigma) = \sigma \otimes 1 + 1 \otimes \sigma + \sum b_{ij} \sigma^i \otimes \sigma^j,
\]

\( b_{ij} \in m \).

* This work was partially supported by NSF grant GP 3512.
as \((s\sigma)^p = s(\sigma^p)\), we obtain:
\[ p \cdot (\sigma \otimes \sigma^{p-1} + \cdots + \sigma^{p-1} \otimes \sigma) \equiv 0 \pmod{m^2 \cdot E \otimes E}, \]
which is a contradiction.

Remark. In the previous situation, by a result of Tate (cf. [13]), we know that \(\alpha_s\) 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 \(a \in m\), and \(b \in m\).

Example (-B). Let \(R\) be an integral domain of characteristic zero, and let \(N = \text{Spec}(E)\) 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 \(B\),
\[ N_0(B) = \left\{ \text{the multiplicative group of matrices } \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \quad \alpha \in B, \quad \beta \in B, \quad \gamma = 1, \quad \delta = 0 \right\}; \]
so \(N_0 = \text{Spec}(E_0),\ E_0 = k[\tau, \rho]\) 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: \(A \subset K \leftarrow \cdots \leftarrow R\), where \(R\) is a characteristic zero local domain, \(\pi: R \to R/m = K\) its residue class map, and \(A\) a subring of \(K\), and that we are given finite free group schemes over these rings
\[
\begin{array}{ccc}
N_0 & \leftarrow & M_0 \\
\downarrow & & \downarrow \\
\text{Spec}(A) & \leftarrow & \text{Spec}(K) \rightarrow \text{Spec}(R),
\end{array}
\]
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 $N \to \text{Spec}(R')$ such that $N_0 \cong N \otimes_{R'} A$ and $M \cong N \otimes_{R'} R$.

Proof. Let $N_0 = \text{Spec}(E_0)$, $M_0 = \text{Spec}(F_0)$, $M = \text{Spec}(F)$. 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 $E_0 \subset F_0$. 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 $E = \{ x \in F \mid \pi(x) \in E_0 \}$, 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 $N = \text{Spec}(E)$ 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_II, 10.3.1).

**Corollary (2.3).** Let $k \leftarrow A \leftarrow K$ be ring homomorphisms, and let $N_0 = \text{Spec}(E_0)$ 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 $\text{char}(k) = p > 0$, take $B = k[T]$, and define a $B$-bialgebra by $E = B[T]$ with $\tau = T \tau$ and $s(\tau) = \tau \otimes 1 + 1 \otimes \tau$; for any field $K \supset k$ and for any $t \in \text{Spec}(B)(K)$ with $t \neq 0$ (i.e. for any $k$-algebra homomorphism $\varphi: B \to K$ such that $\varphi(T) \neq 0$) $E_t$ is the bialgebra of a reduced
group scheme, isomorphic to \( \mathbb{Z}/p \) in case \( K \) is algebraically closed, while \( E_0 \) is the bialgebra of the group scheme \( \mathcal{A}_p \).

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 that 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; \( N = \text{Spec}(E) \). Then there exist integers \( v_1, \ldots, v_m \) and an isomorphism

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

(cf. SGAD, Exp. VII \( B \), 5.4; we are writing \( p = p^a \) 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 \( a \in k, a \neq k^p, E = k[X, Y]/(X^p, X^p - aY) \), and \( s(X) = X \otimes 1 + 1 \otimes X, s(Y) = 1 \otimes 1 \otimes Y \).

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

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

(with \( X_0^0 = 1 \)), 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 \( \mu \) satisfies the condition \( (P \nu)_i \) for \( 1 \leq i \leq m \), if there exists an index \( j \) such that

\[
\alpha_j \cdot p^{v_j} \geq p^{v_j}
\]

or, equivalently \( (X^\alpha)^{p^{v_j}} \) is in the ideal generated by \( X_1^{p^{v_1}}, \ldots, X_m^{p^{v_m}} \). We say that a polynomial in \( X_1, \ldots, X_m \) satisfies \( (P \nu) \), if it is can be written as a sum of monomials which all satisfy condition \( (P \nu)_i \).

We say that a polynomial in the variables \( X_j \otimes X_k, 1 \leq j \leq m, 1 \leq k \leq m \), satisfies condition \( (P \nu)_i \) if it can be written as a sum

\[
\sum_t \mu_{1t} \otimes \mu_{2t}
\]

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

**Remark.** Let \( B \) be an integral domain of characteristic \( p \), and let \( N = \text{Spec}(E) \) be a finite \( B \)-group scheme, \( E = B[\tau_1, \ldots, \tau_m] \) with \( \tau_i^{p^{v_i}} = 0 \),
Deformations and Liftings of Finite, Commutative Group Schemes

1 \leq i \leq m; the comultiplication is denoted by \( s: E \to E \otimes E \). As \( s \) is a \( \tau_{(p)} = 0 \), so \( s(\tau_i) \) is a polynomial in \( \tau_i \otimes \tau_k \) which satisfies condition \((P \psi)\). The same for the polynomials \( \gamma(\tau_i) \), where \( \gamma \): \( E \to E \) defines the inverse.

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

\[
\Sigma(B) = \{ \text{all cocommutative } B \text{-bialgebra structures on } B[\tau_1, \ldots, \tau_m] = E, \text{ such that } s(\tau_i) \text{ are polynomials satisfying condition } (P \psi) \text{ for } \}
\]

\[
1 \leq i \leq m \},
\]

where \( \tau_i^{p \exp(v_i)} = 0 \) for \( 1 \leq i \leq m \), 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 \( \Sigma : C \to \text{Ens} \) 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 \( \Sigma \) 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: \( \Sigma \) is representable. Consider all combinations \((i, \alpha = (\alpha_1, \ldots, \alpha_m), \beta = (\beta_1, \ldots, \beta_m)) \) such that \( 1 \leq i \leq m \), \( 0 \leq \alpha_j < p \exp(v_j) \), \( 0 \leq \beta_j < p \exp(v_j) \), and such that the monomial \( \tau^\alpha \otimes \tau^\beta \) satisfies condition \((P \psi)\) (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 \( \tau_i^{p \exp(v_i)} = 0 \), \( 1 \leq i \leq m \). Then we are given an \( A \)-algebra homomorphism

\[
s: F \to F \otimes_A F
\]

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 \((P \psi)\), 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 \( Is = (s \otimes 1) \cdot s = (1 \otimes s) \cdot s \), and

\[
(I s)(\tau_i) = \sum_J H_{ij} \mu_j, \quad 1 \leq i \leq m,
\]

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

\[
\mathfrak{p} = (\ldots, H_{ij}, \ldots, Y_{i, \alpha, \beta} - Y_{i, \beta, \alpha}, \ldots) \cdot A.
\]
We define \( U = A/p \), and \( E = U[^m] \). It is clear that \( s \) induces a coassociative comultiplication

\[
s : E \to E \otimes_E E,
\]

defined by

\[
s(t_i) = t_i \otimes 1 + 1 \otimes t_i + \sum_{a, \beta} y_{i, a, \beta} \tau^a \otimes \tau^\beta,
\]

where \( y_{i, a, \beta} = Y_{i, a, \beta} \mod p \). Clearly the pair \((U, E)\) represents the functor \( \Omega_m, \gamma = \Omega \) defined by:

\[
\Omega(B) = \{ \text{all cocommutative coassociative } B\text{-algebra homomorphisms } s : E \to E \otimes_B E, \text{ where } E = B[^m], \text{ such that } s(x) = x \otimes 1 + 1 \otimes x \mod a \otimes a, \ a = (t_1, \ldots, t_m) \cdot E, \text{ and such that } s(t_i) \text{ satisfies condition } (P \gamma_i) \text{ for } 1 \leq i \leq m \}.
\]

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

**Lemma (3.2).** Let \( B \) be a ring in which \( p \cdot 1 = 0 \), let \( E = B[^m] \) with \( \tau^{\exp(\nu_i)} = 0 \), \( 1 \leq i \leq m \), and with augmentation ideal \( a = (t_1, \ldots, t_m) \cdot E \). Let \( s : E \to E \otimes_B E \) be a \( B\)-algebra homomorphism such that

\[
s(x) = x \otimes 1 + 1 \otimes x \mod a \otimes a
\]

for all \( x \in a \) (i.e. the augmentation is a left- and a right-coidentity), and such that \( s(t_i) \) satisfies condition \((P \nu)\), for \( 1 \leq i \leq m \). Then there exists a unique \( B\)-algebra homomorphism \( \gamma : E \to E \) such that \( m(\gamma \otimes 1) s(x) = 0 \) for all \( x \in a \) (where \( m : E \otimes_B E \to E \) is the multiplication).

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

\[
m(\gamma_1 \otimes 1) s(x) = a^2
\]

for all \( x \in a \), and it is unique modulo \( a^2 \) among all having this property. Suppose for some \( N \geq 1 \) there is given a \( B\)-algebra homomorphism \( \gamma_N : E \to E \) such that

\[
m(\gamma_N \otimes 1) s(x) = \rho_N(x) \in a^{N + 1}
\]

for all \( x \in a \), and such that \( \gamma_N(t_i) \) satisfies condition \((P \nu)\), for \( 1 \leq i \leq m \). It is easy to see that \( \rho_N(t_i) \) satisfies condition \((P \nu)\); thus

\[
\gamma_{N + 1}(t_i) = \gamma_N(t_i) - \rho_N(t_i), \quad 1 \leq i \leq m,
\]

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

\[
m(\gamma_{N + 1} \otimes 1) s(x) = a^{N + 2}
\]

for all \( x \in a \), and \( \gamma(t_i) - \gamma_{N + 1}(t_i) \in a^{N + 1} \) for all \( i \), then \( \gamma(x) = \gamma_{N + 1}(x) \) (mod
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 $W = \text{Spec}(U)$; consider the point $0 \in W(k)$ defined by $y_{i, a, \rho} \to 0$, i.e. $s(\tau_i) = \tau_i \otimes 1 + 1 \otimes \tau_i$, and $\gamma(\tau) = -\tau_i$; that is the point corresponding to the rigidified group scheme $\mathcal{S}_{\exp(v_0)} \times \cdots \times \mathcal{S}_{\exp(v_m)}$.

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 $H^3_{\text{symm}}(N, G_a) = 0$ (trivial action of the commutative finite group scheme $N$ on the additive linear group $G_a$) (proved in his Harvard thesis, 1966, later generalized into a structure theorem about the cohomology ring $H^*(N, G_a)$, 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

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

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

$$(\Gamma f)(X_i) \equiv 0 \pmod{r} \text{ for } 1 \leq i \leq m$$

(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 $f(X_i) \equiv g(X_i) \pmod{r + 1}$ for $1 \leq i \leq m$ (cf. [5], p. 381, Definition 13.1); a system $f_1, f_2, \ldots$, such that $f_i$ is an $r$-bud on $m$ parameters, and such that $f_i$ and $f_{i+1}$ 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$-bourgeons abéliens") on } m \text{ parameters with coefficients in } R\}$;

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

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

\[ N(m, r) = N = m \binom{r + m}{m} - m - 1; \]

there exists a universal

\[ E_r \in A_{m,r}(A_r), \quad A_r = \mathbb{Z}[T_1, \ldots, T_{N(m, r)}], \]

i.e. \((A_r, E_r)\) represents the functor \(A_{m,r}\), or: the map

\[ \text{RHom}(A_r, R) \rightarrow A_{m,r}(R) \]

defined by \(\varphi \mapsto (A \varphi)(E_r)\) is bijective for every \(R\).

(ii) The natural restriction map \(A_{m,r+1}(R) \rightarrow A_{m,r}(R)\) 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

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

such that \(E_r \in A_r(A_r) \subset A_r(A_{r+1})\) and \(E_{r+1} \in A_{r+1}(A_{r+1})\) define the same \(r\)-bud.

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

\[ \begin{array}{ccc}
A_r & \xrightarrow{\varphi_r} & A_{r+1} \\
\downarrow & & \downarrow \\
R & \xrightarrow{\varphi_{r+1}} & R
\end{array} \]

commutes. Hence

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

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

\[ r \geq 3 \cdot \sum_{i=1}^{m} (p \exp(v_i) - 1). \]

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

\[ \Delta_{m,r,v} = \Delta \subset A_{m,r} \]

\[ \Delta(R) = \{ f \in A_{m,r}(R) \text{ such that } f(X_i) \text{ satisfies condition } (P v_i) \text{ for } 1 \leq i \leq m \}. \]
For \( f \in A(R) \), we define \( \rho(f) \) by

\[
\rho(f)(\tau_i) = f(X_i) \mod (X_i^{p \exp(v_i)}, \ldots, X_m^{p \exp(v_m)});
\]

because of the conditions \((P v)_i\) we thus obtain an \( R \)-algebra homomorphism (!)

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

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

\[
(f \circ s)(\tau_i) = 0, \quad 1 \leq i \leq m,
\]

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):

\[
\Sigma \cong \Omega_m, \Omega \leftarrow \text{A}_{m,r} \subset \text{A}_{m,r}.
\]

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

\[
\text{A}, \text{A}, \Omega: \text{C} \to \text{Ens}
\]

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 \( \rho: D \to W \) is given by a projection

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

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

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

**Lemma (4.2).** Let

\[
f(X_i) = \sum_{x, \beta} a_{i, x, \beta} X^x \otimes X^\beta
\]

be polynomials with coefficients in a ring \( R \) with \( p \cdot 1 = 0 \), such that \( f(X_i) \) satisfies condition \((P v)_i\), \( 1 \leq i \leq m \); 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 \((P v)_i\).

**Proof.**

\[
(f \otimes 1) f(X_i) = \sum_{x, \beta} a_{i, x, \beta} \left( \prod_j \left( \sum a_{i, j, \gamma} X_j^\gamma \otimes X^\beta \right)^{v_j} \right) \otimes X^\beta = \sum_{x, \beta} a_{i, x, \beta} Q_{i, x, \beta}.
\]

It suffices to consider each \( Q_{i, x, \beta} \) separately; either \( X^\beta \) satisfies condition \((P v)_i\), and we are done, or there exists an index \( e \) such that \( x_e \cdot p \exp(v_e) \geq p \exp(v_e) \), so \( p \exp(n + v_e) \geq p \exp(v_e) \) with \( x_e \geq p^n \), and \( n \geq 0 \); in that case

\[
Q_{i, x, \beta} = \left( \left( \sum a_{i, e, \gamma} X^\gamma \otimes X^\beta \right)^{p^n} \times \cdots \right) \otimes X^\beta
\]

\[
= \left( \left( \sum [a_{i, e, \gamma} X^\gamma \otimes X^\beta]^{p^n} \times \cdots \right) \otimes X^\beta; \right.
\]
for each \((e, y, \delta)\) there exists an index \(d\) such that \(p^d \cdot p \exp(v_e) \equiv p \exp(v_e),\)
\(\delta^d \cdot p \exp(v_y) \equiv p \exp(v_y),\)

hence

\[p^d \cdot \delta^d \cdot p \exp(v_e) \equiv p^d \cdot p \exp(v_e) \equiv p \exp(v_e),\]

or the same with \(\delta^d\), and \((Q_{e, y, \delta})^{p \exp(v_e)}\) is divisible by \((X_{e, y, \delta} \otimes 1 \otimes 1)^{p \exp(v_e)}\), respectively divisible by \((1 \otimes X_{e, y, \delta} \otimes 1)^{p \exp(v_e)}\), 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 \(E = R[X_1, \ldots, X_n]\), and \(g : E \rightarrow E \otimes E\) so that

\[g(X_i) \equiv X_i \otimes 1 + 1 \otimes X_i \pmod{M \cdot E \otimes E}.\]

Let \(P = b \cdot X^a \otimes X^b\) be a monomial such that \(X^a\) and \(X^b\) do not satisfy condition \((P \otimes 1)\) (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 \((P \otimes 1)\).

**Proof.**

\[(g \otimes 1)(P) = b \cdot g(X^a) \otimes X^b = b \cdot \prod_j (X_j \otimes 1 + 1 \otimes X_j)^{p^j} \otimes X^b\]

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

(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 \(W(R)_w \rightarrow W(R/I)_w\) is surjective (we write \(W(R)_w\) for the set of morphisms \(W \rightarrow \text{Spec}(R)\) with \((W \rightarrow \text{Spec}(R) \rightarrow \text{Spec}(k)) = w\).

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

\[\rho_* : t_{D, d} \rightarrow t_{W, \rho(d)}\]

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

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

\[k[[e_1, \ldots, e_n]] \rightarrow g_{W, w} \rightarrow g_{D, d}\]

as the tangential map \(\rho_*\) is surjective, the images of the \(e_i\)'s are linearly independent modulo the square of the maximal ideal of \(g_{D, d}\); as \(d\) is
a non-singular point this implies that the composition \( \varphi \cdot \pi \) is injective; thus \( \pi \) is injective (and it is also surjective), so \( \hat{\theta}_{W,w} \) 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 \( A = k[T_1, \ldots, T_N] \) and \( H_1, \ldots, H_d \in A \). Suppose given positive integers \( w(T_1), \ldots, w(T_N) \) such that \( H_1, \ldots, H_d \) are homogeneous polynomials in the weighed variables \( T_1, \ldots, T_N \) (i.e. we write \( w(\prod T_{n_i}) = \sum w(T_{n_i}) \); if \( \mu_1 \) and \( \mu_2 \) are monomials occurring with non-zero coefficients in some \( H_1 \), then \( w(\mu_1) = w(\mu_2) \)). Suppose \( H_i(0) = 0 = H_j(0) = \cdots = H_d(0) \), such that 0 is a non-singular point of \( V = \text{Spec}(A/(H_1, \ldots, H_d)A) \). Then we can renumber the variables, and we can choose \( 0 \leq n \leq N \) so that

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

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

\[
(H_1, \ldots, H_d)A \subset (T_1^2, \ldots, T_i T_j, \ldots, T_N^2)A = b,
\]

so

\[
\text{Spec}(A/b) \subset V = \text{Spec}(k[T_1, \ldots, T_N]),
\]

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

\[
H_d = c T_N + G, \quad c \in k, \quad c \neq 0
\]

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 \( G \in k[T_1, \ldots, T_{N-1}] \). We write

\[
G_i = H_1 \left( T_1, \ldots, T_{N-1}, -\frac{1}{c} G(T_1, \ldots, T_{N-1}) \right), \quad 1 \leq i < d,
\]

and clearly

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

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

**Proof of Proposition (4.1).** We proved that \( \Omega \) is represented by \( W \) in Section 3, by the results of Lazard we know \( A \) is representable, and it is easy to see that \( A \) 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

$$D(R) = D(R')$$

is a surjective map. Thus given $f' \in D(R)' = D(R)'$, we would like to construct $f \in D(R)$ so that $f' \equiv f (\text{mod } I \cdot E \oplus E)$ (where $E = k[X_1, \ldots, X_m]$); by the result of Lazard we know that $A$ is represented by a non-singular scheme (in fact affine space of dimension $N(m, r)$), so for $f' \in A(R)^0 \subset A(R)'$ there exists a $g \in A(R)^0$ so that

$$f' \equiv g \pmod{I \cdot E \oplus E}.$$  

We know that

$$g(X_i) \equiv X_i \otimes 1 + 1 \otimes X_i \pmod{M \cdot E \oplus E},$$

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 $(Pv)$, and $f(X_i)$ consists of monomials which satisfy condition $(Pv)$. We claim that

$$(f') \equiv 0 \pmod{r + 1},$$

i.e. $f \in A(R)^0$; in fact let

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

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

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

$$(g \otimes 1) g(X_i) = [(f \otimes 1) f(X_i)]$$

$$+ \left[ \sum_{a, \beta} b_{i, z, \beta} X^a \otimes X^\beta \otimes 1 + (g \otimes 1) \left( \sum_{a, \beta} b_{i, z, \beta} X^a \otimes X^\beta \right) \right].$$

By (4.2) the first term in square brackets can be written as a sum of monomials all satisfying condition $(Pv)$; by (4.3) the second term can be written as a sum of monomials none of which satisfy condition $(Pv)$. Thus the equation $((f') \equiv 0 \pmod{r + 1})$ proves, by sorting out all $(Pv)$-monomials, that

$$(f') \equiv 0 \pmod{r + 1},$$

thus $f \in A(R)^0$, 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 $\mathfrak{t}_{D, 0} = A(k[\varepsilon])^0$, hence by (4.4) it suffices
to show that

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

is a surjective map. Hence we are given

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

with

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

satisfying \((P \nu)\), and \((I s) = 0\), and we have to construct an \(r\)-bud \(f\) satisfying again the conditions \((P \nu)\), 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

\[ (f \otimes 1)(X_i) = X_i \otimes 1 \otimes 1 + X_i \otimes 1 + 1 \otimes 1 \otimes X_i \]

\[ + \varepsilon \cdot \sum c_{i, \alpha, \beta} X^\alpha \otimes X^\beta \otimes 1 \]

\[ + \varepsilon \cdot \sum c_{i, \alpha, \beta} \prod_j (X_j \otimes 1 + 1 \otimes X_j)^{y_j} \otimes X^\gamma; \]

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 \(\rho_*\) 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 \(A'\) be the set of pairs \((x, \beta)\) with \(x = (x_1, \ldots, x_m)\), \(\beta = (\beta_1, \ldots, \beta_m)\) so that \(1 \leq |x|\) and \(1 \leq |\beta|\) and \(|x| + |\beta| \leq r\); let \(A''\) be the set of triples \((x, \beta, y)\) with \(1 \leq |x|\), \(1 \leq |\beta|\), \(1 \leq |y|\), and \(|x| + |\beta| + |y| \leq r\). Let \(\Omega'\) be the set of pairs \((x, \beta)\) with \(1 \leq |x|\) and \(0 \leq x_j < p \exp(v_j)\) for \(1 \leq j \leq m\), and \(1 \leq |\beta|\) and \(0 \leq \beta_k < p \exp(v_k)\) for \(1 \leq k \leq m\); let \(\Omega''\) be the set of triples \((x, \beta, y)\) with \(1 \leq |x|\) and \(0 \leq x_j < p \exp(v_j)\), etc. Consider

\[ F(X_i) = X_i \otimes 1 + 1 \otimes X_i + \sum_{x, \beta} T_{i, x, \beta} X^x \otimes X^\beta, \]

summation taken over all \((x, \beta)\in A'\), respectively summation taken over all \((x, \beta)\in \Omega'\); we write \(k[A']\), resp. \(k[\Omega']\), for the polynomial ring \(k[\ldots, T_{i, x, \beta}, \ldots], 1 \leq i \leq m\) and \((x, \beta)\in A'\), resp. \(1 \leq i \leq m\) and \((x, \beta)\in \Omega'\). We define polynomials \(H_{i, x, \beta, y} \in k[A']\), resp. \(H_{i, x, \beta, y} \in k[\Omega']\) by

\[ (\Gamma F)(X_i) = \sum_{x, \beta, y} H_{i, x, \beta, y} X^x \otimes X^\beta \otimes X^y. \]

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

\[ T_{i, x, \beta} = T_{i, \beta, x}, \quad \text{all } 1 \leq i \leq m \text{ and } (x, \beta)\in A', \text{ resp. } (x, \beta)\in \Omega'; \]

\[ T_{i, x, \beta} = 0 \quad \text{if } X^x \otimes X^\beta \text{ does not satisfy } (P \nu); \]

\[ H_{i, x, \beta, y} = 0, \quad \text{all } 1 \leq i \leq m \text{ and } (x, \beta, y)\in A'', \text{ resp. } (x, \beta, y)\in \Omega''. \]
Consider \((F \otimes 1) F(X_i)\); part of this has the form
\[
\sum T_{i, x, \beta} \left( \prod_j (X_j \otimes 1 + 1 \otimes X_j) + \sum T_{j, \gamma, \delta} X^\gamma \otimes X^\delta \right) \otimes X^\beta;
\]
each term of this sum is of the form
\[
T_{i, x, \beta} \cdot \prod_{1 \leq r \leq |\beta|} (T_{r, \lambda_r, \mu_r} X^{\lambda_r} \otimes X^{\mu_r}) \otimes X^\beta
\]
(where the question mark indicates some integer, \(1 \leq ? \leq m\), and where \(T_{r, 1, 0} = 1 = T_{r, 0, 1}\)); the monomial in the \(T\)'s obtained thus has weight
\[
|\alpha| + |\beta| - 1 + \sum \left( |\lambda_r| + |\mu_r| - 1 \right) = a,
\]
while the corresponding term in the \(X\)'s has total degree
\[
\sum |\lambda_r| + \sum |\mu_r| + |\beta| = a + 1;
\]
so each term in the polynomial \(H_{i, x, \beta, \gamma}\) has weight \(|\alpha| + |\beta| + |\gamma| - 1\).

Thus both \(D\) and \(W\) are defined by homogeneous equations in the weighed variables \(T_{i, x, \beta}\) 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 \(a \in k[\Delta]\), respectively \(b \subset k[\Omega]\) be the ideal defining \(D\), resp. \(W\). Renaming the variables we obtain: \(k[\Omega] = k[T_1, \ldots, T_N]\) and \(k[\Delta] = k[T_1, \ldots, T_N, T_{N+1}, \ldots, T_{N+m}]\). We have proved already that there exists a number \(n\), with \(0 \leq n \leq N\), so that
\[
k[T_1, \ldots, T_n] \leftarrow k[T_1, \ldots, T_n]
\]
\[
\downarrow
\]
\[
k[T_1, \ldots, T_n]/b.
\]

The morphism \(\rho: D \rightarrow W\) comes from the ringhomomorphism \(\varphi\):
\[
k[T_1, \ldots, T_n] \leftarrow k[T_1, \ldots, T_{N+m}]
\]
\[
\downarrow
\]
\[
k[T_1, \ldots, T_n] / \cong U = k[T_1, \ldots, T_N]/b \rightarrow k[T_1, \ldots, T_{N+m}]/a = B, \quad \rho = \varphi; \quad \text{Spec}(U) = W \leftarrow \rightarrow \rightarrow \rightarrow D = \text{Spec}(B),
\]
we are done if we can prove that if we apply the elimination lemma to \(a \subset k[T_1, \ldots, T_{N+m}]\), none of the variables \(T_1, \ldots, T_n\) is eliminated: in that case
\[
k[T_1, \ldots, T_n] / \cong U \rightarrow B \cong k[T_1, \ldots, T_n, T_{N+1}, \ldots, T_{N+m}]
\]
for some $m$ with $0 \leq m \leq M$ (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 $T_{i,x,\beta}$ with $(\alpha, \beta) \in \Omega'$ appears in the linear term of some $H_{j,\gamma,\delta,\epsilon}$, with $(\gamma, \delta, \epsilon) \in \Delta''$, then $(\gamma, \delta, \epsilon) \in \Omega''$; but this is clear: computing $(F \cap F)(X_i)$ we obtain:

$$
\sum T_{i,\alpha,\beta} X^\alpha \otimes X^\beta \otimes 1 - \sum T_{i,\alpha,\beta} 1 \otimes X^\alpha \otimes X^\beta
$$

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

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

so “$T_{i,\alpha,\beta}$ appears in the linear term of $H_{j,\gamma,\delta,\epsilon}$” and $(\alpha, \beta) \in \Omega'$ imply that $(\gamma, \delta, \epsilon) \in \Omega''$. Thus we have shown that the variables $T_{n_1}, \ldots, T_n$ can be expressed in the variables $T_1, \ldots, T_n$, that $T_{N+1}, \ldots, T_{N+M}$ depend on $T_1, \ldots, T_n,$ $T_{N+1}, \ldots, T_{N+m}$, and that the variables $T_1, \ldots, T_n$ cannot be eliminated. Thus the proof of the proposition is concluded.

**Remark.** The multiplicative semi-group scheme $A^*_i = \text{Spec}(k[T])$ acts on $k[A']$ and on $k[Q']$ (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 $D-\{0\}/G_\text{m}$ and $W-\{0\}/G_\text{m}$ are projective schemes, it easily follows that $\rho:\ D(k)\to W(k)$ 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 $(v_1, \ldots, v_m)$.

**Remark.** Let $V$ be the $k$-algebraic scheme such that for every $B \supseteq k$, $V(B) = \{\text{all commutative } B\text{-bialgebra structures on } B[\tau_1, \ldots, \tau_m] = E\}$; then $V_{\text{red}} = W$, and $V = W$ if and only if $v_1 = \cdots = v_m$.

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 $K \supseteq k$; 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 $N_{\text{sep}} = \text{Spec}(k \times \cdots \times k)$, take any characteristic zero domain $R$ with a reduction $R \to k$, choose $M = \text{Spec}(R \times \cdots \times R)$, etc.). As $k$ is supposed to be algebraically closed, hence perfect, $N_{\text{loc}}$ admits a truncation type $v = (v_1, \ldots, v_m)$, hence by (3.1) there exists a point
where $W$ is an irreducible, smooth $k$-algebraic scheme, and a finite, free group scheme $M \rightarrow W$, such that $N_{\text{loc}} \cong M_w$ (i.e. the fibre of $M$ at the point $w$ is isomorphic, as a group scheme, with $N_{\text{loc}}$). 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 $M^0 \rightarrow W$ over the point $u \in W(k)$ is reduced (by $D$ we denote the dualizing functor associated 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 $W = \text{Spec}(U)$. It follows that the group scheme $M^0_L$ is reduced, so $M^0_L$ can be lifted to characteristic zero by what is said before, so $M^0_L$ can be lifted to characteristic zero as $D$ commutes with base extension, so by (2.3) it follows that $M \otimes_U k \cong M_u \cong N_{\text{loc}}$ 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 $N = \text{Spec}(E)$ be a commutative $R$-group scheme such that $E$ admits a truncation type $E \cong R[\tau_1, \ldots, \tau_m]$, $\tau^p_i \exp(v_i) = 0, 1 \leq i \leq m$ (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

$$f: R[[X_1, \ldots, X_m]] \rightarrow R[[X_1, \ldots, X_m, Y_1, \ldots, Y_m]]$$

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

**Proof.** We take $k = \mathbb{F}_p \subset R$; 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 $e \in D(R) = \Lambda_m, \tau(R) \subset \Lambda_m, \tau(R)$ 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 groups schemes on $m$ parameters which cannot be embedded into a formal Lie group on $m$ parameters. Let $\text{char}(k) = p$, $n$ and $m$ are positive integers, and $a, b \in k$. We define

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

$$s(\tau) = \tau \otimes 1 + 1 \otimes \tau + a \tau^n \otimes \tau^{nm} + b \tau^{nm} \otimes \tau.$$
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 $p^2$, and $k$ is algebraically closed, an embedding 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 $W_n(k)[F,V]/(V-F^2, F^i)$, with $i \geq 3$; this is a local group scheme on one parameter; it has rank $p$, the rank of $\text{Ker}(p \cdot 1_N)$ is $p^2$ and the rank of $\text{Ker}(V_N)$ is $p^2$. If $G$ is an abelian variety of dimension one, the rank of $\text{Ker}(p \cdot 1_N)$ is $p^2$, so $N \subset G$ is excluded. As $0 \neq \text{Ker}(V_N)$, the case $N \subset G_m$ is not possible. As $\text{Ker}(V_N) \neq N$, we cannot embed $N$ into a one-dimensional unipotent group-variety $G$ (since any one-dimensional unipotent group variety is killed by $V$). Thus the $N$ we have chosen cannot be embedded into a one-dimensional group variety.

**Remark.** Let $v_1 \leq v_2 \leq \cdots \leq v_m$, $\mu_1 \leq \mu_2 \leq \cdots \leq \mu_m$, with $\mu_i \geq v_i$ for $1 \leq i \leq m$, and $v_j - v_i \geq \mu_j - \mu_i$ for $1 \leq i < j \leq m$; using the methods exposed above, one can show that any $s \in \Omega_n(R)$ can be extended to an element $t \in \Omega_m(R)$; taking $\mu_1 = a = \mu_2 = \cdots = \mu_m$, and letting $a$ grow, we obtain again (5.2).

**References**

12. — Embedding of finite group schemes into abelian schemes. Mimeographed notes from the advanced science seminar in algebraic geometry, Bowdoin college, summer 1967.

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)