TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 233, 1977

ON CURVES ON FORMAL GROUPS

BY

ROBERT A. MORRIS[1] AND BODO PAREIGIS

ABSTRACT. The structure of the group of curves on a formal group is determined when the formal group is on a truncated power series algebra over a commutative ring. The resulting curve functor is faithful but not full. Applications to the Lie algebra of the formal group are given.

Introduction. Let K be a commutative ring, $A = K[[x_1, \ldots x_n]]/I$ where I is generated by powers of (some of) the x_i. We call such an algebra a truncated power series algebra and endow it with the natural topology. Giving K the discrete topology makes A a topological K-algebra in the $\mathfrak{m}$-adic topology: it is an inverse limit of finitely generated free quotient algebras. It is in fact a *pf*-algebra in the sense of [8], [9] so the functor $A^{\cdot} = K\text{-Alg}_{\text{cont}}(A, -)$ from K-algebras (regarded as discrete) to sets is a formal scheme over K. If, further, A has a topological Hopf-algebra structure then $A^{\cdot}$ is a formal group.

The bialgebras arising in this context are precisely "divided power Hopf algebras".

Studying sequences of divided powers in these Hopf algebras or more generally in divided power coalgebras is the same as studying curves in the corresponding formal schemes.

The formal groups studied here are a mixture of a classical formal group and a finite local group scheme over K. It is known that the curves classify the classical formal groups which are commutative [2], [3], and Oort [10] has used this to derive a related theory for finite local commutative groups.

We give here a Cartier type theory for these mixed truncated power series groups even in the noncommutative case. These groups appear naturally: a famous result of Dieudonné, Cartier and Gabriel asserts that if K is a perfect field any connected formal group of finite type has this form.

The image in a formal group G of any curve is formal subscheme and we give simple examples even over fields where all curves lie in a fixed proper subscheme. However, we prove that the smallest formal subgroup containing

Received by the editors April 26, 1976.

AMS (MOS) subject classifications (1970). Primary 14L05.

Key words and phrases. Formal groups, Dieudonné theory, Hopf algebras, divided powers.

[1] The first author is pleased to acknowledge the hospitality of both The Institute for Advanced Study, Princeton, and the Mathematisches Institut der Universität München during some of this research. Supported in part by the National Science Foundation.

all the curves is G itself and thereby show that our curve functor is faithful on the cateogry of formal groups on truncated power series algebras. The curve functor is not faithful on the category of formal schemes on truncated power series algebras. This is quite different from the situation for nontruncated power series [7, I. 10.3]. This intervenes to prevent our curve functor on the category of groups from being full (cf. [7, III. 8.4] for the nontruncated case) as we show by counterexample. Nevertheless, we are able to describe the structure of the curve groups in terms of a Verschiebung operator and in such a way that the Lie algebra of the formal group can be described just in terms of curves, provided the curves are "long enough". In fact the failure of certain curves to be long enough leads to the counterexample to fullness of the curve functor.

Unexplained terminology and notation is that of [8], [9].

A number of our theorems are implicitly or explicitly contained in the work of Ditters [5 bis]. As these notes do not seem widely available, we have stated for completeness the appropriate results. In many cases a strictly computational proof is possible at the cost of some of Ditters' generality. We sketch or allude to such computation.

We thank the referee for pointing out the overlap with Ditter's notes, and for suggesting an illuminating compression of an early version of our text.

1. Formal groups over truncated power series algebras.

Let

$$A = K[[x_1, \ldots, x_n]]/(x_1^{s_1}, \ldots, x_n^{s_n})$$

with $s_i = 1, 2, 3, \ldots, \infty$. If $s_i = \infty$ we mean no power of x_i lies in the ideal factored out. By abuse of notation we will also write x_i for the canonical generators of A so that $x_i^{s_i} = 0$. We say A has *truncation type* $s = (s_1, \ldots, s_n)$. Note $\mathfrak{m} = (x_1, \ldots, x_n)$ is the kernel of the natural augmentation $\varepsilon\colon A \to K$. As we are going to give a Hopf-algebraic characterization of curves, we require some tools on the diagonalization of elements of $\mathfrak{m}$.

The following lemmas will be easily proved by the reader in the prescribed order. They hold formally, in fact, for any topological Hopf algebra A whose underlying algebra is the limit–with surjective projections–of finite projective K-algebras. Ditters [5 bis] considers the case when all these are free.

Lemma 1. *Observe that A is a topological Hopf algebra with respect to the complete tensor product $\hat{\otimes}$. If a is in $\mathfrak{m}$ then $\Delta(a) = a \hat{\otimes} 1 + 1 \hat{\otimes} a + \Sigma b_i \hat{\otimes} c_i$ with b_i, c_i in $\mathfrak{m}$.*

Lemma 2. $\Delta(\mathfrak{m}^i) \subseteq \Sigma_{k=0}^{i} \mathfrak{m}^k \hat{\otimes} \mathfrak{m}^{i-k}$, *where $\mathfrak{m}^0$ denotes $A = K \oplus \mathfrak{m}$.*

Now set $A^0 = \mathrm{Hom}_{\mathrm{cont}}(A, K)$ [8], [9]. Let $(\mathfrak{m}^i)^\perp = \{f \in A^0 | f(\mathfrak{m}^i) = 0\}$. Note $k\varepsilon = \mathfrak{m}^\perp \subseteq (\mathfrak{m}^2)^\perp \subseteq \ldots$. Let $\langle f, x \rangle$ denote the action on $x \in A$ of

$f \in A^0$. Using Lemma 2 we easily get

LEMMA 3. $(\mathfrak{m}^i)^\perp(\mathfrak{m}^j)^\perp \subseteq (\mathfrak{m}^{i+j-1})^\perp$.

NOTATION. Suppose $\mathbf{j} = (j_1, j_2, \ldots, j_n)$ is an n-tuple of nonnegative integers. Set $X^{\mathbf{j}} = x_1^{j_1} \cdots x_n^{j_n}$. Define $e_{\mathbf{j}}$ in A^0 by $\langle e_{\mathbf{j}}, X^{\mathbf{k}}\rangle = \delta_{\mathbf{j},\mathbf{k}}$ whenever j_r and $k_r < s_r$ (recall s_r is the smallest integer with $x_r^{s_r} = 0$ in A and $s_r = \infty$ if there is no such integer). Then the $e_{\mathbf{j}}$ are a free set of K-generators. It is convenient to set $y_{ij} = e_{(0,\ldots,0,j,0,\ldots,0)}$ with j at the ith place. Since $e_{(j_1,j_2,\ldots,j_n)} \in (\mathfrak{m}^{j_1+j_2+\cdots+j_n+1})^\perp$, we get, in particular, that y_{ij} is in $(\mathfrak{m}^{j+1})^\perp$. By Lemma 3 it is then follows that $y_{1j_1}y_{2j_2}\ldots y_{nj_n}$ is in $(\mathfrak{m}^{j_1+j_2+\cdots+j_n+1})^\perp$.

LEMMA 4. $y_{1j_1}y_{2j_2}\ldots y_{nj_n}|_{\mathfrak{m}^k} = e_{j_1,\ldots,j_n}|_{\mathfrak{m}^k}$ *when* $k = j_1 + j_2 + \cdots + j_n$.

This allows us to give the expected

THEOREM 5. *Suppose A is a K-algebra of truncation type $(s_1, s_2, \ldots, s_n)$. Then $\{y_{1j_1}y_{2j_2}\ldots y_{nj_n}\}$ with $0 \leqslant j_r < i_r$, $r = 1, 2, \ldots, n$, is a free set of K-module generators of A^0.*

PROOF. By Lemma 4, $y_{1j_1} \cdots y_{nj_n} = e_{\mathbf{j}} + z$ with z in $(\mathfrak{m}^{j_1+\cdots+j_n})^\perp$. Now $(\mathfrak{m}^k)^\perp$ has generators $\{e_{\mathbf{k}} | k_1 + \cdots + k_n < k\}$; hence

$$(*) \qquad y_{1j_1}\ldots y_{nj_n} = e_{\mathbf{j}} + \sum \lambda_{\mathbf{k}} e_{\mathbf{k}}$$

where the sum is over all $\mathbf{k}$ with $\Sigma k_r < \Sigma j_r$. Thus by induction, equation $(*)$ may be solved for $e_{\mathbf{j}}$ in terms only of monomials in y_{rj_r}'s. Since the totality of $e_{\mathbf{j}}$'s generate A^0 (because $A^0 = \bigcup(\mathfrak{m}^k)^\perp$), so must the desired monomials. Further, $(*)$ shows these are linearly independent because the $e_{\mathbf{j}}$'s are.

For a converse see [1].

Theorem 5 is related to Theorem 3.5 of [5 bis], which states an equivalence between the existence of the claimed generators of A^0 and the property that the associated formal group is generated by curves (see below). Our Theorem 8 below is a special case of this second condition. Thus our deduction of Theorem 8 is really a proof of (b) ⇒ (a) of Ditters' result, and our Theorem 5 is a verification that (b) holds in our case.

2. Curves and sequences of divided powers.

DEFINITION AND NOTATION. Let C be a K-coalgebra. A finite (resp. infinite) sequence $\{z_i \in C | i = 0, \ldots, n\}$ (resp. $\{z_i \in C | i = 0, 1, \ldots\}$ is a *sequence of divided powers of length n* (resp. an *infinite sequence of divided powers*) if $\Delta(z_i) = \Sigma_{j=0}^{i} z_j \otimes z_{i-j}$ and $\varepsilon(z_i) = \delta_{0,i}$ for all i. (If K is a field and $z_0 \neq 0$ the augmentation condition follows from $(\varepsilon \otimes \mathrm{id}_c)\Delta = \mathrm{id}_c$.)

LEMMA 6. *For each j, $(y_{jr})_r$ is a sequence of divided powers over* 1 *in A^0, where A admits truncation type as in* §1.

Proof. Recall that the y_{jr} are dual to x_j^r. The result is then an easy exercise in the definition of Δ_{A^0} from the multiplication in A.

An element z in C is *grouplike* if $\Delta(z) = z \otimes z$ and $\varepsilon(z) = 1$ (again this is immediate if K is a field and $z \neq 0$). Thus any sequence of divided powers begins with a grouplike z_0.

The functor $K[[t]]^{\cdot}$ (resp. $(K[[t]]/(t^i))^{\cdot}$ is called the *formal affine line* (resp. *truncated line*). For economy of notation we will write $K[[t]]/(t^{\infty})$ for $K[[t]]$. In the notation of [8], [9] if $A^{\cdot}$ is a formal group then

$$\mathrm{Func}_{pf}\big(K[[t]]/(t^i)^{\cdot}, A^{\cdot}\big) = \mathrm{Alg}_{pf}\big(A, K[[t]]/(t^i)\big) = A^{\cdot}\big(K[[t]]/(t^i)\big)$$

is a group for each i, $1 < i < \infty$. The continuous algebra maps $f\colon K \to K[[t]]/(t^i)$ and $g\colon K[[t]]/(t^i) \to K$ given by $g(t) = 0$ induces a semidirect product of groups

$$1 \to \operatorname{Ker} g_* \to \mathrm{Alg}_{pf}\big(A, K[[t]]/(t^i)\big) \overset{g^*}{\underset{f^*}{\rightleftarrows}} \mathrm{Alg}_{pf}(A, k) \to 1.$$

We call the elements of $\operatorname{Ker} g^*$ (*truncated*) *curves in* $A^{\cdot}$ and write $C_i(A^{\cdot}) = \operatorname{Ker} g^*$. The natural identification $K[[t]] = \operatorname{proj\,lim} K[[t]]/(t^i)$ induces an isomorphism $C_{\infty}(A^{\cdot}) \cong \operatorname{proj\,lim} C_i(A^{\cdot})$.

Now $(K[[t]]/(t^i))^0$, for $1 < i < \infty$, is the cocommutative coalgebra $Kx_0 \oplus \cdots \oplus Kx_{i-1}$ with $\langle x_j, t^k\rangle = \delta_{jk}$ and $(x_j)_{j<i-1}$ a sequence of divided powers. Thus

$$\mathrm{Alg}_{pf}\big(A, K[[t]]/(t^i)\big) = \mathrm{Coalg}\big(Kx_0 \oplus \cdots \oplus Kx_{i-1}, A^0\big)$$

identifies $C_i(A)$ with the set of divided powers of length $i - 1$ in A^0. Explicitly, if $\varphi \in \mathrm{Alg}_{pf}(A, K[[t]]/(t^i))$ then one can write $\varphi(a) = \sum_{j=0}^{i-1}\varphi_j(a)t^j$ with $\varphi_j \in A^0$. A continuous linear map is an algebra homomorphism exactly when (φ_j) is a sequence of divided powers. Further there is a natural group structure on the set of divided powers of length $i - 1$ which this identification also respects. It is given by

$$(\varphi_j)_{j<i}(\psi_k)_{k<i} = \Big(\sum_r \varphi_r\psi_{s-r}\Big)_{s<i}.$$

We are interested in $C_i(A^{\cdot}) = \operatorname{Ker} g_*$. This corresponds to the kernel of

$$\mathrm{Coalg}\big(Kx_0 \oplus \cdots \oplus Kx_{i-1}, A^0\big) \to \mathrm{Coalg}(K, A^0),$$

that is, to sequences with $z_0 = \varepsilon_A = 1$ in A^0. We will call them *special* sequences (in case $i = \infty$ one thinks of them as curves through the origin of the group $A^{\cdot}$ [2]).

The following theorem shows that the group valued functor $C = \Pi C_i$ is faithful on the category of formal groups admitting a truncation type:

Theorem 7. *Let $A^{\cdot}$ and $B^{\cdot}$ be formal groups admitting* (*possibly different*) *truncation types and* $f^\cdot, g^\cdot\colon A^\cdot \to B^\cdot$ *be group homomorphisms. If* $C_i(f^\cdot) = C_i(g^\cdot)$ *for all* $i = 1, 2, \ldots, \infty$ *then* $f = g$.

PROOF. Since monomials of the form $y_{1j_1} y_{2j_2} \ldots y_{nj_n}$ are a basis of A^0, if $f \neq g$ then we conclude that $f^0(y_{ij}) \neq g^0(y_{ij})$ for some i, j (f^0 and g^0 are algebra maps). Hence

$$\begin{aligned} &C_j(f^\cdot)(1, y_{i1}, \ldots, y_{ij}) \\ &\quad = \big(1, f^0(y_{i1}), \ldots, f^0(y_{ij})\big) \\ &\quad \neq \big(1, g^0(y_{i1}), \ldots, g^0(y_{ij})\big) = C_j(g^\cdot)(1, y_{i1}, \ldots, y_{ij}). \end{aligned}$$

The following example shows that we cannot expect the stronger result of faithfulness on the category of all formal schemes on truncated power series algebras, as was obtained in [7, "the curves lemma"].

Let k be a field, $A = k[[x, y]]/(x^2, y^2)$ and $B = k[[z]]/(z^2)$. Furthermore define $f, g\colon B \to A$ by $f(z) = 0$ and $g(z) = xy$. The question is: is there a morphism $h\colon A \to k[[t]]/(t^s)$ with $hg \neq hf$? Let h be such a morphism. Then $h(x) = u$, $h(y) = v$ in $k[[t]]/(t^s)$ with $u^2 = 0 = v^2$ and $uv \neq 0$. Now in $k[[t]]/(t^s)$ we have $u = t^i \cdot u_1$, $v = t^j \cdot v_1$ with units u_1 and v_1. We must have $2i \geqslant s$, $2j \geqslant s$ and $i + j < s$. This is impossible. So $C_s(f) = C_s(g)$ for all s.

REMARK. Again, one could deduce Theorem 7 from Theorem 3.5 of [5 bis] for any formal group G whose bialgebra A^0 admits suitable generators, because if G is generated by curves (condition (b), [loc cit]), group maps will certainly be determined by curves.

Now for $1 \leqslant i + 1 \leqslant \infty$ and $j < i + 1$, denote by P_i the commutative (resp., noncommutative) polynomial algebra $P_i = K[x_1, x_2, \ldots, x_j, \ldots]$ (resp., $K\langle x_1, x_2, \ldots, x_j, \ldots\rangle$) with $(1, x_1, x_2, \ldots)$ a sequence of divided powers and with antipode S defined inductively by $\sum_{i+j=k} S(x_i)x_j = \delta_{k0}$ for $k \geqslant 0$ (here $x_0 = 1$), and $\varepsilon(x_j) = \delta_{j0}$. It is straightforward to verify that the functors W_i (resp., Z_i) corresponding to these algebras are flat formal groups. Z_i is the group $Z(i, K)$ of [5, Lemma 1.1] where most of the details are found. W_∞ is the group W_{K^+} of generalized Witt vectors [2], [3]. The curve functors C_i on the category of flat formal commutative groups (resp., all flat formal groups) are represented by W_i (resp., Z_i).

In the category of flat formal groups the finite coproduct $Z_{i_1} \amalg Z_{i_2} \amalg \cdots \amalg Z_{i_n}$ exists. In the category of flat commutative formal groups, the finite coproduct $W_{i_1} \amalg \cdots \amalg W_{i_n}$ exists and is isomorphic to the product $W_{i_1} \times \cdots \times W_{i_n}$. The bialgebra of $W_i \amalg W_j$ is

$$K\langle x_{11}, x_{12}, \ldots, x_{1i}, x_{21}, \ldots, x_{2j}\rangle.$$

Now suppose $A^\cdot$ is a formal group admitting truncation type $(s_1, \ldots, s_n)$.

Then we have

THEOREM 8. *There is an epimorphism of formal groups* $\zeta\colon Z_{s_1} \amalg \cdots \amalg Z_{s_n} \to A^{\cdot}$. *If* $A^{\cdot}$ *is commutative* ζ *factors through* $W_{s_1} \times \cdots \times W_{s_n}$.

PROOF. It suffices to show the corresponding property in Coalg_{pf}. Let $B = K\langle x_{11}, \ldots, x_{1s_1}, \ldots, x_{ns_n}\rangle$ be the bialgebra of the given coproduct. The map $x_{jr} \to y_{jr}$ induces a Hopf-algebra surjection $B \to A^0$, where the $y_{jr} \in A^0$ are those defined in §1. This is a coalgebra map because for each j the y_{jr} form a sequence of divided powers over y_{j1} and by Theorem 5 these y_{jr}'s generate A^0 as an algebra. The commutative claim is clear since $A^{\cdot}$ is commutative if and only if A^0 is a commutative algebra, and

$$B\left(W_{s_1} \times \cdots \times W_{s_n}\right) = K\left[x_{11}, \ldots, x_{1s_1}, \ldots, x_{ns_n}\right].$$

REMARK. Something approaching the strength of admitting a truncation type is necessary for Theorem 8. As remarked in [5 bis, p. 24] one can construct examples, even over fields, of finite formal groups not generated by curves (equivalently, for which Theorem 8 fails): Let k be nonperfect of characteristic p and let α in k/p^p, and $A = k[x, y]/(x^p - \alpha y^p, x^{p^2})$, with x and y primitive. For perfect k, however, being generated by a finite set of finite curves is equivalent to A being finite and local, cf. [6, Exposé VII B, Theorem 5.2].

3. The structure of curves on groups admitting truncation type. In this section we will sketch a "Dieudonné theory" in the spirit of [2] and [3]. The central idea of this kind of program is to introduce a ring of operators on the curve groups in order to identify, via the curve functor, the formal group category as an ordinary module category. The isomorphism to the module category is usually studied with the aid of a decomposition of curves by the operators. However, we show that the curve functor is, in fact, not full, even when the operators are introduced. Lacking a good description of the "image" of the curve functor, we only sketch the arguments leading to the decomposition, for which we have isolated a strictly Hopf-algebraic criterion (Theorem 9). It seems that being generated by curves is sufficient to bring this criterion about, but we do not know how much more general a result is possible than Ditters' decomposition theorem [5 bis, Corollary 1 to Theorem 6.4].

Suppose $A^{\cdot}$ is a formal group, We have seen that

$$C_i(A^{\cdot}) \simeq \mathrm{Coalg}_{\varepsilon}(Kx_0 \oplus \cdots \oplus Kx_i, A^0) \simeq \text{Hopf-Alg}(K\langle x_1, \ldots, x_i\rangle, A^0)$$

where $\mathrm{Coalg}_{\varepsilon}(Kx_0 \oplus \cdots \oplus Kx_i, -)$ $((x_r)$ divided powers over $x_0)$ denotes the set of coalgebra maps φ with $\varphi(x_0) = 1$ in A^0. From this we can deduce

$$\begin{aligned}\text{Group func}(C_i, C_j) &\cong \text{Hopf-Alg}(K\langle x_1, \ldots, x_{i-1}\rangle, K\langle x_1, \ldots, x_{j-1}\rangle)\\ &\simeq C_i(K\langle x_1, \ldots, x_{j-1}\rangle)\\ &\simeq \text{Coalg}_\varepsilon(Kx_0 \oplus \cdots \oplus Kx_{i-1}, K\langle x_1, \ldots, x_{j-1}\rangle)\\ &\supseteq \text{Coalg}(Kx_0 \oplus \cdots \oplus Kx_{i-1}, Kx_0 \oplus \cdots \oplus Kx_{j-1})\end{aligned}$$

where now the last set refers to coalgebra maps φ with $\varphi(x_0) = x_0$. This set is in turn the same as $\text{Alg}_{pf,\varepsilon}(K[[t]]/(t^j), K[[t]]/(t^i))$ of continuous "local" algebra maps. I.e. those ψ with $\psi(t)$ in $t \cdot K[[t]]/(t^i)$. Identifying such a map with $\psi(t)$ requires us to pick an element in $K[[t]]/(t^i)$ which is nilpotent of degree j. Composition of maps corresponds to substitution of power series. Certain of these choices are of special interest:

(1) For $\lambda \in K$ the map $[\lambda]$: $C_i \to C_i$ is that corresponding to λt in $t \cdot K[[t]]/(t^i)$. If $a^0 = (1, a_1^0, \ldots, a_{i-1}^0)$ is a curve of length $i - 1$ in $A^\cdot$, i.e. a sequence of divided powers in A^0 then

$$[\lambda](a^0) = (1, \lambda a_1^0, \lambda^2 a_2^0, \ldots, \lambda^i a_{i-1}^0).$$

(2) T: $C_i \to C_{i-1}$ is defined to correspond to the polynomial t in $t \cdot K[[t]]/(t^{i-1})$. On a curve it is $T(1, a_1^0, \ldots, a_{i-1}^0) = (1, a_1^0, \ldots, a_{i-2}^0)$.

Thus T^s: $C_i \to C_{i-s}$.

For notational convenience if $z = (1, z_1, z_2, \ldots)$ is an infinite sequence and $v = \infty$, we denote by $T^{v-r}z$ the sequence $(1, z_1, z_2, \ldots, z_r)$.

(3) V_j: $C_i \to C_{ij}$ is defined to correspond to t^j in $t \cdot K[[t]]/(t^{ij})$. It is described by

$$V_j(1, a_1^0, \ldots, a_i^0) = (1, 0, \ldots, 0, a_1^0, 0, \ldots, 0, a_2^0, 0, \ldots, a_{i-1}^0, 0, \ldots, 0)$$

where $j - 1$ zeros lie between each of the a_r^0's.

Now for any Hopf algebra H, the set of *primitive elements* is $P(H) = \{h \in H | \Delta(h) = h \otimes 1 + 1 \otimes h\}$. For any such h the relation $(\varepsilon \otimes \text{id})\Delta = \text{id}$ implies $\varepsilon(h) = 0$. Further note that h is primitive if and only if $(1, h)$ is a sequence of divided powers.

If $(1, 0, \ldots, 0, h_r, h_{r+1}, \ldots)$ is a special sequence of divided powers in H then it is easily seen that h_r is primitive.

Assume h is primitive. We say h has degree at least n if there is a special sequence $(1, h, h_2, \ldots, h_n)$ of divided powers of length n. We will say h has *degree n* if it has degree at least n and cannot sit in any longer sequence in a nontrivial way: more precisely, if there is no special sequence of divided powers $(1, 0, \ldots, 0, h_i, h_{i+1}, \ldots, h_j)$ with $h_i = h$ and $j > (n + 1)i$ (observe that $V_i(1, h_1, \ldots, h_n)$ has length $i(n + 1) - 1)$. We say that h in $P(H)$ has degree ∞ if it lies in an infinite special sequence of divided powers. Note that not every primitive need have a degree as would happen if it could be embedded in arbitrarily long finite sequences but not in any infinite sequence. However we shall see that this cannot happen in the case of interest to us, the bialgebra $B(A^{\cdot}) = A^0$ of a formal group admitting a truncation type.

Assume next that all primitives have a degree and that for each u in $P(H)$ we have chosen a sequence $t(u) = (1, u, u_2, \ldots, u_{\deg u})$. Now suppose $z = (1, z_1, z_2, \ldots, z_r)$ is a sequence of length r and let

$$t(z_1) = \left(1, z_1, z_2', \ldots, z'_{\deg z_1}\right)$$

be a sequence of length $\deg z_1$. Then $T^{\deg z_1 - r}(t(z_1))$ is a sequence of length r still with primitive z_1 and $z \cdot T^{\deg z_1 - r}(t(z_1))^{-1}$ is a sequence of length r of the form $(1, 0, z_2'', \ldots, z_r'')$. Here multiplication and $(\ )^{-1}$ are that of special sequences of divided powers, i.e. curves, and, by definition, multiplication of curves induces addition in the primitive component (i.e. the first nonzero element after the leading 1) and inversion induces subtraction (the identity of $C_r(A^{\cdot})$ is $(1, 0, 0, \ldots, 0)$). Now compute

$$(1, 0, z_2'', \ldots, z_r'') \cdot \left(T^{2\deg z_2'' - r} V_2\left(t(z_2'')\right)\right)^{-1}$$

to get $(1, 0, 0, z_3^{(3)}, \ldots, z_r^{(3)})$. Continuing inductively we find primitives $z_2'', z_3^{(3)}, \ldots, z_n^{(n-1)}$ uniquely determined by z (and by the original choice of sequences over each primitive) such that

$$z \cdot T^{\deg z_1 - r}\left(t(z_1)^{-1}\right) \cdot T^{2\deg z_2'' - r} V_2\left(t(z_2'')\right)^{-1} \cdot T^{3\deg z_3^{(3)} - r} V_3\left(t\left(z_3^{(3)}\right)^{-1}\right) \cdots$$
$$= (1, 0, 0, \ldots, 0).$$

Thus we can represent z uniquely as

$$z = \cdots T^{2\deg z_2'' - r} V_2\left(t(z_2'')\right) \cdot T^{\deg z_1 - r} t(z_1).$$

In the infinite curve case truncation is unnecessary but some topological care is needed: Let z be an infinite special sequence of divided powers in a Hopf algebra H whose underlying coalgebra is in Coalg_{pf}. Then

$$C_\infty(H^{*\cdot}) = \text{proj lim } C_i(H^{*\cdot})$$

carries the limit topology (letting each $C_i(H^{*\cdot})$ bc discrete) and the same argument shows z is a convergent product $\prod_{n=1}^{\infty} V_n(t(z_n^{(n)}))$. We summarize this discussion as

THEOREM 9. *Let H be a Hopf algebra such that H^* is in Alg_{pf} and such that every primitive in H has a degree: then for $r < \infty$, any z in $C_{r+1}(H^{*\cdot})$ can be represented as*

$$z = \prod_{n=1}^{r} T^{n \deg(z_n^{(n)}) - r} V_n\left(t\left(z_n^{(n)}\right)\right)$$

and $z \in C_\infty(H^{*\cdot})$ as

$$z = \prod_{n=1}^{\infty} V_n\left(t\left(z_n^{(n)}\right)\right)$$

where the $z_n^{(n)}$ are uniquely determined primitives in H.

Suppose henceforth that A is of truncation type $(s_i, \dots, s_n)$ and that $A^{\cdot}$ is a formal group. Let $e_{j_1, \dots, j_n}$ and y_{ij} be as in §1. Then we recall that Lemma 6 asserts that $(1, y_{i1}, y_{i2}, \dots, y_{is_i - 1})$ is a (special) sequence of divided powers in A^0.

According to Theorem 5, (certain) monomials in the y_{ij} are a basis of A^0 over k. Now if K is a field of char 0 and y is primitive, then the elements $y^j/j!$ form a sequence of divided powers over y. Thus to say that monomials in the primitives span A^0 is the same as to say monomials in the elements of these sequences span. The former is akin to our Theorem 5, the latter to the classical Birkhoff-Witt Theorem when A^0 is a universal enveloping algebra. Now an equivalent statement to (part of) this classical result is the statement that the primitive elements of universal enveloping algebra $\mathfrak{U}(l)$ of a Lie algebra l comprise exactly l. In our case we have

Theorem 10. *$P(A^0)$ is free on $\{y_{11}, y_{21}, \dots, y_{n1}\}$ and every primitive element has a degree. In particular, curves may be decomposed as in Theorem* 9.

Indication of Proof. The first claim comes easily from Theorem 5. For the second, we describe a canonical sequence of maximal length first over $z = \lambda y_{j1}$. If $\lambda^{s_j} \neq 0$, set

$$\tau(z) = \left(1, \lambda y_{j1}, \lambda^2 y_{j2}, \dots, \lambda^{s_j - 1} y_{js_j - 1}\right).$$

If, however, $\lambda^{s_j} = 0$ then set

$$\tau(z) = \left(1, \lambda y_{j1}, \lambda^2 y_{j2}, \dots, \lambda^{s_j - 1} y_{js_j - 1}, 0, 0, \dots\right).$$

It turns out the degree of $\tau(z)$ is $s_j - 1$ if $\lambda^{s_j} = 0$ and infinite otherwise. To define $\tau(z) = \tau(\Sigma_j \lambda_j y_{j1})$, apply this procedure to each term, truncate to the minimum length, v, and multiply the results in the group $C_{v+1}(A^0)$. The resulting curve begins with z and z cannot sit in a longer curve nontrivially, i.e., $\tau(z)$ has degree v. This is deduced from the following technical observation: Let A have truncation type $(s_1, s_2, \dots, s_n)$ and let $z = (1, 0, \dots, 0, z_i, z_{i+1}, \dots, z_r)$ be a sequence of divided powers with primitive $z_i = \lambda_1 y_{11} + \cdots + \lambda_n y_{n1}$; then whenever $r \geqslant i \cdot s_j$, we get $\lambda_j^{s_j} = 0$.

Corollary 11. *The epimorphism ζ: $W_{s_1} \times \cdots \times W_{s_n} \to A^{\cdot}$ (resp. ζ: $Z_{s_1} \amalg \dots \amalg Z_{s_n} \to A^{\cdot}$) of Theorem* 8 *induces surjections*

$$C_i(\zeta)\colon C_i\left(W_{s_1} \times \cdots \times W_{s_n}\right) \to C_i(A^{\cdot})$$

$$\left(\textit{resp. } C_i(\zeta)\colon C_i\left(Z_{s_1} \amalg \dots \amalg Z_{s_n}\right) \to C_i(A^{\cdot})\right)$$

for every $i = 1, 2, \dots, \infty$.

Proof. Suppose $i \leqslant$ length $(1, y_{j1}, \dots)$. In the entire proof we will suppose always that sequences are already truncated to length i. This will result in an abuse of notation but increased readability.

In the notation of Theorem 8, we have

$$(1, y_{j1}, y_{j2}, \ldots) = C_{i+1}(\zeta)(1, x_{j1}, x_{j2}, \ldots).$$

More generally,

$$\tau(\lambda_j y_{j1}) = C_{i+1}(\zeta)(\sigma(\lambda_j x_{j1}))$$

where $\sigma(\lambda_j x_{j1}) = (1, \lambda_j x_{j1}, \lambda_j^2 x_{j2}, \ldots)$ and

$$\tau(\lambda_1 y_{11} + \cdots + \lambda_n y_{n1}) = C_{i+1}(\zeta)[\sigma(\lambda_1 x_{11}) \ldots \sigma(\lambda_n x_{n1})]$$

provided $i < \operatorname{degree}(\lambda_1 y_{11} + \cdots + \lambda_n y_{n1})$. This is the canonical (i.e. that constructed in Theorem 10) sequence of maximal length over any given primitive is in the image of $C_{i+1}(\zeta)$. But according to Theorem 9, these generate C_{i+1}, since the operators T and V_n commute with the $C_i(\zeta)$. This Corollary together with Theorem 9 gives a complete description of all curves of a formal group over a truncated power series algebra.

The counterexample. Now we are ready to discuss if the functor from formal groups to curve groups is full. In [7] a consequence of the faithfulness on the category of all formal schemes on power series rings ("the curves lemma") implies the fullness on formal groups [7, III. 8.4]. The curves lemma does not hold in our context, nor is the functor from formal groups to all curves full. The following is a counterexample even in the commutative case:

Let k be a field of characteristic 2. Let $\alpha_2 = A^{\cdot}$ and $\mu_2 = B^{\cdot}$ with $A = k[[x]]/(x^2)$ and $B = k[[y]]/(y^2)$ with $\Delta(x) = x \otimes 1 + 1 \otimes x$ and $\Delta(y) = y \otimes 1 + 1 \otimes y + y \otimes y$. It is easy to show that $P(A^0) = kt$ with $t^2 = 0$ and $P(B^0) = kt$ with $t^2 = t$. Now let $(1, z_1, \ldots, z_n)$ be a sequence of divided powers in A^0 or B^0. Then the nonzero entries are linearly independent; hence $(1, z_1, \ldots, z_n) = (1, 0, \ldots, 0, \lambda t)$ using the technical observation in Theorem 10. Thus the multiplication of curves in $C_{n+1}(\alpha_2)$ and $C_{n+1}(\mu_2)$ is just addition of primitives. The operators T and V_n also operate in the same way on the curve groups of α_2 and μ_2. Hence the curve groups with all their operators on α_2 and μ_2 are isomorphic, but there is only the zero homomorphism from α_2 to μ_2, which clearly cannot induce this isomorphism.

4. The Lie algebra of a curve group.

Let $A^{\cdot}$ be a formal group and $C_3(A^{\cdot})$ be the set of curves of length 2 in $A^{\cdot}$. Let $z = (1, z_1, z_2)$ be such a curve. The inverse of z has the components $(1, -z_1, z_1^2 - z_2)$ as can be easily checked by computing zz^{-1}. Now let $y = (1, y_1, y_2)$ be another curve. Then $zyz^{-1}y^{-1} = (1, 0, [z_1, y_1])$ with $[z_1, y_1] = z_1 y_1 - y_1 z_1$ in A^0. Hence from $C_3(A^{\cdot})$ we can recover the Lie multiplication of those primitive elements of A^0 which have at least degree 2.

PROPOSITION 12. *If the truncation type* $(s_1, \dots, s_n)$ *of* A *is such that* $s_i > 2$ *for all* i, *then the Lie algebra multiplication of* Lie(A) *can be recovered from* $C_3(A^{\cdot})$.

PROOF. We only have to prove that every primitive element of A^0 has at least degree 2. But the canonical curves $(1, y_{i1}, \dots)$ for $i = 1, \dots, n$ have at least length 2; hence every "linear" combination $[\lambda](y_{1\tau}) \cdot \cdots \cdot [\lambda_n](y_{n\tau})$ does, and by Theorem 10 every primitive element has the form $\lambda_1 y_{11} + \cdots + \lambda_n y_{n1}$.

A similar argument gives also the pth-power map for the Lie algebra if the characteristic of K is a prime p. Let $(1, z_1, \dots, z_p)$ be in $C_{p+1}(A^{\cdot})$; then the sequence of divided powers $(1, z_1, \dots, z_p)^p$ has nth term $\Sigma_{i_1 + \cdots + i_p = n} z_{i_n} \cdot \cdots \cdot z_{i_p}$. Now it is a simple combinatorial problem to show that $(1, z_1, \dots, z_p)^p = (1, 0, \dots, 0, z_1^p)$. It is well known that the pth-power map for the Lie algebra of $A^{\cdot}$ coincides with the pth-power map in A^0. Hence we get.

PROPOSITION 13. *If the truncation type* $(s_1, \dots, s_n)$ *of* A *is such that* $s_i > p$ *for all* i, *then the restricted Lie algebra of* $A^{\cdot}$ *can be recovered from* $C_{p+1}(a^{\cdot})$.

BIBLIOGRAPHY

1. P. Cartier, *Hyperalgèbres et groupes de Lie formels*, Séminaire "Sophus Lie" de la Faculté des Sciences de Paris, 1955–1956, Secrétariat Mathématique, Paris, 1957, 61 pp. MR **19**, 431.

2. ______, *Modules associés à un groupe formel commutatif. Courbes typiques*, C. R. Acad. Sci. Paris Sér. A–B **265** (1967), A129–A132. MR **36** #1449.

3. ______, *Groupes formels associés aux anneaux de Witt généralisés*, C. R. Acad. Sci. Paris Sér A–B **265** (1967), A49–A52. MR **36** #1448.

4. M. Demazure, *Lectures on p-divisible groups*, Lecture Notes in Math., vol. 302, Springer-Verlag, Berlin and New York, 1972. MR **49** #9000.

5. E. J. Ditters, *Curves and formal (co) groups*, Invent.Math. **17** (1972), 1–20. MR **47** #8554.

5 bis. ______, *Groupes formels*, Univ. Paris XI, Orsay, Nos. 149–175, 42 cours 1973/74.

6. P. Gabriel, *Schémas en groupes*. I (SGA 3) 1962/64, Lecture Notes in Math., vol. 151, Springer-Verlag, Berlin and New York, 1970.

7. M. Lazard, *Commutative formal groups*, Lecture Notes in Math., vol. 443, Springer, Berlin and New York, 1975.

8. R. Morris and B. Pareigis, *Formal groups over discrete rings*, Bull. Amer. Math. Soc. **79** (1973), 449–453. MR **48** #302.

9. ______, *Formal groups and Hopf algebras over discrete rings*, Trans. Amer. Math. Soc. **197** (1974), 113–129. MR **51** #3181.

10. F. Oort, *Dieudonné modules of finite local group schemes*, Indag. Math. **36** (1974).

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF OKLAHOMA, NORMAN, OKLAHOMA 73019

MATHEMATISCHES INSTITUT, UNIVERSITÄT MÜNCHEN, MÜNCHEN, FEDERAL REPUBLIC OF GERMANY