A REALIZATION OF THE ADDITIVE WITT GROUP

KENNETH NEWMAN¹ AND MOSS E. SWEEDLER²

ABSTRACT. For each prime p we construct in several ways a canonical sequence of divided powers and give an elementary proof that its coefficients lie $\mathbf{Z}_{(p)}$.

Introduction. Let H be a commutative, cocommutative irreducible Hopf algebra over $\mathbf{Q}$, the rationals. A sequence of elements in H , ${}^0x = 1$, 1x , ${}^2x, \dots$, is called a sequence of divided powers (SDP) if, for all n , $\Delta^n x = \sum_{i=0}^n {}^ix \otimes {}^{n-i}x$. In this paper we consider SDP's such that for a fixed prime p , each p^n th divided power is algebraically independent of the previous terms in the sequence, while the other divided powers are algebraically dependent on the previous terms. Using the exponential Taylor series we give several realizations of this sequence (including a rather complicated formula) and also give an elementary proof that the coefficients of the polynomials representing the elements in the sequence lie in $\mathbf{Z}_{(p)}$. (This was previously shown in [3].)

For convenience, we will call a power series in T , $1 + \sum_{i=1}^{\infty} x_i T^i$, an SDP if $1, x_1, x_2, \dots$ is an SDP.

Also we will denote the primitives of H , $P(H)$.

LEMMA 1 [1, PROPOSITION 2]. *The formal power series in T , $\exp(\sum_{i=1}^{\infty} x_i T^i)$ is an SDP if and only if each x_i is primitive.*

COROLLARY 2 [1, COROLLARY 3]. *$1 + \sum x_i T^i$ is an SDP if and only if the coefficient of T^i in $\log(1 + \sum_{i=1}^{\infty} x_i T^i)$ is a primitive for all i .*

LEMMA 3 [1, THEOREM 4]. *Give $H_n = \mathbf{Q}[X_1, X_2, \dots, X_n]$ a graded Hopf algebra structure by defining ΔX_i so that $1, X_1, X_2, \dots, X_n$ is an SDP and by letting $\deg X_i = i$. Then there exists a homogeneous extension to $1, X_1, X_2, \dots, X_n$. We denote such an extension P_{n+1} .*

LEMMA 4. *Assume that $J = \mathbf{Q}[X_1, X_2, \dots, X_m]$ is a graded irreducible Hopf algebra and contains an SDP $1, {}^1x, {}^2x, \dots, {}^nx$ such that*

- (1) *ix is homogeneous of degree i for all i ;*

Received by the editors June 13, 1978.

AMS (MOS) subject classifications (1970). Primary 16A24.

Key words and phrases. Sequence of divided power, Witt vectors, Artin-Hasse exponential.

¹This research was partially supported by National Science Foundation Grant no. NSF 76-066 38A01.

²This research was partially supported by National Science Foundation Grant no. NSF MCS 73-04876.

$$(2) {}^1x = X_1;$$

$$(3) \text{ for } 2 \leq i \leq m, \exists k_i \geq 2 \text{ such that } X_i = {}^{k_i}x \text{ and } i < j \Rightarrow k_i < k_j.$$

Then there exists a unique homogeneous extension ${}^{n+1}x$ to $1, {}^1x, {}^2x, \dots, {}^nx$.

PROOF. Existence. By Lemma 3, H_n contains a homogeneous extension P_{n+1} to $1, X_1, X_2, \dots, X_n$. Now $\varphi: H_n \rightarrow J$ via $X_i \rightarrow {}^i x$ will be a graded Hopf algebra map and $\varphi(P_{n+1})$ will be the desired extension.

Uniqueness. A second homogeneous extension would differ from the first by a homogeneous primitive d of degree $n+1$. We show $d = 0$ as follows: by [4, Theorem 13.0.1, p. 274] over a field of characteristic 0 any cocommutative irreducible Hopf algebra is the universal enveloping algebra of the Lie algebra of primitives and, since J is also commutative, J is generated by any linear basis of $P(J)$ as a polynomial ring, i.e., if $\{d_\alpha\}$ is a basis for $P(J)$ then $\{d_\alpha\}$ is an algebraically independent generating set in J . If $0 \neq d$, then it may be included in a basis for $P(J)$ and hence in an algebraically independent generating set of J . On the other hand, an element may be included in an algebraically independent generating set only if it is of the form:

$$\gamma + \sum_{i=1}^m \lambda_i X_i + R(X_1, X_2, \dots, X_m) \quad (\dagger)$$

with $\gamma, \lambda_1, \dots, \lambda_m \in \mathbf{Q}$, at least one λ_i not zero, and R in the square of the ideal generated by $X_1, X_2, \dots, X_m$. But an element of the form $(\dagger)$ cannot be homogeneous of degree greater than n since $X_i = {}^{k_i}x$ is homogeneous of degree k_i . Thus d which is homogeneous of degree $n+1$ cannot be written in form $(\dagger)$ and must therefore be zero. Q.E.D.

Note that this lemma implies that the extension in Lemma 3 is unique.

We will be especially interested in the situation of the above lemma where for a prime p , $X_i = {}^{p^i}x$, for all $i \geq 0$. (For convenience we will start subscripting the X 's at 0.) Using the above lemma and induction we know that $\exists!$ homogeneous SDP: $1, P_{1,p}, P_{2,p}, \dots$ in $\mathbf{Q}[X_0, X_1, X_2, \dots]$ such that $P_{p^i,p} = X_i$ and $\deg X_i = p^i$.

Another method of constructing this sequence and one leading to a computational realization derives from Lemma 1. Consider

$$\exp(X_0 T + (X_1 - Q_1) T^p + (X_2 - Q_2) T^{p^2} + \dots) \quad (*)$$

where Q_i is the coefficient of T^{p^i} in

$$\exp(X_0 T + (X_1 - Q_1) T^p + \dots + (X_{i-1} - Q_{i-1}) T^{p^{i-1}}).$$

Note that the coefficient of T^{p^i} in $(*)$ is X_i . Further if we inductively define

$$\Delta X_i = \Delta Q_i + 1 \otimes (X_i - Q_i) + (X_i - Q_i) \otimes 1,$$

we have that X_0 and $X_i - Q_i$ are primitive for all i . Thus $(*)$ is an SDP. The uniqueness part of Lemma 4 ensures that this is the same SDP defined above.

A somewhat more "magical" algorithm using the same idea can be stated as follows:

Consider $\exp(X_0 T)$ and replace the coefficient of T^p by X_1 . Take log and discard all T^i with $i > p$. Then all coefficients are primitives and $\exp$ of this will be an SDP. Now replace the coefficient of T^{p^2} with X_2 , take log, discard T^i with $i > p^2$, etc.

In any case, we see from (*) that if we inductively define

$$Q_i = \sum_{m_0 + pm_1 + \dots + p^{i-1}m_{i-1} = p^i} \frac{X_0^{m_0}}{m_0!} \frac{(X_1 - Q_1)^{m_1}}{m_1!} \dots \frac{(X_{i-1} - Q_{i-1})^{m_{i-1}}}{(m_{i-1})!}$$

then

$$P_{n,p} = \sum_{m_0 + pm_1 + \dots + p^i m_i = n} \frac{X_0^{m_0}}{m_0!} \frac{(X_1 - Q_1)^{m_1}}{m_1!} \dots \frac{(X_i - Q_i)^{m_i}}{m_i!}$$

where p^i is the largest power of p less than or equal to n .

For example if $n < p$ then $P_{n,p} = x_0^n/n!$. If $p < n < p^2$ then

$$P_{n,p} = \sum_{m_0 + pm_1 = n} \frac{X_0^{m_0}}{m_0!} \frac{(X_1 - X_0^p/p!)^{m_1}}{m_1!}$$

since $Q_1 = x_0^p/p!$.

What is remarkable about this sequence is that the coefficients lie in $\mathbf{Z}_{(p)}$, i.e., the denominators are relatively prime to p and therefore one can use the $P_{n,p}$ to construct SDP's over fields of char p . We give an elementary proof using Witt vectors and the Artin-Hasse exponential.

In $\mathbf{Q}[Y_0, Y_1, \dots]$ let $\phi_n = Y_0^{p^n} + pY_1^{p^{n-1}} + \dots + p^n Y_n$. If we let each ϕ_n be primitive then the ΔY_i are defined inductively.

LEMMA 5 [2, Chapter V, §4, no° 4.1, p. 617]. *Let the coefficient of T^i in*

$$\exp\left(-\phi_0 T - \phi_1 \frac{T^p}{p} - \phi_2 \frac{T^{p^2}}{p^2} - \dots\right) \quad (**)$$

be E_i . Then, $E_i \in \mathbf{Z}_{(p)}[Y_0, Y_1, \dots]$ for all i .

Now since $\phi_0, \phi_1, \dots$ are primitives (**) is an SDP with coefficients in $\mathbf{Z}_{(p)}$. Further, since $E_{p^n} = Y_n + (\text{polynomial in } Y_0, Y_1, \dots, Y_{n-1})$, the coefficients of the T^i can be expressed in terms of the E_{p^n} . As the substitution process takes place over $\mathbf{Z}_{(p)}$, we have just shown that there is an SDP with coefficients in $\mathbf{Z}_{(p)}[E_1, E_p, E_{p^2}, \dots]$ such that the p^n th term is E_{p^n} . Using the uniqueness part of Lemma 4 we have (with X_i replacing E_{p^i}):

THEOREM 6. *The coefficients of $P_{n,p}$ lie in $\mathbf{Z}_{(p)}$ for all n .*

BIBLIOGRAPHY

1. A. Berkson and K. Newman, *Constructing sequences of divided powers. II*, Proc. Amer. Math. Soc. **72** (1978), 11–15.
2. M. Demazure and P. Gabriel, *Groupes algébriques*, Tome 1, North-Holland, Amsterdam, 1970.
3. K. Newman, *Constructing sequences of divided powers*, Proc. Amer. Math. Soc. **31** (1972), 32–38.
4. M. E. Sweedler, *Hopf algebras*, Benjamin, New York, 1969.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT CHICAGO CIRCLE, CHICAGO, ILLINOIS 60680

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MASSACHUSETTS, BOSTON, MASSACHUSETTS 02125 (Current address of Kenneth Newman)

DEPARTMENT OF MATHEMATICS, CORNELL UNIVERSITY, ITHACA, NEW YORK 14853 (Current address of M. E. Sweedler)