

*Pacific
Journal of
Mathematics*

THE HOPF ALGEBRA OF A UNISERIAL GROUP

ALAN KOCH

Volume 215 No. 2

June 2004

THE HOPF ALGEBRA OF A UNISERIAL GROUP

ALAN KOCH

We give a Dieudonné module description for the finite commutative infinitesimal unipotent group schemes over a perfect field of prime characteristic. Witt vector addition is used to describe the algebra and coalgebra structures of the representing Hopf algebra of a uniserial group.

1. Introduction

Let k be an algebraically closed field of characteristic $p > 0$. The purpose of this paper is to describe the Hopf algebra of a finite commutative infinitesimal unipotent k -group scheme which is uniserial, i.e., which has a unique composition series. As there is only one simple finite commutative infinitesimal unipotent group scheme (namely $\alpha_p := \ker \{F : \mathbb{G}_a \rightarrow \mathbb{G}_a\}$, with \mathbb{G}_a being the additive group scheme and F the Frobenius map), composition series on this class of group schemes are a bit easier to study than for arbitrary group schemes. A certain class of uniserial groups, namely the V -uniserial groups, are important in studying representation theory: A finite connected k -group scheme G has finite representation type if and only if the quotient $G/M(G)$, where $M(G)$ is the multiplicative center of G , is a semidirect product of a V -uniserial unipotent group U together with a group of type μ_{p^n} [FV, 2.7].

In [FRV], the authors introduce Dieudonné modules to classify the V -uniserial unipotent groups in an effort to describe all groups of finite representation type. It is shown that the (isomorphism classes of) uniserial groups follow one of six different “types”, three of which are dual to the other three.

Here, we will also use classical Dieudonné module theory to describe uniserial groups, but we will reduce the number of types needed in the description. Surprisingly, there is an easy way to write the isomorphism classes of uniserial groups in terms of Dieudonné modules: They all fit into one of two types, and furthermore the types are dual to each other. Since any representation-finite local algebra is of the form $k[t]/(t^m)$, by [FV, 2.7 and 3.1] we have that $G = \text{Spec}(H)$ is V -uniserial if and only if $H^* = \text{Hom}(H, k)$ is monogenic (i.e., generated as a k -algebra by a single element), and by duality G is F -uniserial if and only if H is monogenic. Using the classification

found in [K2], this enables us to quickly describe all uniserial groups in terms of their Dieudonné modules.

In [FRV, 5.1], most of the attention is focused on the classification of V -uniserial groups due to their relationship with representation theory. A group is V -uniserial if and only if the dual to the representing algebra is monogenic. We will look primarily at F -uniserial groups due to the simple structure of their representing Hopf algebras. Duality will give us the results for V -uniserial groups. We will explicitly show how our classification is equivalent to the Farnsteiner–Röhrle–Voigt classification in the third section.

While the representation-theoretic applications appear to be most common when k is algebraically closed, in the final section we extend our results to the case where k is a perfect (not necessarily algebraically closed) field of characteristic p . In this case, it is still true that $G = \text{Spec}(H)$ is uniserial if and only if either H or H^* is monogenic, however there are usually many more isomorphism classes of monogenic Hopf algebras than when k is algebraically closed. For the case where k is finite we provide a formula for the number of (isomorphism classes of) uniserial groups of order p^n for some n .

Throughout this paper, all groups are commutative, finite, connected, and unipotent. Until the final section, k is an algebraically closed field of positive characteristic p .

2. Uniserial groups and their Dieudonné modules

Let $W = W(k)$ be the ring of Witt vectors with coefficients in k . Following the notation in [O] we let E be the non-commutative polynomial ring $E = W[F, V]$ with relations $FV = VF = p$, $Fw = w^\sigma F$, and $wV = Vw^\sigma$, where σ is the Frobenius map on W . There is an antiequivalence D^* between finite connected unipotent commutative group schemes and finite length E -modules killed by a power of F and V . The correspondence is given by

$$D^*(G) = \text{Hom}(G, C)$$

where C is the ring of Witt covectors as described in [F1, p. 1273]. We will use the term *Dieudonné module* to indicate a finite length E -module killed by a power of F and V . There are other definitions of Dieudonné module which encompass a larger variety of group schemes, for example in [F1] and [F2] a Dieudonné module theory is constructed that can be used to describe formal groups as well as non-connected, non-unipotent group schemes. However, our definition is all that is needed for the results to follow.

The Cartier dual of an infinitesimal unipotent group scheme G , given by $G^* = \text{Hom}(G, \mathbb{G}_m)$ (where \mathbb{G}_m is the multiplicative group scheme), is also infinitesimal and unipotent. In terms of Dieudonné modules, $D^*(G^*)$ is simply the module $D^*(G)$ with the roles of F and V interchanged [DG, V, 4, 5.6].

Of particular interest to us will be Dieudonné modules that are cyclic, i.e., are of the form E/I for some ideal $I \subset E$. Each of the uniserial groups will be what is called a *Witt subgroup*, that is, a subgroup of a group W_n of Witt vectors of length n for some n . The antiequivalence D^* restricts to a correspondence between Witt subgroups and cyclic Dieudonné modules [K1, 1.2].

Recall that a group scheme G is uniserial if it has a unique composition series. Additionally, there are the notions of F -uniserial and V -uniserial. The group scheme G is F -uniserial if the kernel of the Frobenius map $F : G \rightarrow G^{(p)}$ is simple, i.e., if $\ker F \cong \alpha_p$. Likewise, G is V -uniserial if the cokernel of the Verschiebung $V : G^{(p)} \rightarrow G$ is simple. A group scheme G is uniserial if and only if it is either F -uniserial or V -uniserial [FRV, Sec. 1.2].

A Dieudonné module M is called F -uniserial if $\text{coker } F$ is simple as a Dieudonné module, i.e., if $\text{coker } F \cong E/E(F, V)$. Letting n be the smallest positive integer so that $F^n M = 0$, this gives rise to a composition series

$$0 = F^n M \subset F^{n-1} M \subset \dots \subset F^2 M \subset FM \subset M$$

which is the only composition series for M , hence an F -uniserial module is necessarily a uniserial module (that is it has a unique composition series). Indeed, suppose M is a nonsimple uniserial module with composition series

$$0 = M_0 \subset M_1 \subset M_2 \subset \dots \subset M_{n-1} \subset M_n = M.$$

Observe that F acts trivially on $M_{i+1}/M_i \cong k$ and hence $FM_{i+1} \subset M_i$. Then we have

$$FM_{i+1} \subset M_i \subset M_{i+1}$$

with $M_i \neq M_{i+1}$. Since F induces a composition series on M_{i+1} it follows that $FM_{i+1} = M_i$.

Similarly, M is V -uniserial if $\ker V \cong E/E(F, V)$, that is we have that

$$0 \subset V^{n-1} M \dots \subset V^2 M \subset VM \subset M$$

is a composition series, where $V^{n-1} M \neq 0$ and $V^n M = 0$. By an argument similar to the one above a V -uniserial module is also uniserial. Conversely, it is straightforward to show that any uniserial Dieudonné module is either F -uniserial or V -uniserial.

Using the definitions of uniserial above it follows that G is F -uniserial (resp. V -uniserial) if and only if $D^*(G)$ is F -uniserial (resp. V -uniserial) [FRV, 2.5].

We will now give a simple description for the Dieudonné module structure of an F -uniserial group.

Proposition 2.1. *A commutative finite infinitesimal unipotent group scheme G is F -uniserial if and only if*

$$D^*(G) \cong E/E(F^n, F^r - V)$$

for some $1 \leq r \leq n$.

Proof. Of course, $G = \text{Spec } H$ is F -uniserial if and only if H is monogenic. The result follows from [K2, 2.2] taking $\eta = 1$, which can be done since $E/E(F^n, F^r - V) \cong E/E(F^n, F^r - \eta V)$ for all $\eta \in k^\times$ as k is algebraically closed (see [K2, p. 199]). \square

Dualizing switches the roles of F and V , and consequently changes F -uniserial modules to V -uniserial modules, giving us:

Corollary 2.2. *A commutative finite infinitesimal unipotent group scheme G is V -uniserial if and only if*

$$D^*(G) \cong E/E(V^n, V^r - F)$$

for some $1 \leq r \leq n$.

3. Equivalence to the Farnsteiner–Röhrle–Voigt classification

As stated above, the classification of (finite commutative infinitesimal unipotent) uniserial group schemes has also been done by R. Farnsteiner, G. Röhrle and D. Voigt in [FRV] using Dieudonné modules. Here we will show how the two classifications are equivalent.

We start by recalling the Farnsteiner–Röhrle–Voigt classification. For each pair of positive integers d and n , let $M_{n,d}$ be a free $W_n(k)$ -module with basis $\{e_1, \dots, e_d\}$. For $d \geq 2$, let $E_{n,d}$ be the Dieudonné module defined as follows: $E_{n,d} \cong M_{n,d}$ as $W_n(k)$ -modules, with E -module structure given by

$$\begin{aligned} V(e_i) &= e_{i+1} \text{ for } 1 \leq i \leq d - 1, \quad V(e_d) = pe_1 \\ F(e_1) &= e_d, \quad F(e_i) = pe_{i-1} \text{ for } 2 \leq i \leq d. \end{aligned}$$

For $d, n \geq 2$ and $1 \leq j \leq d - 1$ let

$$E_{n,d}^j = E_{n,d}/V^{(n-1)d+j}E_{n,d}.$$

For $d \geq 1$ let E_d be the Dieudonné module defined as follows: $E_d \cong M_{1,d}$ as $W_1(k)$ -modules, with E -module structure given by

$$\begin{aligned} V(e_i) &= e_{i+1} \text{ for } 1 \leq i \leq d - 1, \quad V(e_d) = 0 \\ F(e_i) &= 0 \text{ for } 1 \leq i \leq d. \end{aligned}$$

Then every V -uniserial Dieudonné module is of one of these three forms: $E_{n,d}$, $E_{n,d}^j$, or E_d ; furthermore every module of each of these forms is V -uniserial. Duality, of course, gives us the F -uniserial modules.

Proposition 3.1. *With the notation above we have:*

- 1) $E_{n,d} \cong E/E(V^{nd}, V^{d-1} - F)$
- 2) $E_{n,d}^j \cong E/E(V^{(n-1)d+j}, V^{d-1} - F)$
- 3) $E_d \cong E/E(V^d, F) = E/E(V^d, V^d - F)$.

Thus every V -uniserial group is of the form $E/E(V^s, V^r - F)$. Furthermore, any $M = E/E(F^s, F^r - V)$ is isomorphic to either $E_{n,d}$, $E_{n,d}^j$, or E_d for some choice of j, n , and d .

Proof. We will consider each of these three forms, and show that they are isomorphic to $E/E(V^s, V^r - F)$ for some choice of r and s . Define $\phi : E_{n,d} \rightarrow E/E(V^{nd}, V^{d-1} - F)$ by $\phi(e_i) = F^{i-1}e$ for $1 \leq i \leq d$, where e is the projection of the identity 1 under the canonical projection $E \rightarrow E/E(V^{nd}, V^{d-1} - F)$. As $E/E(V^{nd}, V^{d-1} - F)$ has $W_n(k)$ -basis $\{e, Ve, V^2e, \dots, V^{d-1}e\}$, this is clearly an isomorphism of $W_n(k)$ -modules. In fact, it is quite easy to show that this map also preserves the F and V actions on each module, hence $E_{n,d} \cong E/E(V^{nd}, V^{d-1} - F)$ as Dieudonné modules.

For the second form, the module $E_{n,d}^j$ is given by

$$E_{n,d}^j = E_{n,d}/V^{(n-1)d+j}E_{n,d}$$

where $n, d \geq 2$ and $1 \leq j \leq d - 1$. Identifying $E_{n,d}$ with the isomorphism above gives us

$$E_{n,d}^j \cong E/E(V^{nd}, V^{d-1} - F, V^{(n-1)d+j}) = E/E(V^{(n-1)d+j}, V^{d-1} - F).$$

For the third form, E_d is the k -module with basis $\{e_1, e_2, \dots, e_d\}$ with F acting trivially and $V(e_i) = e_{i+1}$ for $1 \leq i \leq d - 1$ and $V(e_d) = 0$. Here we define $\phi : E_d \rightarrow E/E(V^d, F)$ by $\phi(e_i) = V^{i-1}e$ for $1 \leq i \leq d$. This is an isomorphism of Dieudonné modules.

If we let $s = nd$ and $r = d - 1$ with, then we see that the first form is $E/E(V^s, V^r - F)$. The substitutions of s for $(n - 1)d + j$ and r for $d - 1$ shows that the second class is also $E/E(V^s, V^r - F)$. Finally, setting $s = nd$ and observing $E/E(F^n, V) = E/E(F^n, F^n - V)$ gives the result for the third form. Thus the Dieudonné module for any F -uniserial group is of the form $E/E(F^s, F^r - V)$ for some $1 \leq r \leq s$.

Conversely, suppose $M = E/E(V^s, V^r - F)$. If $s = r$ we get

$$M = E/E(V^s, V^s - F) = E/E(V^s, F) \cong E_s.$$

If $r + 1$ divides s then letting $t = s/(r + 1)$ gives

$$M = E/E(V^{t(r+1)}, V^{(r+1)-1} - F) \cong E_{t,r+1}.$$

If $r + 1$ does not divide s , then writing $s = t(r + 1) + j$ gives

$$M = E/E(V^{t(r+1)+j}, V^{(r+1)-1} - F) \cong E_{t,r+1}^j.$$

Thus every Dieudonné module in our classification also appears somewhere in the Farnsteiner–Röhrle–Voigt classification. \square

Our classification of uniserial Dieudonné modules translates easily to the corresponding uniserial group schemes. The proofs of the statements about the heights will be obvious by the explicit algebra structure for the representing algebras given in the next section.

Corollary 3.2.

- 1) Suppose $D^*(G) = E/E(V^s, V^r - F)$. Then $G = \ker\{V^r - F : W_s \rightarrow W_s\}$. Explicitly, for any k -algebra A we have

$$G(A) = \left\{ (a_0, \dots, a_{s-1}) \in W_s(A) \mid a_j^{p^{\lceil s/r \rceil}} = 0 \text{ for } j < r, \right. \\ \left. a_i = a_{i-r}^p \text{ for all } r \leq i \leq s-1 \right\} \leq W_s(A)$$

when $s > r$, and

$$G(A) = \{(a_0, \dots, a_{s-1}) \in W_s(A) \mid a_i^p = 0 \text{ for } 0 \leq i \leq s-1\} \leq W_s(A).$$

This group scheme has height $\lceil s/r \rceil$, where $\lceil \cdot \rceil$ is the ceiling function.

- 2) If $D^*(G) = E/E(F^s, F^r - V)$, then $G = \ker\{F^r - V : W_m \rightarrow W_m\}$ where $m = \lceil s/r \rceil$. For any k -algebra A we have

$$G(A) = \left\{ (a_0, \dots, a_{s-1}) \in W_m(A) \mid a_i^{p^s} = 0 \text{ for all } i, \right. \\ \left. a_i^{p^r} = a_{i-1} \text{ for } i \neq 0 \right\} \leq W_m(A).$$

This group scheme has height s .

Remark. While the use of cyclic Dieudonné modules unifies the description of the F -uniserial (resp. V -uniserial) modules in a nice way, there are differences in these classes that may be important for various applications. For example, the modules $E_{n,d}$ correspond to the F -uniserial group schemes $G_{n,d}$ that can be lifted to $W(k)$, i.e., for which there is a $W(k)$ -group scheme \hat{G} with $\hat{G} \times_{\text{Spec } W(k)} \text{Spec}(k) \cong G$. The other two classes do not lift to $W(k)$. See [K2, 4.2], where $\alpha = 1$.

4. The Hopf algebra structure

We now use the simplified Dieudonné module structure for uniserial groups to compute their representing Hopf algebras. By insisting on the form used in Proposition 2.1 we can determine the underlying Hopf algebra structure.

Given a finite abelian (that is, commutative and cocommutative) local Hopf algebra H with local dual, we can associate to it a Dieudonné module M by setting $M = D^*(\text{Spec}(H))$. Conversely, given a Dieudonné module M , we can associate to it a k -Hopf algebra $\mathcal{H}(M)$. We will show how this

is done after introducing the notation of Witt polynomials. For any $n > 0$ define a polynomial $w_n(Z_0, Z_1, \dots, Z_n)$ by

$$w_n(Z_0, Z_1, \dots, Z_n) = p^n Z_n + p^{n-1} Z_{n-1}^p + \dots + Z_0^{p^n}.$$

The w_n 's are used to define polynomials $S_0, S_1, \dots; P_0, P_1, \dots$ via

$$\begin{aligned} w_n(S_0, \dots, S_n) &= w_n(X_0, \dots, X_n) + w_n(Y_0, \dots, Y_n) \\ w_n(P_0, \dots, P_n) &= w_n(X_0, \dots, X_n)w_n(Y_0, \dots, Y_n). \end{aligned}$$

For example,

$$\begin{aligned} S_0(X_0, Y_0) &= X_0 + Y_0 \\ S_1((X_0, X_1), (Y_0, Y_1)) &= X_1 + Y_1 - \frac{(X_0 + Y_0)^p - X_0^p - Y_0^p}{p} \\ P_0(X_0, Y_0) &= X_0 Y_0 \\ P_1((X_0, X_1), (Y_0, Y_1)) &= X_0^p Y_1 + X_1 Y_0^p + p X_1 Y_1. \end{aligned}$$

Further properties of these polynomials can be found in [J].

We are now ready to describe $\mathcal{H}(M)$. As a k -algebra, $\mathcal{H}(M) = k[T_x \mid x \in M]$ with the following relations:

$$\begin{aligned} T_{F_x} &= (T_x)^p \\ T_{x+y} &= S_N((T_{V^{N_x}}, T_{V^{N-1_x}}, \dots, T_x); (T_{V^{N_y}}, T_{V^{N-1_y}}, \dots, T_y)) \\ T_{wx} &= P_N((w_0^{p-N}, w_1^{p-N}, \dots, w_N^{p-N}); (T_{V^{N_x}}, T_{V^{N-1_x}}, \dots, T_x)) \end{aligned}$$

where $x, y \in M$, $w = (w_0, w_1, \dots) \in W(k)$, and N is any nonnegative integer so that $V^{N+1}M = 0$. The comultiplication is given by

$$\begin{aligned} \Delta(T_x) &= S_N\left((T_{V^{N_x}} \otimes 1, T_{V^{N-1_x}} \otimes 1, \dots, T_x \otimes 1); \right. \\ &\quad \left. (1 \otimes T_{V^{N_x}}, 1 \otimes T_{V^{N-1_x}}, \dots, 1 \otimes T_x)\right). \end{aligned}$$

These operations make $\mathcal{H}(M)$ into a Hopf algebra, giving a 1-1 correspondence between finite local Hopf algebras with local dual and Dieudonné modules [G, II, Sec. 5].

We can now give an explicit description of the Hopf algebra based on the Dieudonné module. If $M = E/E(F^s, F^r - V)$ then $\mathcal{H}(M) \cong k[t]/(t^{p^s})$ (under this isomorphism $t \in H$ corresponds to T_e where e is the image of $1 \in E$ under the canonical map $E \rightarrow M$) with

$$\Delta(t) = S_N\left(\left(t^{p^{Nr}} \otimes 1, \dots, t^{p^r} \otimes 1, t \otimes 1\right); \left(1 \otimes t^{p^{Nr}}, \dots, 1 \otimes t^{p^r}, 1 \otimes t\right)\right)$$

where $N = \lceil s/r \rceil - 1$. Clearly $\mathcal{H}(E/E(F, V))$ is the representing algebra of α_p . In general the generator t is primitive if and only if $s = r$.

If, on the other hand, $M \cong E/E(V^s, V^r - F)$ we let $\varepsilon_i = \lceil (s + 1 - i)/r \rceil$ for $1 \leq i \leq r - 1$, which gives us

$$\mathcal{H}(M) \cong k[t_1, t_2, \dots, t_{r-1}] / \left(t_1^{p^{\varepsilon_1}}, t_2^{p^{\varepsilon_2}}, \dots, t_{r-1}^{p^{\varepsilon_{r-1}}} \right)$$

with a straightforward but usually messy coalgebra structure: In this case $t_i \in H$ corresponds to $T_{V^{i \cdot 1_M}}$. As a small example, if $s = 3$ and $r = 2$ we have

$$\begin{aligned} \mathcal{H}(M) &\cong k[t_1, t_2]/(t_1^{p^2}, t_2^p) \\ \Delta(t_1) &= S_2((t_1^p \otimes 1, t_2 \otimes 1, t_1 \otimes 1); (1 \otimes t_1^p, 1 \otimes t_2, 1 \otimes t_1)) \\ \Delta(t_2) &= S_2((0, t_1^p \otimes 1, t_2 \otimes 1); (0, 1 \otimes t_1^p, 1 \otimes t_2)) \\ &= S_1((t_1^p \otimes 1, t_2 \otimes 1); (1 \otimes t_1^p, 1 \otimes t_2)). \end{aligned}$$

5. Uniserial groups over perfect fields of characteristic p

Finally, we can quickly extend these results to the case where k is any perfect (but not necessarily algebraically closed) field of characteristic p . The definitions of uniserial, F -uniserial, and V -uniserial are the same as in the algebraically closed case, both when speaking about group schemes as well as Dieudonné modules. In fact, it is still true that $G = \text{Spec } H$ is uniserial if and only if H or H^* is monogenic. By [K2, Th. 2.2], we obtain:

Proposition 5.1. *Let M be an F -uniserial Dieudonné module. Then*

$$M \cong E/E(F^n, F^r - \eta V)$$

where η is a nonzero element of k .

Caveat. The F -uniserial Dieudonné modules are not parameterized by triples (n, r, η) since different choices of η can give isomorphic modules. Adopting the notation $M_{n,r,\eta} = E/E(F^n, F^r - \eta V)$ gives that if $M_{n,r,\eta} \cong M_{n',r',\eta'}$ then $n = n'$ and $r = r'$; [K1, 3.1]. Furthermore, $M_{n,r,\eta} \cong M_{n,r,\eta'}$ if and only if there is an invertible element $a \in k$ such that

$$\left(\frac{\eta}{\eta'} \right)^{p^m} = a^{p^{l+m}-1}$$

[K1, 3.2]. In the case where k is a finite field, it is possible to give a complete list of non-isomorphic F -uniserial Dieudonné modules. The proof follows immediately from the above proposition together with [K2, 3.1].

Corollary 5.2. *Let $k = \mathbf{F}_{p^\ell}$, and let M be an F -uniserial Dieudonné module. Let $k_0 = \mathbf{F}_{p^d}$, where $d = \text{gcd}(\ell, r + 1)$. Fix $\alpha \in k$ such that $k = k_0[\alpha]$. Then*

$$M \cong E/E(F^n, F^r - \alpha^z V) \text{ or } M \cong E/E(F^n, V)$$

where $1 \leq r \leq n - 1$ and $0 \leq z \leq p^d - 2$.

For an explicit description of $\mathcal{H}(M)$ in the former case, as well as a description of the corresponding V -uniserial group scheme, see [K3, Sec. 4].

Finally, the above corollary enables us to provide a formula for the number of uniserial groups of order p^n for some n when k is a finite field.

Corollary 5.3. *The number of isomorphism classes of uniserial group schemes over a field $k = \mathbf{F}_{p^\ell}$ of order p^n for $n > 1$ is given by*

$$2 \left(2 - n - \sum_{r=1}^{n-1} p^{\gcd(\ell, r+1)} \right).$$

Of course, if $n = 1$ then the only isomorphism class is the one containing α_p .

References

- [DG] M. Demazure and P. Gabriel, *Groupes Algébriques*, Masson, Paris, and North-Holland, Amsterdam, 1970, MR 0302656 (46 #1800), Zbl 0203.23401.
- [FRV] R. Farnsteiner, G. Röhrle and D. Voigt, *Infinitesimal unipotent group schemes of complexity 1*, Colloq. Math., **89(2)** (2001), 179–192, MR 1854701 (2002m:14039), Zbl 0989.16013.
- [FV] R. Farnsteiner and D. Voigt, *On cocommutative Hopf algebras of finite representation type*, Adv. Math., **155** (2000), 1–22, MR 1789845 (2001e:16070), Zbl 0981.16030.
- [F1] J.-M. Fontaine, *Sur la construction du module de Dieudonné d'un groupe formel*, C.R. Acad. Sc. Paris, **280** (1975), 1273–1276, MR 0374151 (51 #10351), Zbl 0331.14022.
- [F2] ———, *Groupes finis commutatifs sur les vecteurs de Witt*, C. R. Acad. Sci. Paris, **280** (1975), 1423–1425, MR 0374153 (51 #10353), Zbl 0331.14023.
- [G] A. Grothendieck, *Groupes de Barsotti–Tate et Cristaux de Dieudonné*, Les Presses de L'Université de Montreal, Canada, 1974, MR 0417192 (54 #5250), Zbl 0331.14021.
- [J] N. Jacobson, *Lectures in Abstract Algebra III: Theory of Fields and Galois Theory*, Springer-Verlag, New York, 1964, MR 0172871 (30 #3087), Zbl 0124.27002.
- [K1] A. Koch, *Witt subgroups and Cyclic Dieudonné modules killed by p* , Rocky Mountain J. Math., **31(3)** (2001), 1023–1038, MR 1877332 (2002j:14051).
- [K2] ———, *Monogenic bialgebras over finite fields and rings of Witt vectors*, J. Pure Appl. Algebra, **163** (2001), 193–207, MR 1846661 (2002g:14067), Zbl 0988.16026.
- [K3] ———, *Monogenic Hopf algebras and local Galois module theory*, J. Algebra, **264** (2003), 408–41, MR 1981413 (2004d:16068).
- [O] T. Oda, *The first De Rham cohomology group and Dieudonné modules*, Ann. Sci. Ecole. Norm. Sup., **2** (1969), 63–125, MR 0241435 (39 #2775), Zbl 0175.47901.

Received January 13, 2003.

DEPARTMENT OF MATHEMATICS
AGNES SCOTT COLLEGE
DECATUR, GA 30030
E-mail address: akoch@agnesscott.edu