We shall describe the structure of a certain kind of Hopf algebra over an algebraically closed field \( k \) of characteristic \( p \), namely those Hopf algebras whose coalgebra structure is commutative and which have an antipodal map \( S: H \to H \). (See below for definitions.) Such a Hopf algebra turns out to be of the form \( kG \# U \), the smash product of a group algebra with a Hopf algebra whose coalgebra structure is "like" that of a universal enveloping algebra. If \( p = 0 \) the second factor actually is a universal enveloping algebra.

For \( p > 0 \), we generalize the Birkhoff-Witt theorem by introducing the notion of divided powers. These also play a role in the theory of algebraic groups where certain sequences of divided powers correspond to one parameter subgroups. The divided powers appear in a "Galois Theory" for all finite normal field extensions.

The structure theory of \( \mathbb{Z}_2 \)-graded coanticommutative Hopf algebras is similar, and mentioned below.

Lemma 1, Theorem 1, its generalization to the graded case, and Theorem 2 are unpublished results of B. Kostant, whose guidance we gratefully acknowledge.

1. \( H \) is a cocommutative Hopf algebra with multiplication \( m \), augmentation \( e \) and diagonal \( d \).

**Definition.** An element \( g \in H \) is grouplike if \( dg = g \otimes g \) and \( g \neq 0 \).

**Lemma 1.** The set \( G \) of grouplike elements of \( H \) form a multiplicative semigroup whose elements are linearly independent in \( H \). For each \( g \in G \) there exists a unique maximal coalgebra \( H^o \subset H \) whose only grouplike element is \( g \). \( H \cong \oplus H^o \) as a coalgebra, and \( H^o \cap H^h \subset H^o \).

**Definition.** \( S: H \to H \) is an antipode if

\[
m \circ (I \otimes S) \circ d = e = m \circ (S \otimes I) \circ d.
\]

**Theorem 1.** If \( H \) has an antipode \( G \) is a group and \( S(g) = g^{-1} \). If \( e \) is the identity of \( G \), \( H^e = gH^e = H^e g \), and \( H \cong kG \# H^e \) as a Hopf algebra.

**Remark.** Since \( g^{-1}H^e g = H^e \), the elements of \( G \) act as Hopf algebra automorphisms of \( H^e \) and so we can form the smash product \( kG \# H^e \).

---

1 Part of the research described here was done while the author held an N.S.F. Graduate Fellowship.
(As a coalgebra this is \( kG \otimes H^* \), \((1 \otimes h)(g \otimes 1) = (g \otimes g^{-1}h) \) \( g \subseteq G, h \in H^* \).)

If \( F \) is a cocommutative Hopf algebra with one grouplike element, \( G \) a group of Hopf algebra automorphisms of \( F \) then \( kG \# F \) has a unique antipode.

In the \( Z_2 \)-graded coanticommutative situation, \( G \subseteq H_0, H^* = (H^* \cap H_0) \oplus (H^* \cap H_1) \). If \( H \) has an antipode, \( G \) is a group and \( H \cong kG \# H^* \) as a graded Hopf algebra.

2. We now determine the structure of \( H^* \), i.e. we consider a Hopf algebra \( H \) with one grouplike element.

**Theorem 2.** If \( p = 0 \), \( H \) is the universal enveloping algebra of the Lie algebra \( L \) (under \([ , ]\)), where

\[
L = \{ x \in H \mid dx = x \otimes 1 + 1 \otimes x \}.
\]

**Definition.** For arbitrary \( p \) the elements of \( L \) are called primitive. If \( p > 0 \), \( L \) is a restricted Lie algebra but \( H \) is not necessarily its restricted universal enveloping algebra. However, using the Birkhoff-Witt theorem we can get a form of Theorem 2 which does generalize to \( p > 0 \). Namely it says for \( p = 0 \), \( H = \otimes C \gamma \) as a coalgebra, where \( C \gamma \) is the subspace of \( H \) spanned by the elements \( e^\gamma = e! e ! \) \( e = 0, 1, \cdots \) and \( \{ e^\gamma \} \) is a basis for \( L \). Note that \( C \gamma \) is a coalgebra because \( d^\gamma e^\gamma = \sum e^\gamma \otimes e^\gamma \).

**Definition.** A finite or infinite sequence of elements \( 1 = 0, 1, 2, \cdots \) is called a sequence of divided powers of \( e^\gamma \) if \( d^n = \sum^n i \otimes n^i e^\gamma \).

Given an indeterminate \( x \), let \( H^n_x \) be the Hopf algebra with a basis of indeterminates \( x^i, i = 0, 1, 2, \cdots \), the algebra structure is determined by \( x^i x^j = (x^i + x^j) x^{i+j} \) and the coalgebra structure is determined by \( 0x, 1x, \cdots \), which is a sequence of divided powers of \( x \). If \( p > 0 \) we let \( H^n_x \) be the sub-Hopf algebra spanned by \( 0x, 1x, \cdots, n^{n-1}x \).

Let \( H' = \text{Hom}(H, k) \) have the algebra structure “transpose” to the coalgebra structure of \( H \). Thus for \( a', b' \subseteq H', a' \ast b' \) is the map \((a' \otimes b') \circ d: H \rightarrow k \). \( H' \) is a commutative algebra since \( H \) is cocommutative.

**Theorem 3.** For \( p > 0 \), let \( I^n \subseteq H' \) be the ideal generated by \( \{ a' \in H' \mid a'^n = 0 \} \). If the sequence of ideals \( I^1 \subseteq I^2 \subseteq \cdots \) terminates, then \( H \cong \otimes H^n_x \) as a coalgebra, for some set of elements \( \{ x \} \) and positive integers (or \( \infty \)), \( \{ n_x \} \).

If \( I^1 = 0 \), \( H \cong \otimes H^n_x \) as a coalgebra, where we may choose \( \{ x \} \) to be a basis for \( L \).
If \( I^1 = \{ a' \in H' \mid a'(1) = 0 \} \), then \( H \) is the restricted universal enveloping algebra of \( L \). So \( H \cong \mathbb{H}_L \) as a coalgebra, where \( \{ x \} \) is a basis for \( L \).

The techniques involved in proving Theorem 3 yield information about sequences of divided powers lying above an element of \( L \). For example, \( l \in L \) is orthogonal to \( I^a \) if and only if \( l \) lies in a sequence of divided powers \( 0_l, 1_l, 2_l, \ldots, r\). In the coanticommutative situation the Hopf algebra \( H \) contains a unique maximal sub Hopf algebra \( F \subset H_0 \). Theorem 2 or 3 applies to \( F \). If \( L_0 = L \cap H_0 \) and \( L_1 = L \cap H_1 \) then \( L = L_0 \oplus L_1 \) and \( L \) is a graded Lie algebra. If \( \Lambda L_1 \) is the exterior algebra on \( L_1 \) then \( H \cong F \otimes \Lambda L_1 \) as a coalgebra. If \( p = 0 \), \( H \) is the graded universal enveloping algebra of \( L \).

**BIBLIOGRAPHY**


**Massachusetts Institute of Technology**