COHOMOLOGY OF ALGEBRAS OVER HOPF ALGEBRAS

BY
MOSS EISENBERG SWEEDLER

We present a cohomology theory for algebras which are modules over a given Hopf algebra. The algebras are commutative, the Hopf algebra cocommutative and under the module action the underlying coalgebra of the Hopf algebra "respects" the multiplication and unit in the algebras.

The cohomology is defined by means of an explicit complex. Whenever C is a coalgebra and A an algebra Hom (C, A) has a certain natural algebra structure. The groups in our complex consist of the multiplicative group of invertible elements in Hom (C, A) where C is the underlying coalgebra of the Hopf algebra tensored with itself a number of times. The complex arises as the chain complex associated with a semi-cosimplicial complex whose face operators are induced by maps of the form $\bigotimes^{n+1} H \to \bigotimes^n H$, $h_0 \otimes \cdots \otimes h_n \to h_0 \otimes \cdots \otimes h_i h_{i+1} \otimes \cdots \otimes h_n$. Under Hom $(*, A)$ these maps become coface operators.

Familiar examples of Hopf algebras are the group algebra kG of the group G and the universal enveloping algebra UL of the Lie algebra L. If the commutative algebra A is an admissible kG-module then the Hopf algebra cohomology $H^i(kG, A)$ is canonically isomorphic to $H^i(G, A^r)$, the group cohomology of G in the multiplicative group of invertible elements of A. If A is an admissible UL-module, then for $i > 1$ the Hopf cohomology $H^i(UL, A)$ is canonically isomorphic to $H^i(L, A^+)$, the Lie cohomology of L in the underlying vector space of A. If A has enough nilpotent elements then $H^1(UL, A) \cong H^1(L, A^+)$. All the preceding isomorphisms arise from isomorphisms on the complex level.

We consider relative cohomology and show how an injective (surjective) algebra morphism $A \to \tilde{A}$ can give rise to a long exact cohomology sequence relating $H^*(H, A)$, $H^*(H, \tilde{A})$ and the relative cohomology groups. Using relative cohomology one can completely recover the usual group (Lie) cohomology theory for modules. One considers the module as a trivial algebra and adjoins a unit to form A. The injection of the ground field into A gives rise to relative cohomology groups which are precisely the classical cohomology groups of the group (Lie algebra) with coefficients in the module.

The last comparison is that of $H^*(H, A)$ with the Amitsur cohomology of A. First we show that there always is a natural transformation from the Amitsur cohomology of A to $H^*(H, A)$. We then specialize to the case that A is a finite field extension and give conditions on A and H which imply the natural transformation is an isomorphism. We also show that many field extensions A can

Received by the editors April 11, 1967.

satisfy these conditions; such as, separable normal extensions, purely inseparable extensions which are the tensor product of primitively generated extensions, etc.

The last half of the paper is devoted to studying extensions. An extension of an algebra by a Hopf algebra is itself an algebra and has further properties. We describe equivalence and product of extensions and arrive at the usual result that $H^2(H, A)$ is isomorphic to the group of equivalence classes of extensions. Part of the theory involves the definition of certain algebras which we call crossed products. They generalize existing instances of crossed products.

The extension theory is particularly interesting for field extensions A, where A and H satisfy certain conditions. (These conditions imply that the Amitsur cohomology is isomorphic to $H^*(H, A)$.) When the conditions are satisfied any crossed product of A by H is a central simple algebra (over the ground field) with splitting field A. This leads to an isomorphism between $H^2(H, A)$ and the subgroup of the Brauer group over k consisting of classes split by A. One of the key results needed to give the isomorphism is the existence of "inner" coalgebra actions. This result generalizes known results about inner automorphisms and derivations.

1. **Preliminaries.** All vector spaces are over the ground field k, which has characteristic p. A coalgebra is a vector space C equipped with maps $\Delta: C \to C \otimes C$ and $\varepsilon: C \to k$ satisfying $(I \otimes \Delta)\Delta = (\Delta \otimes I)\Delta$ and $(\varepsilon \otimes I)\Delta = I = (I \otimes \varepsilon)\Delta$. The first identity is called coassociativity, Δ is called the diagonal map and ε is called the counit or augmentation. If C is a coalgebra the structure morphisms pertaining to C may be denoted Δ_C and ε_C, to avoid confusion. Similarly, if A is an algebra the structure morphisms may be denoted $m_A: A \otimes A \to A$ and $\mu_A: k \to A$, $(\lambda \to \lambda 1)$. When no confusion can arise we omit the subscripts C and A.

For $c \in C$ we write $\sum_{(c)} c_{(1)} \otimes c_{(2)}$ to denote $\Delta(c)$, $\sum_{(c)} c_{(1)} \otimes c_{(2)} \otimes c_{(3)}$ to denote $(\Delta \otimes I)\Delta(c)$, etc. An n-linear map $f: C \oplus \cdots \oplus C \to V$ induces a linear map $\tilde{f}: C \otimes \cdots \otimes C \to V$; let $\sum_{(c)} f(c_{(1)}, \ldots, c_{(n)})$ denote $\tilde{f}(\sum_{(c)} c_{(1)} \otimes \cdots \otimes c_{(n)})$. In this notation the identity relating ε and Δ becomes $\sum_{(c)} \varepsilon(c_{(1)})c_{(2)} = c = \sum_{(c)} c_{(1)}\varepsilon(c_{(2)})$.

If V and W are vector spaces we use t to denote the twist map $t: V \otimes W \to W \otimes V, v \otimes w \to w \otimes v$. A coalgebra C is called cocommutative if $t\Delta = \Delta$ or for all $c \in C$, $\sum_{(c)} c_{(1)} \otimes c_{(2)} = \sum_{(c)} c_{(2)} \otimes c_{(1)}$. If C is a cocommutative coalgebra we can permute the numerical subscripts arbitrarily in any computation involving $\sum_{(c)} c_{(1)} \otimes \cdots \otimes c_{(n)}$.

If C and D are coalgebras then $C \otimes D$ is a coalgebra where $\Delta_{C \otimes D} = (I \otimes t \otimes I) \cdot (\Delta_C \otimes \Delta_D)$ and $\varepsilon_{C \otimes D} = \varepsilon_C \otimes \varepsilon_D$. Thus $\Delta_{C \otimes D}(c \otimes d) = \sum_{(c),(d)} (c_{(1)} \otimes d_{(1)}) \otimes (c_{(2)} \otimes d_{(2)})$.

A Hopf algebra H is an algebra and a coalgebra where the coalgebra structure morphisms Δ_H, ε_H are algebra homomorphisms. Thus for example, $\Delta_H(gh) = \sum_{(g),(h)} g_{(1)}h_{(1)} \otimes g_{(2)}h_{(2)}$, $g, h \in H$. If V is a left H-module then $V \otimes V$ is naturally a left $H \otimes H$-module. By pull back along $\Delta: H \to H \otimes H$, $V \otimes V$ becomes a left H-module. Specifically, $h \cdot (v \otimes \tilde{v}) = \sum_{(h)} h_{(1)} \cdot v \otimes h_{(2)} \cdot \tilde{v}$. The augmentation $\varepsilon: H \to k$ gives k the structure of a left H-module.

DEFINITION. An algebra A which is a left H-module is called a (left) *H-module algebra* if m_A and μ_A are H-module morphisms. A coalgebra C which is a left H-module is called an *H-module coalgebra* if Δ_C and ε_C are H-module morphisms. ($A \otimes A$, k, $C \otimes C$ each have the H-module structure indicated in the preceding paragraph.)

If A is an H-module algebra then $h \cdot (a\tilde{a}) = \sum_{(h)} (h_{(1)} \cdot a)(h_{(2)} \cdot \tilde{a})$ and $h \cdot 1 = \varepsilon(h)1$. If C is an H-module coalgebra then $\Delta_C(h \cdot c) = \sum_{(h),(c)} (h_{(1)} \cdot c_{(1)}) \otimes (h_{(2)} \cdot c_{(2)})$ and $\varepsilon_C(h \cdot c) = \varepsilon_H(h)\varepsilon_C(c)$.

EXAMPLE 1.1. Let C be the underlying coalgebra of H and let C have the left H-module structure induced by multiplication. The fact that Δ_H is an algebra morphism implies that Δ_C is an H-module morphism. The fact that ε_H is an algebra morphism implies that ε_C is an H-module morphism. Thus C is an H-module coalgebra.

EXAMPLE 1.2. We generalize the above example. For a vector space V and $0 < q \in z$ let $\bigotimes^q V$ denote $V \otimes \cdots \otimes V$ q-times. $\bigotimes^q H$ has the coalgebra structure on the tensor product of coalgebras. $\bigotimes^q H$ is a left H-module where $h \cdot (h_1 \otimes \cdots \otimes h_q)$ is defined to be $(hh_1) \otimes h_2 \otimes \cdots \otimes h_q$. Then the induced H-module structure on $(\bigotimes^q H) \otimes (\bigotimes^q H)$ is given by

$$h \cdot [(h_1 \otimes \cdots \otimes h_q) \otimes (\tilde{h}_1 \otimes \cdots \otimes \tilde{h}_q)]$$
$$= \sum_{(h)} [(h_{(1)}h_1) \otimes h_2 \otimes \cdots \otimes h_q] \otimes [(h_{(2)}\tilde{h}_1) \otimes \tilde{h}_2 \otimes \cdots \otimes \tilde{h}_q].$$

For the same reasons as in Example 1.1, $\bigotimes^q H$ is an H-module coalgebra.

We let $\bigotimes^0 V$ denote k for any vector space V. If $\bigotimes^0 H$ has the H-module structure induced by ε and the usual trivial coalgebra structure it is an H-module coalgebra. (It also is an H-module algebra.)

EXAMPLE 1.3. If G is a semigroup, by which we mean that G is associative has a unit but may lack inverses, then the (semi)group algebra kG has a Hopf algebra structure where $\Delta(g) = g \otimes g$, $\varepsilon(g) = 1$, for $g \in G$. Suppose G is a semigroup of unit preserving homomorphisms of an algebra A. The induced kG-module structure on A gives A a kG-module algebra structure.

EXAMPLE 1.4. Suppose L is a Lie algebra with universal enveloping algebra UL. Then UL has a Hopf algebra structure where $\Delta(l) = 1 \otimes l + l \otimes 1$, $\varepsilon(l) = 0$ for $l \in L$, [12, p. 152, Theorem 1]. If L is a Lie algebra of derivations on an algebra A, there is induced a UL-module structure on A with respect to which A is a UL-module algebra.

If C is a coalgebra and A an algebra then Hom (C, A) has an algebra structure. For $f, g \in$ Hom (C, A) the product $f * g$ is $m_A(f \otimes g)\Delta_C$. Thus for $c \in C$, $f * g(c) = \sum_{(c)} f(c_{(1)})g(c_{(2)})$. The unit of Hom (C, A) is $\mu_A\varepsilon_C$. This product of functions is called *convolution*. If C is a cocommutative coalgebra and A is a commutative algebra then it is clear that Hom (C, A) is a commutative algebra.

DEFINITION. If A is an algebra A^r denotes the multiplicative group of invertible-regular-elements of A. If C is a coalgebra and A an algebra $\mathrm{Reg}\,(C, A)$ denotes $\mathrm{Hom}\,(C, A)^r$.

Observe $\mathrm{Reg}\,(C, A)$ is a multiplicative abelian group when C is cocommutative and A is commutative.

Suppose C is an H-module coalgebra and A an H-module algebra. $\mathrm{Hom}_H\,(C, A)$ denotes the H-module morphisms from C to A. Clearly $\mu_A\varepsilon_C \in \mathrm{Hom}_H\,(C, A)$. Suppose $f, g \in \mathrm{Hom}_H\,(C, A)$ then

$$h\cdot[f * g(c)] = \sum_{(c)} h\cdot[f(c_{(1)})g(c_{(2)})] = \sum_{(h),(c)} (h_{(1)}\cdot f(c_{(1)}))(h_{(2)}\cdot f(c_{(2)}))$$
$$= \sum_{(h),(c)} f(h_{(1)}\cdot c_{(1)})g(h_{(2)}\cdot c_{(2)}) = f * g(h\cdot c),$$

for $h \in H$, $c \in C$. Thus $\mathrm{Hom}_H\,(C, A)$ is a subalgebra of $\mathrm{Hom}\,(C, A)$ and we define $\mathrm{Reg}_H\,(C, A)$ to be $\mathrm{Hom}_H\,(C, A)^r$. This is the subgroup of $\mathrm{Reg}\,(C, A)^D$ consisting of all H-module morphisms.

2. **Definition of the cohomology.** *Throughout the paper H will denote a cocommutative Hopf algebra; i.e., where the underlying coalgebra is cocommutative and A will denote a commutative algebra.*

We form a semisimplicial complex [7, p. 55], [8, p. 56], whose objects are the H-module coalgebras $\{\bigotimes^{q+1} H\}_{q\geqq 0}$ of Example 1.2. The object of q-degree is $\bigotimes^{q+1} H$ for $q=0, 1, \ldots$. The face operators are given by $\partial_i\colon \bigotimes^{q+1} H \to \bigotimes^q H$, $(x_0 \otimes \cdots \otimes x_q) \to (x_0 \otimes \cdots \otimes x_i x_{i+1} \otimes \cdots \otimes x_q)$ for $i=0, \ldots, q-1$ and $\partial_q\colon \bigotimes^{q+1} H \to \bigotimes^q H$, $(x_0 \otimes \cdots \otimes x_{q-1})\varepsilon(x_q)$.

The degeneracy operators are given by $s_i\colon \bigotimes^{q+1} H \to \bigotimes^{q+2} H$, $(x_0 \otimes \cdots \otimes x_q) \to (x_0 \otimes \cdots \otimes x_i \otimes 1 \otimes x_{i+1} \otimes \cdots \otimes x_q)$ for $i=0, \ldots, q$. All the face and degeneracy operators are H-module coalgebra morphisms; i.e., H-module morphisms and coalgebra morphisms. We omit the calculations verifying the face-degeneracy operator identities.

Suppose A is an H-module algebra. We have the contravariant functor $\mathrm{Reg}_H\,(*, A)$ from cocommutative H-module coalgebras to abelian groups. We apply this functor to the above semisimplicial complex to obtain a semi-cosimplicial complex whose objects are $\{\mathrm{Reg}_H\,(\bigotimes^{q+1} H, A)\}_{q\geqq 0}$. We denote the coface operators, $\mathrm{Reg}_H\,(\partial_i, A)\colon \mathrm{Reg}_H(\bigotimes^q H, A) \to \mathrm{Reg}_H\,(\bigotimes^{q+1} H, A)$, by ∂^i for $i=0, \ldots, q$. The homology of the semi-cosimplicial complex is defined by means of the differential $d^{q-1}\colon \mathrm{Reg}_H\,(\bigotimes^q H, A) \to \mathrm{Reg}_H\,(\bigotimes^{q+1} H, A)$ where $d^{q-1} = (\partial^0) * (\partial^1)^{-1} * \cdots * (\partial^q)^{\pm 1}$. Thus we have

$$\mathrm{Reg}_H\,(\textstyle\bigotimes^1 H, A) \xrightarrow{d^0} \mathrm{Reg}_H\,(\bigotimes^2 H, A) \xrightarrow{d^1} \cdots \xrightarrow{d^{n-1}} \mathrm{Reg}_H\,(\bigotimes^{n+1} H, A) \xrightarrow{d^n} \cdots.$$

The cohomology of H in A is defined to be the homology of the above complex and the qth group—$\mathrm{Ker}\, d^q/\mathrm{Im}\, d^{q-1}$ for $q>0$ and $\mathrm{Ker}\, d^0$ for $q=0$—is denoted $H^q(H, A)$.

(In [17, p. 235] the homology of a semisimplicial complex is defined. Our complex is obtained from a contravariant functor applied to a semisimplicial complex; hence, is a semi-cosimplicial complex. By dualizing the theory in [17, p. 235] one obtains the above homology of $\{\mathrm{Reg}_H(\bigotimes^{q+1} H, A)\}$.)

REMARK. Since $\bigotimes^1 H = H$ and we have $\varepsilon\colon H \to k$ it seems as if

$$\cdots \;\begin{array}{c}\longrightarrow\\ \vdots\\ \rightleftarrows\\ \vdots\\ \longleftarrow\end{array}\; \bigotimes^{q+1} H \;\begin{array}{c}\longrightarrow\\ \vdots\\ \rightleftarrows\\ \vdots\\ \longleftarrow\end{array}\; \cdots \;\begin{array}{c}\longrightarrow\\ \longrightarrow\\ \rightleftarrows\\ \longleftarrow\end{array}\; \bigotimes^2 H \;\begin{array}{c}\longrightarrow\\ \rightleftarrows\end{array}\; H \xrightarrow{\varepsilon} k$$

is a semisimplicial resolution of k to which we are applying the functor $\mathrm{Reg}_H(*, A)$ and taking homology. In this sense the cohomology seems similar to the right derived functors of $\mathrm{Reg}_H(*, A)$.

There is a normal subcomplex of our simplicial complex

$$\{\mathrm{Reg}_H(\bigotimes^{q+1} H, A), d^q\}_{q \geqq 0}.$$

For $q > 0$ let

$$s^i \equiv \mathrm{Reg}_H(s_i, A)\colon \mathrm{Reg}_H(\bigotimes^{q+2} H, A) \to \mathrm{Reg}_H(\bigotimes^{q+1} H, A), \quad i = 0, \ldots, q.$$

Let $N^{q+1} = \mathrm{Ker}\, s^0 \cap \cdots \cap \mathrm{Ker}\, s^q$. For $q = 0$ let $N^0 = \mathrm{Reg}_H(\bigotimes^1 H, A)$. Then $\{N^q, d^q | N^q\}_{q \geqq 0}$ is a subcomplex of $\{\mathrm{Reg}_H(\bigotimes^{q+1} H, A), d^q\}_{q \geqq 0}$. The injection map induces an isomorphism of homology. (The dual result and proof can be found in [17, p. 236, Theorem 6.1].)

We now present realizations of the complexes

$$\{\mathrm{Reg}_H(\bigotimes^{q+1} H, A), d^q\}_{q \geqq 0} \quad \text{and} \quad \{N^q, d^q | N^q\}_{q \geqq 0}.$$

There is a natural algebra isomorphism $\mathrm{Hom}_H(\bigotimes^q H, A) \to \mathrm{Hom}(\bigotimes^{q-1} H, A)$ induced by $\bigotimes^{q-1} H \to \bigotimes^q H$, $x \to 1 \otimes x$. This induces an isomorphism

$$\iota\colon \mathrm{Reg}_H(\bigotimes^q H, A) \to \mathrm{Reg}(\bigotimes^{q-1} H, A).$$

Let $\psi\colon H \otimes A \to A$, $h \otimes a \to h \cdot a$; then with respect to ι the coface operator $\partial^0\colon \mathrm{Reg}_H(\bigotimes^q H, A) \to \mathrm{Reg}_H(\bigotimes^{q+1} H, A)$ corresponds to the map

$$\delta^0\colon \mathrm{Reg}(\bigotimes^{q-1} H, A) \to \mathrm{Reg}(\bigotimes^q, H, A), \quad f \to \psi(I \otimes f).$$

For $i = 1, \ldots, q-1$ the coface operator ∂^i corresponds to $\delta^i\colon \mathrm{Reg}(\bigotimes^{q-1} H, A) \to \mathrm{Reg}(\bigotimes^q H, A), f \to f(I \otimes \cdots \otimes I \otimes m \otimes I \otimes \cdots \otimes I)$, where m is in the ith position. The coface operator ∂^q corresponds to the map $\delta^q\colon \mathrm{Reg}(\bigotimes^{q-1} H, A) \to \mathrm{Reg}(\bigotimes^q H, A), f \to f \otimes \varepsilon$. Thus if we define the differential

$$D^{q-1}\colon \mathrm{Reg}(\bigotimes^{q-1} H, A) \to \mathrm{Reg}(\bigotimes^q H, A),$$

$$\begin{aligned} D^{q-1}(f) = {} & [\psi(I \otimes f)] * [f^{-1}(m \otimes I \otimes \cdots \otimes I)] \\ & * [f(I \otimes m \otimes I \otimes \cdots \otimes I)] * \cdots * [f^{\pm 1}(I \otimes \cdots \otimes I \otimes m)] \\ & * [f^{\mp 1} \otimes \varepsilon], \end{aligned}$$

the simplicial complex $\{\mathrm{Reg}\,(\bigotimes^q H, A), D^q\}_{q\geqq 0}$ is isomorphic to the simplicial complex $\{\mathrm{Reg}_H\,(\bigotimes^{q+1} H, A), d^q\}_{q\geqq 0}$ which defines the cohomology $H^q(H, A), q\geqq 0$.

Let $\mathbf{1}_i\colon \bigotimes^q H \to \bigotimes^{q+1} H$, $h_1 \otimes \cdots \otimes h_q \to h_1 \otimes \cdots \otimes h_i \otimes 1 \otimes h_{i+1} \otimes \cdots \otimes h_q$, $i=0,\ldots,q$. With respect to ι the codegeneracy operator $s^i\colon \mathrm{Reg}_H\,(\bigotimes^{q+2} H, A) \to \mathrm{Reg}_H\,(\bigotimes^{q+1} H, A)$ corresponds to the map $\sigma^i\colon \mathrm{Reg}\,(\bigotimes^{q+1} H, A) \to \mathrm{Reg}\,(\bigotimes^q H, A), f \to f\mathbf{1}_i$. We define (for $q\geqq 0$)

$$\mathrm{Reg}_+^{q+1}\,(H, A) = \mathrm{Ker}\,\mathbf{1}_1 \cap \cdots \cap \mathrm{Ker}\,\mathbf{1}_q$$

and $\mathrm{Reg}_+^0\,(H, A) = \mathrm{Reg}\,(\bigotimes^0 H, A)$. Then $\{\mathrm{Reg}_+^q\,(H, A), D_+^q \equiv D^q|\mathrm{Reg}_+^q\,(H, A)\}_{q\geqq 0}$ is a subcomplex of $\{\mathrm{Reg}\,(\bigotimes^q H, A), D^q\}_{q\geqq 0}$ which is isomorphic to $\{N^q, d^q|N^q\}_{q\geqq 0}$ under the restriction of ι. Thus $\{\mathrm{Reg}_+^q\,(H, A), D_+^q\}_{q\geqq 0}$ is a *normal* subcomplex and the inclusion map induces an isomorphism of homology.

Note that if $q>0$ and $f\in \mathrm{Reg}_+^q\,(H, A)$ then $f(h_1 \otimes \cdots \otimes h_q) = \varepsilon(h_1)\cdots\varepsilon(h_q)$ if some $h_i \in k$; in particular $f(1 \otimes \cdots \otimes 1) = 1$. We introduce the notation $\mathrm{Reg}^q\,(H, A)$ to denote $\mathrm{Reg}\,(\bigotimes^q H, A)$. Thus the simplicial complex $\{\mathrm{Reg}\,(\bigotimes^q H, A), D^q\}_{q\geqq 0}$ will be denoted $\{\mathrm{Reg}^q\,(H, A), D^q\}_{q\geqq 0}$, and referred to as the *standard* complex to compute $H^q(H, A)$.

We briefly look at $H^i(H, A)$ for $i=0, 1$. $\mathrm{Reg}^0\,(H, A) \cong A^r$ and if $a \in H^0(H, A)$ then $(h\cdot a)a^{-1} = \varepsilon(h)$ for all $h \in H$. Thus $h\cdot a = \varepsilon(h)a$ for all $h \in H$. We denote by A^H the set $\{a \in A | h\cdot a = \varepsilon(h)a$ for all $h \in H\}$. This is a subalgebra of A since A is an H-module algebra. Suppose $a \in A^r \cap A^H$. For all $h \in H$, $\varepsilon(h) = h\cdot 1 = h\cdot(aa^{-1}) = \sum_{(h)} (h_{(1)}\cdot a)(h_{(2)}\cdot a^{-1}) = \sum_{(h)} \varepsilon(h_{(1)})a(h_{(2)}\cdot a^{-1}) = a(h\cdot a^{-1})$ which implies $a^{-1} \in A^H \cap A^r$. Thus $H^0(H, A) = A^{Hr}$. Note, A^H is just the "invariants" with respect to the Hochschild theory, [6, p. 170].

If $f\colon H \to A$ is a 1-cocycle then $\mu(\varepsilon \otimes \varepsilon) = D^1(f) = [\psi(I \otimes f)] * [f^{-1}m] * [f \otimes \varepsilon]$ or $fm = [\psi(I \otimes f)] * [f \otimes \varepsilon]$. This implies for all $g, h \in H$ that

$$f(gh) = \sum_{(g),(h)} (g_{(1)}\cdot f(h_{(1)}))(f(g_{(2)})\varepsilon(h_{(2)})) = \sum_{(g)} (g_{(1)}\cdot f(h))f(g_{(2)}).$$

In case $A = A^H$ this reduces further to $f(gh) = f(h)f(g)$ so that f is a homomorphism. In general f is a "crossed" homomorphism and $H^1(H, A)$ is the group of regular crossed homomorphisms modulo the subgroup of regular inner crossed homomorphisms. An inner crossed homomorphism is one of the form $D^1(a)$ for $a \in A$. For $h \in H$, $D^1(a)(h) = (h\cdot a)a^{-1}$.

We point out that there is a dual theory to the preceding for cocommutative coalgebras which are comodules over commutative Hopf algebras. They must be comodule coalgebras—the dual notion to "H-module algebra". The functor is the group (under convolution) of invertible comodule morphisms from the coalgebra to the objects, which are algebras, in the semi-cosimplicial complex. The algebras, which are the objects, consist of the Hopf algebra tensored with itself a number of times. The coface operators are maps of the form $I \otimes \cdots \otimes I \otimes \Delta_{\tilde{H}} \otimes I \otimes \cdots \otimes I$ and $\mu_{\tilde{H}} \otimes I \otimes \cdots \otimes I$, (where $\tilde{H}$ is the commutative Hopf algebra). The codegeneracy operators are maps of the form $I \otimes \cdots \otimes I \otimes \varepsilon \otimes I \otimes \cdots \otimes I$. This

theory may be useful in the area of affine algebraic groups where the commutative Hopf algebra is taken to be the coordinate ring of the algebraic group. Rational modules for the group correspond to the comodules for the Hopf algebra.

3. **Comparison with group cohomology.** Suppose G is a group and kG is the group algebra Hopf algebra as in Example 1.3, (which is cocommutative). Let A be a kG-module algebra. The elements of G act as automorphisms of A so they carry A^r into itself. By restricting the module action the multiplicative abelian group A^r becomes a G-module and we can consider the group cohomology $H^q(G, A^r)$.

THEOREM 3.1. *$H^q(kG, A)$ and $H^q(G, A^r)$ are canonically isomorphic for all q. The isomorphism is induced by a canonical isomorphism between the standard complex to compute $H^q(kG, A)$ and the "standard complex" to compute $H^q(G, A^r)$,* [20, p. 121, (**)].

Proof. For $g_1, \ldots, g_q \in G$ the element $g_1 \otimes \cdots \otimes g_q \in kG \otimes \cdots \otimes kG$ diagonalizes $\Delta(g_1 \otimes \cdots \otimes g_q) = (g_1 \otimes \cdots \otimes g_q) \otimes (g_1 \otimes \cdots \otimes g_q)$. Thus $f^{-1}(g_1 \otimes \cdots \otimes g_q) = [f(g_1 \otimes \cdots \otimes g_q)]^{-1}$ and $f(g_1 \otimes \cdots \otimes g_q) \in A^r$ for all $f \in \mathrm{Reg}^q(kG, A)$. The map $G \times \cdots \times G \to kG \otimes \cdots \otimes kG$, $g_1 \times \cdots \times g_q \to g_1 \otimes \cdots \otimes g_q$ induces the group homomorphism $\mathrm{Reg}^q(kG, A) \to \mathrm{Hom}_{\mathrm{set}}(G \times \cdots \times G, A^r)$ which is a group isomorphism since $\{g_1 \otimes \cdots \otimes g_q \mid g_1 \times \cdots \times g_q \in G \times \cdots \times G\}$ is a basis for $kG \otimes \cdots \otimes kG$. When $q=0$, $\mathrm{Reg}^0(kG, A) = \mathrm{Reg}(k, A)$ which is canonically isomorphic to A^r the 0th group in the standard group cohomology complex. The group isomorphisms $\mathrm{Reg}^q(kG, A) \to \mathrm{Hom}_{\mathrm{set}}(G \times \cdots \times G, A^r)$ and $\mathrm{Reg}^0(kG, A) \to A^r$ form a morphism of complexes. Q.E.D.

EXAMPLE 3.1. If A is a field which is a finite Galois extension of k, G is the Galois group of A over k and the action of kG on A is induced by the action of G, it follows from Theorem 3.1 that $H^q(kG, A)$ is precisely the Galois cohomology. By [19, p. 330, Theorem 1] this is the Amitsur cohomology of A. In §5 we relate Amitsur's cohomology to the Hopf algebra cohomology. This will give a simple direct proof that $H^q(kG, A)$ is isomorphic to the Amitsur cohomology.

EXAMPLE 3.2. Suppose G is a group and V is a vector space which is a G-module; hence, a kG-module. We consider V to have trivial multiplication and let $A = k \oplus V$, V with a unit adjoined. Thus $(\lambda, v)(\tilde{\lambda}, \tilde{v}) = (\lambda\tilde{\lambda}, \tilde{\lambda}v + \lambda\tilde{v})$. A has a kG-module algebra structure where we define $g \cdot (\lambda, v)$ to be $(\lambda, g \cdot v)$ for $g \in G$. A^r is naturally isomorphic to the direct sum of the multiplicative group k^r and the additive group V, where an isomorphism is given by $k^r \times V \to A^r$, $(\lambda \times v) \to (\lambda, v)$. Thus $H^1(kG, A) = H^1(G, k^r \times V)$. We shall show in §6 that $H^1(G, V)$ can be recovered from $H^1(kG, A)$ as a relative cohomology group. It will be a direct summand of $H^1(kG, A)$.

4. **Comparison with Lie cohomology.** Although we give a proof of our main result which is independent of characteristic we first give a proof for characteristic

zero. In this case the proof is much simpler but contains the main technique of the general proof.

Suppose L is a Lie algebra and UL is the universal enveloping Hopf algebra as in Example 1.4. (UL is cocommutative since UL is generated by L as an algebra and $\Delta(l)=1\otimes l+l\otimes 1$ for all $l\in L$.) Let A be a UL-module algebra and let A^+ denote the underlying vector space structure of A. By restricting the module action A^+ becomes an L-module and we can consider the Lie cohomology $H^q(L, A^+)$.

THEOREM 4.1. *Suppose p (the characteristic of k) is zero. $H^q(UL, A)$ and $H^q(L, A^+)$ are canonically isomorphic for $q\geqq 2$. The isomorphism is induced by a canonical isomorphism of complexes between the rth groups of the normal complex to compute the Hopf cohomology of $H^q(UL, A)$ and the rth groups of the normal complex* [6, p. 175–176] *to compute the Hochschild cohomology of $H^q(UL, A^+)$ for $r\geqq 1$.*

Proof. In [6, p. 175–176] the normal complex to compute $H^q(UL, A^+)$ has groups $C_n=\{f\in \operatorname{Hom}(\bigotimes^n UL, A) \mid f(\lambda_1\otimes\cdots\otimes\lambda_n)=0$ if some $\lambda_i\in k\}$ for $n>0$ and $C_0=A^+$. The differential is given by

$$\begin{aligned}\delta^n(f)(\lambda_1\otimes\cdots\otimes\lambda_{n+1}) &= \lambda_1 f(\lambda_2\otimes\cdots\otimes\lambda_{n+1})\\ &\quad+\sum_1^n(-1)^i f(\lambda_1\otimes\cdots\otimes\lambda_i\lambda_{i+1}\otimes\cdots\otimes\lambda_{n+1})\\ &\quad+(-1)^{n+1}f(\lambda_1\otimes\cdots\otimes\lambda_n)\varepsilon(\lambda_{n+1})\end{aligned}$$

for $n>0$, and for $n=0$, $a\in A^+$, $\delta^0(a)(\lambda)=\lambda a-a\varepsilon(\lambda)$.

We now give a group isomorphism from C_n to $\operatorname{Reg}^n_+(UL, A)$ for $n\geqq 1$; we do this by means of an exponential map. Suppose $f\in C_n$ and $g\in\operatorname{Hom}(\bigotimes^n UL, A)$, then $f*g\in C_n$ since $\Delta(1)=1\otimes 1$. Thus C_n is an ideal in $\operatorname{Hom}(\bigotimes^n UL, A)$.

$\operatorname{Hom}(UL, A)$ is a left UL-module if we define $u\rightharpoonup f$ by setting $(u\rightharpoonup f)(v)=f(vu)$ for $f\in\operatorname{Hom}(UL, A)$ $u, v\in UL$. The identity of $\operatorname{Hom}(UL, A)$ is $\mu\varepsilon$ and $(u\rightharpoonup\mu\varepsilon)(v)=\mu\varepsilon(vu)=\mu(\varepsilon(v)\varepsilon(u))$. Thus $u\rightharpoonup\mu\varepsilon=\varepsilon(u)\mu\varepsilon$. For $f, g\in\operatorname{Hom}(UL, A)$

$$\begin{aligned}[u\rightharpoonup(f*g)](v) &= (f*g)(vu)=\sum_{(u),(v)} f(v_{(1)}u_{(1)})g(v_{(2)}u_{(2)})\\ &= \sum_{(u)}(u_{(1)}\rightharpoonup f)*(u_{(2)}\rightharpoonup g)(v).\end{aligned}$$

Thus $\operatorname{Hom}(UL, A)$ is a left UL-module algebra. In particular since $\Delta(l)=1\otimes l+l\otimes 1$ for $l\in L$, the elements of L act as derivations on $\operatorname{Hom}(UL, A)$.

Suppose $f\in C_1$, we shall show by induction that for any $g\in\operatorname{Hom}(UL, A)$ and $l_1,\ldots,l_n\in L$ then $f^n*g(l_1\cdots l_n)=n!f(l_1)\cdots f(l_n)g(1)$. The result is clear for $n=1$ since $f*g(l_1)=f(l_1)g(1)+f(1)g(l_1)=f(l_1)g(1)$. Suppose the result has been proved for $n-1$.

$$f^n*g(l_1\cdots l_n) = nf^{n-1}*(l_n\rightharpoonup f)*g(l_1\cdots l_{n-1})+f^n*(l_n\rightharpoonup g)(l_1\cdots l_{n-1}).$$

By the induction the first term on the right hand side equals $n(n-1)!f(l_1)\cdots f(l_{n-1})[(l_n \rightharpoonup f) * g(1)] = n!f(l_1)\cdots f(l_n)g(1)$. Also, by the induction the second term on the right equals $(n-1)!f(l_1)\cdots f(l_{n-1})[f * (l_n \rightharpoonup g)(1)] = 0$ since $f * (l_n \rightharpoonup g)(1) = 0$. This concludes the induction.

The main two implications of the preceding paragraph are that $f^n(l_1\cdots l_n) = n!f(l_1)\cdots f(l_n)$ and for $n > r$ $f^n(l_1\cdots l_r) = f^r * f^{n-r}(l_1\cdots l_r) = 0$, for $f \in C_1$, $l_1, \ldots, l_r \in L$. It is well known, [12, p. 152, Theorem 1], that UL is spanned by monomials of elements of L. Thus if $x \in UL$, $f^n(x) = 0$ for large n.

By [6, p. 268, Proposition 1.2] $\bigotimes^n UL$ is isomorphic to the universal enveloping algebra of $L \oplus \cdots \oplus L$ (n times). One easily checks this is an isomorphism of Hopf algebras. Clearly for $f \in C_n$, $f(1 \otimes \cdots \otimes 1) = 0$ so that by the preceding paragraph with L replaced by $L \oplus \cdots \oplus L$ it follows that if $x \in \bigotimes^n UL$, $f^m(x) = 0$ for large m. Let $e = \mu(\varepsilon \otimes \cdots \otimes \varepsilon)$ the unit of Hom $(\bigotimes^n UL, A)$. For $f \in C_n$ we define $\exp f = e + \sum_1^\infty f^i/i!$. This is a well-defined element of Hom $(\bigotimes^n UL, A)$ since for $x \in \bigotimes^n UL$, $(\exp f)(x) = e(x) + \sum_1^\infty f^i(x)/i!$ and the sum is actually finite. If $x = \lambda_1 \otimes \cdots \otimes \lambda_n$ and some $\lambda_i \in k$ then $f^i(x) = 0$ since $f^i \in C_n$; thus, $(\exp f)(x) = \mu(\varepsilon(\lambda_1)\cdots\varepsilon(\lambda_n))$, which implies $(\exp f) \in \mathrm{Reg}^n_+ (UL, A)$. By formal considerations $\exp(f+g) = (\exp f) * (\exp g)$ for $f, g \in C_n$, so that exp is a group homomorphism from the additive group C_n to the multiplicative group $\mathrm{Reg}^n_+ (UL, A)$. To show that exp is an isomorphism we construct the inverse, log.

For $f \in \mathrm{Reg}^n_+ (UL, A)$, $f - e \in C_n$. Thus if we define $\log f = \sum_1^\infty (-1)^{i-1}(f-e)^i/i$, $\log f$ is a well-defined element of C_n. By formal considerations log is a group homomorphism from $\mathrm{Reg}^n_+ (UL, A)$ to C_n which is the inverse to exp. Next we show that the group isomorphism exp forms an isomorphism of complexes (in positive degree).

The maps Hom $(\bigotimes^n UL, A) \to$ Hom $(\bigotimes^{n+1} UL, A)$

$$
\begin{aligned}
&f \to \psi(I \otimes f),\\
&f \to f(m \otimes I \otimes \cdots \otimes I),\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
&f \to f(I \otimes \cdots \otimes I \otimes m),\\
&f \to f \otimes \varepsilon
\end{aligned}
$$

are algebra morphisms, (ψ: $UL \otimes A \to A$, $u \otimes a \to ua$). Let F be one of the above maps, then $F(f^n) = F(f)^n$ for all $f \in$ Hom $(\bigotimes^n UL, A)$. If $f \in C_n$ this implies $F(\exp f) = \exp F(f)$. This shows exp is an isomorphism of complexes (in positive degree). By [6, p. 282, Theorem 8] the Hochschild cohomology of $H^q(UL, A^+)$ is equivalent to the Lie cohomology $H^q(L, A^+)$. Q.E.D.

We briefly investigate the relationship between $H^i(UL, A)$ and $H^i(L, A^+)$ for $i = 0, 1$. $H^0(L, A^+) = \{a \in A^+ \mid la = 0 \text{ for all } l \in L\}$, [6, p. 270, §2]. The elements of $H^0(L, A^+)$ are called the invariants of A. $H^0(L, A^+)$ is a subalgebra of A since the elements of L act as derivations. Since UL is generated by L it follows that $H^0(L, A^+) = A^{UL}$. Thus $H^0(UL, A) = A^{UL_r} = H^0(L, A^+)^r$.

PROPOSITION 4.2. *Suppose $p=0$ and $A=H^0(L, A^+)+I$ where I is the ideal consisting of all nilpotent elements of A. Then, $H^1(UL, A)\cong H^1(L, A^+)$ and the isomorphism is induced by the isomorphism of complexes (in positive degree) given in Theorem* 4.1.

Proof. Since exp is an isomorphism of complexes in positive degree it carries the 1-cocycles of C_1 isomorphically onto the 1-cocycles of Reg^1_+ (UL, A). It suffices to show that exp is an isomorphism between the 1-coboundaries.

Suppose $\delta^0(a)$ is a 1-coboundary in C_1. Since $A=H^0(L, A^+)+I$ we may assume $a\in I$. Thus $\exp a=1+\sum_1^\infty a^i/i!$ is defined since a is nilpotent. Then $\exp \delta^0(a) = D^0_+(\exp a)$ so that exp carries the 1-coboundaries of C_1 into the 1-coboundaries of Reg^1_+ (UL, A).

Suppose $D^0_+(a)$ is a 1-coboundary in Reg^1_+ (UL, A) where $a\in A^r$. By hypothesis $a=b+x$ where $b\in H^0(L, A^+)$, $x\in I$. Since $b=a-x$ it has inverse $a^{-1}+a^{-2}x +a^{-3}x^2+a^{-4}x^3+a^{-5}x^4+\cdots$ which is well defined since x is nilpotent. Let $z =1+b^{-1}x$, then $a=bz$ and z is invertible. $D^0_+(a)(l_1\cdots l_n)=[(l_1\cdots l_n)\cdot bz]/bz =[(l_1\cdots l_n)\cdot z]/z$ since $b\in H^0(L, A^+)$. Since L generates UL it follows that $D^0_+(a)= D^0_+(z)$. We have $z-1=b^{-1}x\in I$ so that $\log z=\sum_1^\infty (-1)^{i-1}(b^{-1}x)^i/i$ is defined and lies in I. Clearly $z=\exp\log z$ and $D^0_+(z)=\exp \delta^0(\log z)$. Thus exp carries the 1-coboundaries of C_1 surjectively to the 1-coboundaries of Reg^1_+ (UL, A). Q.E.D.

We now prove Theorem 4.1 for arbitrary characteristic. The proof is substantially the same, the main technique being the use of the group isomorphism exp and its inverse log. However, the definition of exp and log and verifying that they are morphisms of complexes is more difficult than before.

THEOREM 4.3 *For arbitrary characteristic $H^q(UL, A)$ and $H^q(L, A^+)$ are canonically isomorphic for $q\geqq 2$. The isomorphism is induced by a canonical isomorphism of complexes between the rth groups of the normal complex to compute the Hopf cohomology of $H^q(UL, A)$ and the rth groups of the normal complex to compute the Hochschild cohomology of $H^q(UL, A^+)$ for $r\geqq 1$.*

Proof. The normal complex to compute the Hochschild cohomology of $H^q(UL, A^+)$ is the complex $\{C_n, \delta^n\}$ which is exhibited in the proof of Theorem 4.1. C_n is an ideal in Hom $(\bigotimes^n UL, A)$ and Hom (UL, A) is a left UL-module algebra as indicated in the second and third paragraphs of the proof of Theorem 4.1.

By restricting the action Hom (UL, A) is a left L-module and the elements of L act as derivations. For $f\in C_1$ we define a sequence of elements ${}^0f, {}^1f, {}^2f, \ldots$ inductively, (${}^if$ should be thought of as $f^i/i!$). Let ${}^0f=\mu\varepsilon$ the unit of Hom (UL, A) and let ${}^1f=f$. Suppose ${}^{n-1}f$ has been defined where $l\rightharpoonup {}^if={}^{i-1}f*(l\rightharpoonup f)$ for $l\in L$, $1\leqq i\leqq n-1$. Let X be a one-dimensional vector space with basis x. Hom $(UL, A)\oplus X$ has an L-module structure where $l\rightharpoonup (u, \lambda x)$ is defined to be $l\rightharpoonup u+\lambda({}^{n-1}f)*(l\rightharpoonup f)$ for $u\in$ Hom (UL, A), $\lambda\in k$, $l\in L$. Hom $(UL, A)\oplus X$ has a natural left UL-module structure induced by the L-module structure [5, p. 39]. Hom (UL, A) is a submodule, and the module structure is that which was given

originally. If u lies in the kernel of the augmentation of UL—known as the augmentation ideal—then u is the sum of monomials of L, [12, p. 159, Theorem 3], so that $u \rightharpoonup x \in \mathrm{Hom}\,(UL, A)$. ${}^n f(u)$ is defined to be $(u \rightharpoonup x)(1)$ and ${}^n f(1)$ is defined to be 0; since UL is the direct sum of k and the augmentation ideal ${}^n f$ is well defined. By construction

$$l \rightharpoonup {}^n f = {}^{n-1} f * (l \rightharpoonup f), \qquad l \in L \tag{0}$$

and $\{{}^0 f, {}^1 f, \ldots\}$ is the unique sequence of elements of $\mathrm{Hom}\,(UL, A)$ satisfying (0) (for all positive n), ${}^0 f = 1$, ${}^1 f = f$ and ${}^n f(1) = 0$ (for all positive n).

Using the uniqueness property and induction one obtains the following:

$$ {}^n(f+g) = \sum_0^n ({}^i f) * ({}^{n-i} g), \tag{1}$$

$$ ({}^m f)({}^n f) = \binom{m+n}{m} ({}^{m+n} f) \tag{2}$$

$$ {}^m({}^n(f)) = ((mn)!/m!(n!)^m)({}^{mn} f), \tag{3}$$

$$\begin{aligned} ({}^n f) * h(l_1 \cdots l_r) &= 0 && \text{if } r < n, \\ &= f(l_1) \cdots f(l_n) h(1) && \text{if } r = n, \end{aligned} \tag{4}$$

where $f, g \in C_1$, $h \in \mathrm{Hom}\,(UL, A)$, $l_1, \ldots l_r \in L$. (Note, in (4) the induction is on $n+r$.)

Since UL is generated by L, by (4), $\sum_0^\infty {}^i f \equiv \exp f$ and $\sum_0^\infty i!(-1)^i({}^{i+1} f) \equiv \log(f + \mu\varepsilon)$ are well-defined elements of $\mathrm{Hom}\,(UL, A)$ when $f \in C_1$. By the identities (1)–(3) exp is an isomorphism from the additive group C_1 to the multiplicative group $\mathrm{Reg}^1_+(UL, A)$ with log being the inverse isomorphism.

Suppose M and N are Lie algebras by [6, p. 268, Proposition 1.2], the tensor product of universal enveloping algebras is (isomorphic to) a universal enveloping algebra. Let ψ: $UL \otimes A \to A$, $u \otimes a \to u \cdot a$. We have the following identities:

$$\begin{aligned} &\exp(\psi(I \otimes f)) = \psi(I \otimes \exp f) \in \mathrm{Hom}\,(UL \otimes UM, A) \\ &\qquad\qquad \text{for } f \in \mathrm{Hom}\,(UM, A) \quad \text{where } f(1) = 0, \end{aligned} \tag{5}$$

$$\begin{aligned} &\exp(f(I \otimes m \otimes I)) = (\exp f)(I \otimes m \otimes I) \in \mathrm{Hom}\,(UL \otimes UM \otimes UM \otimes UN, A) \\ &\qquad\qquad \text{for } f \in \mathrm{Hom}\,(UL \otimes UM \otimes UN) \quad \text{where } f(1 \otimes 1 \otimes 1) = 0, \end{aligned} \tag{6}$$

$$\begin{aligned} &\exp(f \otimes \varepsilon) = (\exp f) \otimes \varepsilon \in \mathrm{Hom}\,(UL \otimes UM, A) \\ &\qquad\qquad \text{for } f \in \mathrm{Hom}\,(UL, A) \quad \text{where } f(1) = 0. \end{aligned} \tag{7}$$

Since the proofs of these are similar we only present the proof of (5). It suffices to show for all n that

$$ {}^n(\psi(I \otimes f)) = \psi(I \otimes {}^n f). \tag{8}$$

Suppose this has been shown for $0 < n-1$. $UL \otimes UM$—as the universal enveloping algebra of $L \oplus M$—contains L in the space $L \otimes k$ and M in the space $k \otimes M$.

By the uniqueness property (0), it suffices to show the derivation $l \otimes 1$ gives the same element applied to either side of (8) and the derivation $1 \otimes r$ gives the same element applied to either side of (8), $l \in L$, $r \in M$.

$$\begin{aligned}(l \otimes 1) \rightharpoonup {}^n(\psi(I \otimes f)) &= {}^{n-1}(\psi(I \otimes f)) * [(l \otimes 1) \rightharpoonup \psi(I \otimes f)] \\ &= [\psi(I \otimes {}^{n-1}f)] * [\psi(I \otimes l \cdot f)] = \psi[(I \otimes ({}^{n-1}f * (l \cdot f))] \\ &= \psi[I \otimes l \cdot {}^n f] = (l \otimes 1) \rightharpoonup \psi(I \otimes {}^n f),\end{aligned}$$

where for all $g \in \operatorname{Hom}(UM, A)$ $l \cdot g$ is the function $u \to l \cdot g(u)$, $u \in UM$. The first equality above follows from (0), the second by induction, the third since A is a UL-module algebra. The fifth equality is clear. For the fourth equality we must show $l \cdot {}^n f = ({}^{n-1}f) * (l \cdot f)$. Say this is true for $n-1$. It is clear $l \cdot {}^n f(1) = ({}^{n-1}f) * (l \cdot f)(1) = 0$. Since UM is spanned by elements of the form 1 and ur, $u \in UM$, $r \in M$ it suffices to show $l \cdot {}^n f(ur) = {}^{n-1}f * (l \cdot f)(ur)$ or that $r \rightharpoonup (l \cdot {}^n f) = r \rightharpoonup ({}^{n-1}f * (l \cdot f))$. We have

$$\begin{aligned}r \rightharpoonup (l \cdot {}^n f) &= l \cdot (r \rightharpoonup {}^n f) = l \cdot ({}^{n-1}f * (r \rightharpoonup f)) = (l \cdot {}^{n-1}f) * (r \rightharpoonup f) + {}^{n-1}f * (l \cdot (r \rightharpoonup f)) \\ &= ({}^{n-2}f) * (l \cdot f) * (r \rightharpoonup f) + {}^{n-1}f * (r \rightharpoonup (l \cdot f)) = r \rightharpoonup ({}^{n-1}f * (l \cdot f)).\end{aligned}$$

$$\begin{aligned}(1 \otimes r) \rightharpoonup {}^n(\psi(I \otimes f)) &= {}^{n-1}(\psi(I \otimes f)) * [(1 \otimes r) \rightharpoonup \psi(I \otimes f)] \\ &= [\psi(I \otimes {}^{n-1}f)] * [\psi(I \otimes r \rightharpoonup f)] = \psi(I \otimes ({}^{n-1}f * (r \rightharpoonup f))) \\ &= \psi(I \otimes (r \rightharpoonup {}^n f)) = (1 \otimes r) \rightharpoonup (\psi(I \otimes {}^n f)).\end{aligned}$$

Here, all the equalities are clear.

The last fact we need to verify before showing that exp gives an isomorphism of complexes in positive degree is that:

$$(9) \quad (\exp f)(u \otimes 1 \otimes v) = \mu(\varepsilon(u)\varepsilon(v)), \quad \log(f + \mu(\varepsilon \otimes \varepsilon \otimes \varepsilon))(u \otimes 1 \otimes v) = 0,$$

for $f \in \operatorname{Hom}(UL \otimes UM \otimes UN, A)$ where $f(u \otimes 1 \otimes v) = 0$, $u \in UL$, $v \in UN$. It suffices to show ${}^n f(u \otimes 1 \otimes v) = 0$ for positive n. Assume by induction the result is true for $0 < n-1$. UN is spanned by 1 and elements of the form vr where $r \in N$,

$$\begin{aligned}{}^n f(u \otimes 1 \otimes vr) &= [(1 \otimes 1 \otimes r) \rightharpoonup {}^n f](u \otimes 1 \otimes v) \\ &= {}^{n-1}f * ((1 \otimes 1 \otimes r) \rightharpoonup f)(u \otimes 1 \otimes v)\end{aligned}$$

which is equal to zero by the induction and the fact $\Delta(1) = 1 \otimes 1$. We must consider ${}^n f(u \otimes 1 \otimes 1)$. UL is spanned by 1 and elements of the form ul where $l \in L$.

$$\begin{aligned}{}^n f(ul \otimes 1 \otimes 1) &= [(l \otimes 1 \otimes 1) \rightharpoonup {}^n f](u \otimes 1 \otimes 1) \\ &= {}^{n-1}f * ((l \otimes 1 \otimes 1) \rightharpoonup f)(u \otimes 1 \otimes 1)\end{aligned}$$

which is equal to zero by the induction and the fact $\Delta(1) = 1 \otimes 1$. Finally, ${}^n f(1 \otimes 1 \otimes 1) = 0$ by definition of ${}^n f$.

We have $\exp: C_n \to \operatorname{Reg}^n(UL, A)$ is a group homomorphism and by (9) $\exp: C_n \to \operatorname{Reg}^n_+(UL, A)$ is a group isomorphism with inverse log. That exp is a mor-

phism of complexes (in positive degree) follows from the form of the differential in the two complexes and (5), (6) and (7). By [6, p. 282, §8] the Hochschild cohomology is equivalent to the Lie cohomology. Q.E.D.

PROPOSITION 4.4. *Suppose $p>0$ and $A=H^0(L, A^+)+I$ where I is an ideal in A which is a UL submodule and $0=I\cdot I\cdot\cdots\cdot I$ (p times); then $H^1(UL, A)\cong H^1(L, A^+)$ and the isomorphism is induced by the isomorphism of complexes (in positive degree) given in Theorem* 4.3.

Proof. Suppose $f\in C_1$ then for $n<p$ ${}^nf=f^n/n!$. This follows from the uniqueness property (0) in the proof of Theorem 4.3. We must now prove that if f is of the form $f(u)=ua-\varepsilon(u)a$ for $u\in UL$, $a\in I$ then ${}^nf=0$ for $n\geqq p$. Suppose $\{f_i\}\subset \mathrm{Hom}\,(UL, A)$ and each f_i is of the form $f_i(u)=ua_i$, $a_i\in I$. We shall show that ${}^nf*f_1*\cdots*f_m=0$ if $n+m\geqq p$. We consider ${}^nf*f_1*\cdots*f_m(l_1\cdots l_r)$ and proceed by induction on $n+r$. If $n+r=0$ then ${}^nf*f_1*\cdots*f_m(1)=a_1\cdots a_m$ and $m\geqq p$. By the p-nilpotence of I this is zero. Suppose the result has been proved for values less than $n+r$. Then

$$\begin{aligned}{}^nf*f_1*\cdots*f_m(l_1\cdots l_r) &= [l_r\rightharpoonup({}^nf*f_1*\cdots*f_m)](l_1\cdots l_{r-1})\\ &= {}^{n-1}f*(l_r\rightharpoonup f)*f_1*\cdots*f_m(l_1\cdots l_{r-1})\\ &\quad+\left[\sum_1^m {}^nf*f_1*\cdots*(l_r\rightharpoonup f_i)*\cdots*f_m\right](l_1\cdots l_{r-1}).\end{aligned}$$

As a function $(l_r\rightharpoonup f)$ has the form $(l_r\rightharpoonup f)(u)=u(l_ra)$ and $(l_r\rightharpoonup f_i)$ has the form $(l_r\rightharpoonup f_i)(u)=u(l_ra_i)$. Since I is a UL submodule, l_ra, $l_ra_1,\ldots,l_ra_m\in I$ and the above equation is zero by the induction.

As a consequence of ${}^nf=0$ for $n\geqq p$ it follows that $\exp f=\sum_0^{p-1}f^i/i!$.

If g denotes the function $UL\to A$, $u\to u\cdot a$ and h denotes the function $UL\to A$, $u\to -\varepsilon(u)a$ then $f=g+h$. Also, since $a\in I$ we have $0=g^p=h^p$; and thus, $\exp f=(\exp g)(\exp h)$ where $\exp g$ is defined to be $\sum_0^{p-1}g^i/i!$ and $\exp h$ is defined to be $\sum_0^{p-1}h^i/i!$. Since $a\in I$ we have $\exp a=\sum_0^{p-1}a^i/i!\in A^r$ and it follows that $\exp\delta^0(a)=D_+^0(\exp a)$. Since $A=H^0(L, A^+)+I$ any 1-coboundary in C_1 is of the form $\delta^0(a)$ for $a\in I$. Thus exp carries the 1-coboundaries of C_1 into the 1-coboundaries of $\mathrm{Reg}_+^1\,(UL, A)$.

Suppose $D_+^0(c)$ is a 1-coboundary in $\mathrm{Reg}_+^1(UL, A)$ where $c\in A^r$. By hypothesis $c=b+x$ where $b\in H^0(L, A^+)$, $x\in I$. Since $c^p=b^p+x^p=b^p$ it follows that b is invertible and letting $z=1+b^{-1}x$ we have $c=bz$, so that z is invertible. $D_+^0(c)(l_1\cdots l_n)=[(l_1\cdots l_n)\cdot(bz)]/bz=[(l_1\cdots l_n)\cdot z]/z=D_+^0(z)(l_1\cdots l_n)$. Since L generates UL it follows that $D_+^0(c)=D_+^0(z)$. Since $z-1=b^{-1}x\in I$ we have $a=\log z=\sum_1^{p-1}(-1)^{i-1}(b^{-1}x)^i/i$ is defined, $a\in I$ and $\exp a=z$. In the preceding paragraph we have shown $\exp\delta^0(a)=D_+^0(\exp a)=D_+^0(z)$. Thus exp carries the 1-coboundaries of C_1 surjectively onto the 1-coboundaries of $\mathrm{Reg}_+^1\,(UL, A)$. Since exp is an isomorphism of complexes in positive degree it carries the 1-cocycles of C_1 isomorphically onto the 1-cocycles of $\mathrm{Reg}_+^1\,(UL, A)$. Q.E.D.

EXAMPLE 4.1. Suppose L is a Lie algebra and V an L-module; hence, a UL-module. As in Example 3.2 we consider V to have trivial multiplication and let $A=k\oplus V$, V with a unit adjoined. A has a UL-module algebra structure where we define $t\cdot(\lambda, v)=(\varepsilon(t)\lambda, t\cdot v)$ for $t\in UL$, $\lambda\in k$, $v\in V$, $H^0(UL, A)\cong A^{Lr}$ which is isomorphic to the direct product of the groups k^r and the additive group V^L. Since V is a 2-nilpotent ideal ($VV=0$) and $k+V=A$ it follows from Propositions 4.2 and 4.4 that $H^1(UL, A)\cong H^1(L, A^+)$. For $q\geqq 2$ it follows from Theorem 4.3 that $H^q(UL, A)=H^q(L, A^+)$. We shall show in §6 that $H^q(L, V)$ can be recovered from $H^q(UL, A)$ as a relative cohomology group. It will be a direct summand of $H^q(UL, A)$.

5. **Comparison with Amitsur cohomology.** For a commutative algebra A we let $\bigotimes^q A^r$ denote $(\bigotimes^q A)^r$. For $i=0,\ldots,q$ there is the algebra morphism $e_i\colon \bigotimes^q A \to \bigotimes^{q+1} A$, $a_1\otimes\cdots\otimes a_q\to a_1\otimes\cdots\otimes a_i\otimes 1\otimes a_{i+1}\otimes\cdots\otimes a_q$. There is the differential $E_{q-1}\colon \bigotimes^q A^r\to\bigotimes^{q+1} A^r$, $x\to e_0(x)e_1(x)^{-1}\cdots e_q(x)^{\pm 1}$. The Amitsur complex of A is the complex $\{\bigotimes^{q+1} A^r, E_q\}_{q\geqq 0}$ and the qth homology group $\operatorname{Ker} E_q/\operatorname{Im} E_{q-1}$ is denoted $H^q(A)$, [19, p. 327]. Note, that the qth group in the Amitsur complex is $\bigotimes^{q+1} A^r$.

Let H be a cocommutative Hopf algebra and A be a commutative H-module algebra. We have a map $M\colon \bigotimes^{q+1} A\to \operatorname{Hom}(\bigotimes^q H, A)$. This is given by

$$M(a_1\otimes\cdots\otimes a_{q-1})(h_1\otimes\cdots\otimes h_q) = a_1h_1\cdot(a_2h_2\cdot(\cdots a_{q-1}h_{q-1}\cdot(a_qh_q\cdot a_{q+1})\cdots)).$$

M is an algebra morphism—because A is an H-module algebra—and induces a morphism of complexes $M^r\colon\{\bigotimes^{q+1} A^r, E_q\}\to\{\operatorname{Reg}^q(H, A), D^q\}$. We present a verification for the case $q=1$ which contains all of the aspects of the most general case.

$$\begin{aligned} M(a_1\otimes a_2)*M(b_1\otimes b_2)(h) &= \sum_{(h)}(a_1h_{(1)}\cdot a_2)(b_1h_{(2)}\cdot b_2)\\ &= \sum_{(h)} a_1b_1(h_{(1)}\cdot a_2)(h_{(2)}\cdot b_2) = a_1b_1h\cdot(a_2b_2)\\ &= M(a_1b_1\otimes a_2b_2)(h).\\ M(1\otimes 1)(h) &= 1h\cdot 1 = \varepsilon(h)\cdot 1 = \mu\varepsilon(h). \end{aligned}$$

Thus M is an algebra homomorphism.

$$\begin{aligned} \psi(I\otimes M(a_1\otimes a_2))(h_1\otimes h_2) &= h_1\cdot(a_1h_2\cdot a_2)\\ &= M(1\otimes a_1\otimes a_2)(h_1\otimes h_2) = M(e_0(a_1\otimes a_2))(h_1\otimes h_2). \end{aligned}$$

$$\begin{aligned} M(a_1\otimes a_2)m(h_1\otimes h_2) &= a_1h_1h_2\cdot a_2 = a_1h_1\cdot(1h_2\cdot a_2)\\ &= M(a_1\otimes 1\otimes a_2)(h_1\otimes h_2) = M(e_1(a_1\otimes a_2))(h_1\otimes h_2). \end{aligned}$$

$$\begin{aligned} (M(a_1\otimes a_2)\otimes\varepsilon)(h_1\otimes h_2) &= a_1h_1\cdot a_2\varepsilon(h_2) = a_1h_1\cdot(a_2h_2\cdot 1)\\ &= M(a_1\otimes a_2\otimes 1)(h_1\otimes h_2) = M(e_2(a_1\otimes a_2))(h_1\otimes h_2). \end{aligned}$$

Thus $M^r = M \mid \bigotimes^q A^r$ is a morphism of complexes. This leads to a natural map $\Omega: H^q(A) \to H^q(H, A)$ for $q \geqq 0$. In the setting of Example 3.1 this gives a map of the Amitsur cohomology of the field extension A to the Galois cohomology.

THEOREM 5.1. *If A is a field and $H^0(H, A) = k^r$—equivalently, $A^H = k$—then the morphism of complexes $M^r: \{\bigotimes^{q+1} A^r, E_q\} \to \{\mathrm{Reg}^q(H, A), D^q\}$ is injective. If in addition A is a finite extension of k and $[A:k] = \dim_k H$ then M^r is an isomorphism of complexes; thus, $\Omega: H^q(A) \to H^q(H, A)$ is an isomorphism.*

Proof. For clarity we denote the map $M: \bigotimes^{q+1} A \to \mathrm{Hom}(\bigotimes^q H, A)$ by M_q. To prove the first statement it suffices to show all M_q are injective for $q \geqq 0$. For $q = 0$ $M_0(a)(\lambda) = \lambda a$ for $\lambda \in k$, $a \in A$. Thus M_0 is injective.

We next prove M_1 is injective and then "go up" by induction. Suppose M_1 is not injective. Let $a_1 \otimes b_1 + \cdots + a_n \otimes b_n$ be a nonzero element in Ker M_1 where n is minimal. Suppose $n > 1$. Since M_1 is an algebra morphism it follows $(a_1 \otimes b_1 + \cdots + a_n \otimes b_n)(1 \otimes b_n^{-1}) \in \mathrm{Ker}\, M_1$. (By minimality of n, $b_n \neq 0$.) Thus we can assume $b_n = 1$. By minimality of n not all b_i lie in k so we can assume $b_1 \notin k$. Thus there is $h \in H$ where $h \cdot b_1 \neq \varepsilon(h) b_1$. Since $h \cdot 1 = \varepsilon(h) 1$ it follows that,

$$\begin{aligned} 0 &\neq a_1 \otimes h \cdot b_1 + \cdots + a_n \otimes h \cdot b_n - (a_1 \otimes \varepsilon(h) b_1 + \cdots + a_n \otimes \varepsilon(h) b_n) \\ &= a_1 \otimes [h - \varepsilon(h)] \cdot b_1 + \cdots + a_{n-1} \otimes [h - \varepsilon(h)] \cdot b_{n-1}. \end{aligned}$$

This is a nonzero element of shorter length and for any $g \in H$,

$$\begin{aligned} M_1\left(\sum_1^{n-1} a_i \otimes [h - \varepsilon(h)] \cdot b_i\right)(g) &= \sum_1^{n-1} a_i(g[h - \varepsilon(h)] \cdot b_i) = \sum_1^{n} a_i(g[h - \varepsilon(h)] \cdot b_i) \\ &= M_1\left(\sum_1^{n} a_i \otimes b_i\right) g[h - \varepsilon(h)] = 0. \end{aligned}$$

This contradiction implies $n = 1$. But if $a_1 \otimes b_1 \in \mathrm{Ker}\, M_1$ then $a_1 \otimes 1 \in \mathrm{Ker}\, M_1$ and $M_1(a_1 \otimes 1)$ is not zero on the unit of H. Thus M_1 is injective.

Suppose we have shown M_{q-1} is injective where $q - 1 \geqq 1$. Let $0 \neq x \in \bigotimes^{q+1} A$, we can write $x = \sum a_i \otimes x_i$ where $\{a_i\}$ is a linearly independent set of elements of A and $\{x_i\} \subset \bigotimes^q A$. Since x is nonzero some x_i is nonzero, say x_1. Note that for $h_1, \ldots, h_q \in H$,

$$\begin{aligned} M_q(x)(h_1 \otimes \cdots \otimes h_q) &= \sum_i a_i h_1 \cdot [M_{q-1}(x_i)(h_2 \otimes \cdots \otimes h_q)] \\ &= M_1\left(\sum_i a_i \otimes [M_{q-1}(x_i)(h_2 \otimes \cdots \otimes h_q)]\right)(h_1). \end{aligned}$$

By the induction there exist $h_2, \ldots, h_q \in H$ so that $M_{q-1}(x_1)(h_2 \otimes \cdots \otimes h_q) \neq 0$ and $\sum a_i \otimes [M_{q-1}(x_i)(h_2 \otimes \cdots \otimes h_q)]$ is a nonzero element of $A \otimes A$. Again by the induction there is $h_1 \in H$ where $M_q(x)(h_1 \otimes \cdots \otimes h_q) \neq 0$. This gives the injectivity.

Suppose $[A:k]=\dim_k H=n<\infty$. Then both $\bigotimes^{q+1} A$ and $\operatorname{Hom}(\bigotimes^q H, A)$ have k-dimension n^{q+1}. M_q being injective implies it is an isomorphism. This gives the last statement. Q.E.D.

If A is a Galois extension of k and $H=kG$ the group algebra of the Galois group, then all the hypotheses of Theorem 5.1 are satisfied and this shows the Amitsur cohomology agrees with the Hopf algebra cohomology (agrees with the Galois cohomology).

The next lemma allows us to apply Theorem 5.1 to a large collection of fields.

Suppose H_1 and H_2 are cocommutative Hopf algebras and A_i are commutative algebras which are H_i-module algebras for $i=1, 2$. Then $A_1 \otimes A_2$ is an $H_1 \otimes H_2$-module algebra where $(h_1 \otimes h_2)\cdot(a_1 \otimes a_2)$ is defined to be $(h_1\cdot a_1 \otimes h_2\cdot a_2)$.

LEMMA 5.2. *$(A_1 \otimes A_2)^{k\otimes H_2}=A_1 \otimes A_2^{H_2}$ and $(A_1 \otimes A_2)^{H_1\otimes H_2}=A_1^{H_1} \otimes A_2^{H_2}$.*

Proof. Let $f_h: A_2 \to A_2$, $a \to [h-\varepsilon(h)]\cdot a$ for all $h \in H_2$. Then $A_2^{H_2}=\bigcap_{h\in H_2} \operatorname{Ker} f_{h_2}$ and $(A_1 \otimes A_2)^{k\otimes H_2}=\bigcap_{h\in H_2} \operatorname{Ker}(I \otimes f_h)=\bigcap_{h\in H_2} A_1 \otimes (\operatorname{Ker} f_h)$ $=A_1 \otimes A_2^{H_2}$. This is the first result.

Similarly $(A_1 \otimes A_2)^{H_1\otimes k}=A_1^{H_1} \otimes A_2$. The second result follows from $A_1^{H_1} \otimes A_2^{H_2}\subset(A_1 \otimes A_2)^{H_1\otimes H_2}\subset(A_1 \otimes A_2)^{H_1\otimes k} \cap (A_1 \otimes A_2)^{k\otimes A_2}=A_1^{H_1} \otimes A_2^{H_2}$. Q.E.D.

EXAMPLE 5.1. Suppose A is a purely inseparable field extension of k and $A=k[x]$ where $x^{p^n} \in k$ and $x^{p^n-1} \notin k$. We define a commutative cocommutative Hopf algebra H with basis $D_0, \ldots, D_{p^n-1}$. Multiplication is given by

$$D_iD_j = \binom{i+j}{i} D_{i+j}$$

so that D_0 is the unit. The coalgebra structure is given by $\varepsilon(D_i)=1$ if $i=0$ and 0 otherwise and $\Delta(D_t)=\sum_{j=0}^{t} D_j \otimes D_{t-j}$. A is an H-module algebra where $D_i(x^j)$ is defined as $C_{j,i}\, x^{j-i}$; then $A^H=k$, [14, p. 195]. Also, $[A:k]=p^n=\dim_k H$ so that by Theorem 5.1 $H^q(H, A)=H^q(A)$ for all q.

EXAMPLE 5.2. Suppose A is a finite normal and modular extension of k, [23, §2, Definition above Corollary 8]. Then as an algebra $A\cong A_1 \otimes A_2 \otimes\cdots\otimes A_n$ where A_1 is a Galois extension of k and each A_i is an extension of k of the form in Example 5.2 for $i=2, \ldots, n$, [23, §2, Remark after Corollary 8]. Let H_1 be the Galois group algebra Hopf algebra and H_i a Hopf algebra associated as in Example 5.2, with each A_i for $i=2, \ldots, n$. Then if $H=H_1 \otimes\cdots\otimes H_n$ A is naturally an H-module algebra and by Lemma 5.2 it follows $A^H=k$. Also, $[A:k]=\dim_k H$ so that by Theorem 5.1 the Amitsur cohomology of A is the same as the cohomology $H^q(H, A)$.

6. **Relative cohomology.** Suppose A and B are commutative algebras which are H-module algebras and $f: A \to B$ is a *morphism of H-module algebras*; i.e., an algebra morphism and H-module morphism. The map $f^r: \operatorname{Reg}^q(H, A) \to \operatorname{Reg}^q(H, B)$, $g \to fg$ is a group homomorphism since f is an algebra morphism

and is a morphism of complexes since f is an H-module morphism. This gives rise to two simplicial complexes $\operatorname{Ker} f^r$ a subcomplex of $\{\operatorname{Reg}^q(H, A), D^r\}$ and $\operatorname{Coker} f^r$ a quotient complex of $\{\operatorname{Reg}^q(H, B), D^r\}$. Taking homology we have natural maps $H^q(\operatorname{Ker} f^r) \to H^q(H, A)$ and $H^q(H, B) \to H^q(\operatorname{Coker} f^r)$.

DEFINITION. When f is injective—so that A may be considered an H submodule algebra of B—the group $H^q(\operatorname{Coker} f^r)$ will be denoted $H^q(H, A \hookrightarrow B)$. When f is surjective—so that B may be considered an H quotient module algebra of A—the group $H^q(\operatorname{Ker} f)$ will be denoted $H^q(H, A \twoheadrightarrow B)$.

Suppose f is injective, Reg is a left exact functor so there is an exact sequence of complexes:

$$(*) \qquad 0 \to \{\operatorname{Reg}^q(H, A), D^r\} \xrightarrow{f^r} \{\operatorname{Reg}^q(H, B), D^r\} \to \operatorname{Coker} f^r \to 0.$$

This gives rise to the long exact cohomology sequence:

$$\begin{aligned} 0 &\to H^0(H, A) \to H^0(H, B) \to H^0(H, A \hookrightarrow B) \to H^1(H, A) \to \cdots \\ &\to H^n(H, B) \to H^n(H, A \hookrightarrow B) \to H^{n+1}(H, A) \to H^{n+1}(H, B) \to \cdots. \end{aligned}$$

In addition suppose there is an H-module algebra morphism $g: B \to A$ such that $gf = I_A$. In other words $B = f(A) \oplus \operatorname{Ker} g$. Then the exact sequence (*) splits, the splitting induced by g^r. The morphisms f and g give rise to the relative cohomology groups $H^q(H, A \hookrightarrow B)$, $H^q(H, B \twoheadrightarrow A)$ respectively. The splitting implies these groups are naturally isomorphic and for all q,

$$H^q(H, B) = H^q(H, A) \oplus H^q(H, A \hookrightarrow B).$$

In the notation of Example 3.2 and for $q \geqq 0$ we have the commutative diagram,

$$\begin{array}{ccccc} 0 & \longrightarrow & H^q(kG, k) & \longrightarrow & H^q(kG, A) \\ & & \downarrow & & \downarrow \\ 0 & \longrightarrow & H^q(G, k^r) & \longrightarrow & H^q(G, A^r), \end{array}$$

where the vertical maps are isomorphisms and the horizontal sequences exact. $H^q(G, A^r)$ is naturally isomorphic to a direct sum of (the image of) $H^q(G, k^r)$ and $H^q(G, V)$. Thus $H^q(G, V)$ is naturally isomorphic to $H^q(kG, k \hookrightarrow A)$ and $H^q(kG, A \twoheadrightarrow k)$.

Similar reasoning applied to Example 4.1 shows that $H^q(L, V)$ is naturally isomorphic to $H^q(UL, k \hookrightarrow A)$ and $H^q(UL, A \twoheadrightarrow k)$ for $q \geqq 1$.

Next we consider the situation $f: A \to B$ is surjective. Since $\operatorname{Reg}^q(H, *)$ is not generally right exact, we have no long exact sequence but only the natural morphism $H^q(H, A \twoheadrightarrow B) \to H^q(H, A)$, for all q. We discuss two situations where exact sequences arise.

LEMMA 6.1. *If $f: A \to B$ is a surjective algebra morphism whose kernel consists of nilpotent elements, then $f^r: \operatorname{Reg}^q(H, A) \to \operatorname{Reg}^q(H, B)$ is surjective for all q.*

Proof. It suffices to prove that f^r: $\mathrm{Reg}^1(H, A) \to \mathrm{Reg}^1(H, B)$ is surjective since $\mathrm{Reg}^q(H, *) = \mathrm{Reg}^1(\bigotimes^q H, *)$ for $q \geqq 0$. Let $w \in \mathrm{Reg}^1(H, B)$. We can find $u, v \in \mathrm{Hom}(H, A)$ satisfying $fu = w$ and $fv = w^{-1}$. We shall show that $u \in \mathrm{Reg}^1(H, A)$ and be done.

$f(u * v) = (fu) * (fv) = w * w^{-1} = \mu_B \varepsilon$, the unit. Thus $u * v = \mu_A \varepsilon - x$ for some $x \in \mathrm{Hom}(H, A)$ where $fx = 0$ and hence $\mathrm{Im}\, x \subset \mathrm{Ker}\, f$. To prove u is invertible it suffices to show that $\mu_A \varepsilon - x$ is invertible. Let $h \in H$, by [16, Proposition 2.5] there is a finite dimensional coalgebra $C \subset H$ where $h \in C$. The space $x(C)$ is a finite dimensional subspace of $\mathrm{Ker}\, f$ so that there is large N where $x(C)^N = x(C) \cdots x(C) = 0$. Then for $m \geqq N$, $x^m(h) = \sum_{(h)} x(h_{(1)}) \cdots x(h_{(m)}) \in x(C)^m = 0$. This shows that $\mu_A \varepsilon + x + x^2 + x^3 + \cdots$ is a well defined element of $\mathrm{Hom}(H, A)$ and this element is the inverse—with respect to convolution—of $\mu_A \varepsilon - x$. Q.E.D.

As a result of Lemma 6.1 if f satisfies the hypothesis, there is a short exact sequence of complexes,

$$0 \to \mathrm{Ker}\, f^r \to \{\mathrm{Reg}^q(H, A), D^r\} \to \{\mathrm{Reg}^q(H, B), D^r\} \to 0,$$

which gives rise to the long exact sequence,

$$\begin{aligned} 0 &\to H^0(H, A \twoheadrightarrow B) \to H^0(H, A) \to H^0(H, B) \to H^1(H, A \twoheadrightarrow B) \to \cdots \\ &\to H^n(H, A) \to H^n(H, B) \to H^{n+1}(H, A \twoheadrightarrow B) \to H^{n+1}(H, A) \to \cdots. \end{aligned}$$

We now consider another situation leading to a long exact sequence. This time we put a restriction on H.

Definition. A cocommutative coalgebra is called *connected* if it has a unique minimal nonzero subcoalgebra, which is 1-dimensional. A Hopf algebra is called connected if the underlying coalgebra is connected. In this case $k1$ is the unique minimal subcoalgebra.

Such Hopf algebras are studied in [22]. The universal enveloping algebra of a Lie algebra and the restricted universal enveloping algebra of a restricted Lie algebra are connected Hopf algebras. The tensor product of connected Hopf algebras is again connected. This follows from the coalgebra considerations in [10, §3].

Lemma 6.2. *If H is a connected Hopf algebra then the functor* $\mathrm{Reg}^q_+(H, *)$ *is right exact for* $q \geqq 1$.

Proof. Suppose f: $\tilde{B} \to B$ is a surjective algebra morphism and $g \in \mathrm{Reg}^q_+(H, B)$. If $I = \mathrm{Ker}\, f$ we can find a linear complement V to I where $1 \in V$. Thus $\tilde{B} = I \oplus V$ and $f|V$: $V \to B$ is a linear isomorphism where $(f|V)(1) = 1$. Let η: $B \to V$ be the inverse linear isomorphism and let e be the composite $B \xrightarrow{\eta} V \to A$. Then $\tilde{g} = eg \in \mathrm{Hom}(\bigotimes^q H, \tilde{B})$, $f\tilde{g} = g$ and $\tilde{g}(h_1 \otimes \cdots \otimes h_q) = \mu_{\tilde{B}} \varepsilon(h_1 \cdots h_q)$ if any $h_i \in k$. Thus we are done when we show that $\tilde{g}$ is invertible in $\mathrm{Hom}(\bigotimes^q H, B)$. This follows from the next lemma, since the tensor product of connected Hopf algebras is connected.

LEMMA 6.3. *Let C be a connected coalgebra with C_0 being the unique minimal 1-dimensional subcoalgebra. Let D be an arbitrary algebra—not necessarily commutative. If $h \in \mathrm{Hom}(C, D)$ and h carries the nonzero elements of C_0 into D^r then h is invertible; i.e., $h \in \mathrm{Reg}(C, D)$.*

Proof. The following proof is a generalization to ungraded coalgebras of [18, p. 259, Proposition 8.2]. By [22, §1], C has a filtration by subcoalgebras $C_0 \subset C_1 \subset \cdots$ where $C = \bigcup C_i$ and $\Delta(C_n) \subset \sum_0^n C_i \otimes C_{n-i}$. C_0 contains a unique element g where $\varepsilon(g) = 1$ and $\Delta(g) = g \otimes g$. One can deduce that if $x \in C_n$ and $n > 0$ then

$$\Delta(x) = g \otimes x + x \otimes g + Y, \quad \text{where } Y \in C_{n-1} \otimes C_{n-1}. \tag{1}$$

We define the left inverse to h by induction on the filtration. Define $h^{-1}(g) = (h(g))^{-1}$. Suppose h^{-1} has been defined on C_{n-1} for $n-1 \geqq 0$, let $x \in C_n$. We diagonalize x as in (1) and define $h^{-1}(x)$ to be

$$[\varepsilon(x) - h^{-1}(g)h(x) - m_D(h^{-1} \otimes h)(Y)](h(g))^{-1}. \tag{2}$$

Then we automatically have $h^{-1} * h(x) = \varepsilon(x)$. Thus h^{-1} is defined on C_n and by induction we have h^{-1} defined on C, a left inverse to h. Similarly h has a right inverse; thus, the two inverses are equal and h is invertible. Q.E.D.

We shall use this lemma again in later sections.

If $f: A \to B$ is surjective then the morphism of complexes $f_+^r: \mathrm{Reg}_+^q(H, A) \to \mathrm{Reg}_+^q(H, B)$ is surjective in positive degree. The kernel is denoted $\mathrm{Ker} f_+^r$ and the homology of $\mathrm{Ker} f_+^r$ is denoted $H_+^q(H, A \twoheadrightarrow B)$. By Lemma 6.2 we have the short exact sequence of complexes in positive degree

$$0 \to \mathrm{Ker} f_+^r \to \{\mathrm{Reg}_+^q(H, A), D_+^r\}_{q \geqq 1} \to \{\mathrm{Reg}_+^q(H, B), D_+^r\}_{q \geqq 1} \to 0,$$

which as usual gives rise to a long exact sequence,

$$\begin{aligned} 0 &\to Z_+^1(H, A \twoheadrightarrow B) \to Z_+^1(H, A) \to Z_+^1(H, B) \to H_+^2(H, A \twoheadrightarrow B) \\ &\to H^2(H, A) \to H^2(H, B) \to H_+^3(H, A \twoheadrightarrow B) \to H^3(H, A) \to \cdots \\ &\to H^n(H, B) \to H_+^{n+1}(H, A \twoheadrightarrow B) \to H^{n+1}(H, A) \to H^{n+1}(H, B) \to \cdots, \end{aligned}$$

where Z_+^1 is the group of cocycles in the indicated complex.

PROPOSITION 6.4. *The natural map of complexes $\mathrm{Ker} f_+^r \to \mathrm{Ker} f^r$ induces an injective morphism $\iota: H_+^q(H, A \twoheadrightarrow B) \to H^q(H, A \twoheadrightarrow B)$ for all q.*

Proof. For $q = 0$ ι is actually an isomorphism since $\mathrm{Reg}^0(H, *) = \mathrm{Reg}_+^0(H, *)$; this also implies ι is injective when $q = 1$.

Suppose $q \geqq 2$. There is a natural inclusion map from $Z_+^1(H, A) \to Z^1(H, A)$ which we wish to show is surjective. Say $g \in Z^1(H, A)$ then $D^1(g) = \mu(\varepsilon \otimes \varepsilon)$ which

implies $1 = D^1(g)(1 \otimes 1) = (1g(1))g^{-1}(1)g(1) = g(1)$. Thus $g \in Z^1_+(H, A)$. $\operatorname{Im} f^r$ is a subcomplex of $\{\operatorname{Reg}^q(H, B), D^r\}$. From the commutative diagram with exact rows,

$$\begin{tikzcd}
 & & & \{\operatorname{Reg}^q(H, B), D^r\} & \\
0 \arrow[r] & \operatorname{Ker} f^r \arrow[r] & \{\operatorname{Reg}^q(H, A), D^r\} \arrow[r] & \operatorname{Im} f^r \arrow[r] \arrow[u] & 0 \\
0 \arrow[r] & \operatorname{Ker} f^r_+ \arrow[r] \arrow[u] & \{\operatorname{Reg}^q_+(H, A), D^r_+\} \arrow[r] \arrow[u] & \{\operatorname{Reg}^q_+(H, B), D^r_+\} \arrow[r] \arrow[u] & 0,
\end{tikzcd}$$

we have induced a long commutative diagram with exact rows and the vertical composites identity maps,

$$\begin{tikzcd}
 & Z^1(H, A) \arrow[r] & Z^1(\operatorname{Im} f^r) \arrow[r] & H^2(H, A \twoheadrightarrow B) \arrow[r] & H^2(H, A) \arrow[r] & \cdots \\
 & Z^1_+(H, A) \arrow[r] \arrow[u] & Z^1(H, B) \arrow[r] \arrow[u] & H^2_+(H, A \twoheadrightarrow B) \arrow[r] \arrow[u] & H^2(H, A) \arrow[r] \arrow[u] & \cdots
\end{tikzcd}$$

$$\begin{tikzcd}
 & & H^n(H, B) & & & \\
\cdots \arrow[r] & H^n(H, A) \arrow[r] & H^n(\operatorname{Im} f^r) \arrow[r] \arrow[u] & H^{n+1}(H, A \twoheadrightarrow B) \arrow[r] & H^{n+1}(H, A) \arrow[r] & \cdots \\
\cdots \arrow[r] & H^n(H, A) \arrow[r] \arrow[u] & H^n(H, B) \arrow[r] \arrow[u] & H^{n+1}_+(H, A \twoheadrightarrow B) \arrow[r] \arrow[u] & H^{n+1}(H, A) \arrow[r] \arrow[u] & \cdots.
\end{tikzcd}$$

By the 5 Lemma, [6, p. 5, Proposition 1.1], it follows that $H^q_+(H, A \twoheadrightarrow B) \to H^q(H, A \twoheadrightarrow B)$ is injective for $q \geqq 2$. Q.E.D.

7. **Extensions.** Let M be a vector space and C a coalgebra. We say $\psi: M \to M \otimes C$ gives M the structure of a right C-comodule if $(I \otimes \varepsilon)\psi = I$ and $(I \otimes \Delta)\psi = (\psi \otimes I)\psi$. For example if C is a coalgebra then $\Delta: C \to C \otimes C$ gives C the structure of a right C-comodule. In keeping with our previous notation for all $m \in M$ we denote $\psi(m)$ by $\sum_{(m)} m_{(0)} \otimes m_{(1)} \in M \otimes C$. We denote $(I \otimes \Delta)\psi(m)$ by $\sum_{(m)} m_{(0)} \otimes m_{(1)} \otimes m_{(2)} \in M \otimes C \otimes C$, etc. We use the same convention as in §1 regarding n-linear maps. Thus for example $\sum_{(m)} m_{(0)}\varepsilon(m_{(1)}) = m$ and if C is cocommutative $\sum_{(m)} m_{(0)} \otimes m_{(1)} \otimes m_{(2)} = \sum_{(m)} m_{(0)} \otimes m_{(2)} \otimes m_{(1)}$.

Let A be a commutative algebra, B an arbitrary algebra which contains A, and H a cocommutative Hopf algebra for which A is an H-module algebra.

Definition. We say that an algebra homomorphism $\psi: B \to B \otimes H$ is an extension of A by H if:

(1) $A = \psi^{-1}(B \otimes 1) = \{b \in B \mid \psi(b) = b \otimes 1\}$,

(2) ψ gives B the structure of a right H-comodule (with respect to the underlying coalgebra structure of H),

(3) $ba = \sum_{(b)} (b_{(1)} \cdot a)b_{(0)}$ for all $b \in B$, $a \in A$.

Example 7.1. Let G_3 be a group. Let G_1 be an abelian group which is a G_3-module and on which G_3 operates as automorphisms. An extension of G_1 by G_3

is an exact sequence of group morphisms:

$$1 \longrightarrow G_1 \xrightarrow{g} G_2 \xrightarrow{f} G_3 \longrightarrow 1,$$

where $g(x \cdot a) = wg(a)w^{-1}$, for $a \in G_1$, $w \in G_2$, $x = f(w) \in G_3$, [6, p. 299]. By means of g we consider G_1 as a subgroup of G_2, and we consider $A = kG_1$ as a subalgebra of $B = kG_2$. Let $H = kG_3$. Since G_3 acts as automorphisms of G_1, A has induced an H-module algebra structure which extends the given action of G_3 on G_1. The map f induces a Hopf algebra morphism kf: $B \to H$, $\lambda w \to \lambda f(w)$, for $w \in G_2$, $\lambda \in k$. Let ψ: $B \to B \otimes H$ be the composite $B \xrightarrow{\Delta} B \otimes B \xrightarrow{I \otimes kf} B \otimes H$. It is easily shown that (ψ, B) is an extension of A by H.

EXAMPLE 7.2. Let L_3 be a Lie algebra. Let L_1 be an abelian Lie algebra which is an L_3-module and on which L_3 operates as derivations. An extension of L_1 by L_3 is an exact sequence of Lie algebra morphisms:

$$0 \longrightarrow L_1 \xrightarrow{g} L_2 \xrightarrow{f} L_3 \longrightarrow 0,$$

where

$$(*) \qquad g(x \cdot a) = [w, g(a)]$$

for $a \in L_1$, $w \in L_2$, $x = f(w) \in L_3$, [6, p. 304]. By means of g we consider L_1 as a sub Lie algebra of L_2, and we consider $A = UL_1$ as a subalgebra of $B = UL_2$. Let $H = UL_3$. Since L_3 acts as derivations of L_1, A has induced an H-module algebra structure which extends the given action of L_3 on L_1. The map f induces a Hopf algebra morphism $Uf : B \to H$, induced by $w \to f(w)$ for $w \in L_2$. Let ψ: $B \to B \otimes H$ be the composite $B \xrightarrow{\Delta} B \otimes B \xrightarrow{I \otimes Uf} B \otimes H$. Clearly ψ is an algebra morphism which gives B the structure of a right H-comodule. By (*), (3) is satisfied for elements in the Lie algebras. By induction one shows that (3) is satisfied for monomials of elements in the Lie algebras. Since Lie algebras generate their universal enveloping algebras, (3) is satisfied. $A \subset \psi^{-1}(B \otimes 1)$, and by an application of the Birkhoff-Witt theorem one can prove that $A = \psi^{-1}(B \otimes 1)$. Thus (ψ, B) is an extension of A by H.

EXAMPLE 7.3 THE SMASH PRODUCT. Let A be an H-module algebra. We define the algebra $A \# H$ to be $A \otimes H$ as a vector space. (We write $a \# h$ for $a \otimes h$ when thought of as an element of $A \# H$, $a \in A$, $h \in H$.) Multiplication is defined by setting

$$(a \# g)(b \# h) \equiv \sum_{(g)} a(g_{(1)} \cdot b) \# g_{(2)}h, \quad \text{for } a, b \in A,\ g, h \in H.$$

One easily checks $A \# H$ is an associative algebra with unit $1 \# 1$ and subalgebra $A \# k \cong A$. (Here and in following sections the notation $\sum_{(g)} g_{(1)} \otimes g_{(2)}$ is especially good because it makes formulas look like known formulas for groups. Thus multiplication in $A \# H$ looks like multiplication in the semidirect product of groups. A proof that multiplication is associative in the semidirect product of

groups could be changed into a proof that multiplication is associative in $A \# H$ simply by adding the summation signs and parenthesized subscripts.) $A \# H$ is called the smash product of A by H.

Let $B = A \# H$, identify A with $A \# k$ and let $\psi: B \to B \otimes H$, $a \# h \to \sum_{(h)} a \# h_{(1)} \otimes h_{(2)}$ ($\psi = I \# \Delta$). Then one can easily check that (ψ, B) is an extension of A by H.

DEFINITION. Let (ψ_i, B_i) be extensions of A by H for $i = 1, 2$ and let $T: B_1 \to B_2$. T is called a morphism of extensions if:

(1) $T(A) \subset A$ and $T|A$ considered as a map from A to A is the identity map.

(2) T is an algebra morphism.

(3) T is a morphism of H-comodules; i.e., $(T \otimes I)\psi_1 = \psi_2 T$, which is equivalent to $\psi_2 T(b) = \sum_{(b)} T(b_{(0)}) \otimes b_{(1)}$ for all $b \in B_1$. A bijective morphism of extensions is called an isomorphism of extensions. Of course the inverse map is a morphism of extensions.

In Example 7.1 (7.2) a morphism of group (Lie-algebra) extensions gives rise to an isomorphism of the associated algebra-by-Hopf algebra extensions.

We now describe the "product" of extensions. Let (ψ_i, B_i) be extensions of A by H for $i = 1, 2$. Since $(I \otimes \psi_2): B_1 \otimes B_2 \to B_1 \otimes B_2 \otimes H$ and $(I \otimes t)(\psi_1 \otimes I)$: $B_1 \otimes B_2 \to B_1 \otimes B_2 \otimes H$ are both algebra morphisms $K = \operatorname{Ker}((I \otimes t)(\psi_1 \otimes I) - (I \otimes \psi_2))$ is a subalgebra of $B_1 \otimes B_2$. One easily shows $(I \otimes \psi_2)(K) \subset K \otimes H$ by showing $([(I \otimes t)(\psi_1 \otimes I) - (I \otimes \psi_2)] \otimes I)(I \otimes \psi_2)(K) = 0$. Thus $I \otimes \psi_2$ (or $(I \otimes t) \cdot (\psi_1 \otimes I)$) induces an H-comodule structure on K. Note $A \otimes k$ and $k \otimes A$ are subalgebras of K, let V be the subspace of K, $\{a \otimes 1 - 1 \otimes a \mid a \in A\}$. Then $(I \otimes \psi_2)(V) \subset V \otimes H$. Since $(I \otimes \psi_2)$ is an algebra homomorphism, if J is the 2-sided ideal in K generated by V then $(I \otimes \psi_2)(J) \subset J \otimes H$. Thus J is a subcomodule of K and $(I \otimes \psi_2)$ induces an H-comodule structure $\psi_3: K/J \to (K/J) \otimes H$. We let B_3 denote K/J. Since J is an ideal, B_3 is an algebra and ψ_3 is an algebra morphism. Thus (ψ_3, B_3) satisfies (2) in the definition of extension.

We now assume there exist maps $P: B_1 \to A$ and $\gamma: H \to B_1$ such that

$$B_1 \to A \otimes H, b \to \sum_{(b)} P(b_{(0)}) \otimes b_{(1)} \tag{1}$$

$$A \otimes H \to B_1, a \otimes h \to a\gamma(h) \tag{2}$$

are inverse linear isomorphisms. One can deduce that γ is a morphism of right H-comodules, P is a morphism of left A-modules, $P|A = I_A$ and $P\gamma = \mu_A \varepsilon$. Such P and γ always exist for the "cleft" extensions discussed later. In fact the existence of a suitable γ implies the existence of P. We shall show that under these additional assumptions (ψ_3, B_3) is an extension.

If $B_1 \otimes B_2$ and $A \otimes B_2$ have the H-comodule structure induced by $(I \otimes \psi_2)$ then $P \otimes I: B_1 \otimes B_2 \to A \otimes B_2$ is a morphism of right H-comodules and $(P \otimes I) \mid K: K \to A \otimes B_2$ is a morphism of right H-comodules. $B_1 \otimes B_2$ has a natural left $A \otimes A$-module structure (left-multiplication in each factor) under

which K and $A \otimes B_2$ are submodules. Observe $(P \otimes I)|K$ is a morphism of left $A \otimes A$-modules. Let $M = \operatorname{Ker}(A \otimes A \xrightarrow{m} A)$; as an ideal M is generated by $\{a \otimes 1 - 1 \otimes a \mid a \in A\}$.

By (4) in the definition of an extension it follows that J, the 2-sided ideal generated by V, is equal to the right ideal generated by V and thus $J = M \cdot K$. We have $(P \otimes I)|K$ induces $\tilde{P}: K/J \to (A \otimes B_2)/M \cdot (A \otimes B_2) \cong B_2$, or $\tilde{P}: B_3 \to B_2$ and is a morphism of right H-comodules. There is a natural map $\iota: A \to B_3$, $a \to$ the coset of $(1 \otimes a)$, (or $(a \otimes 1)$). Since $P|A = I_A$ it follows that $\tilde{P}\iota = I_A$ and ι is an injective algebra morphism. We identify A with its image under ι. Then $\tilde{P}$ is also a morphism of left A-modules.

The image of the map $Q: B_2 \to B_1 \otimes B_2$, $b \to \sum_{(b)} \gamma(b_{(1)}) \otimes b_{(0)}$ lies in K because γ is a comodule morphism. Thus $\tilde{Q}$ the composite $B_2 \xrightarrow{Q} K \to K/J = B_3$ is a morphism of right H-comodules (and left A-modules). Using $P\gamma = \mu_A \varepsilon$ one easily verifies $\tilde{P}\tilde{Q} = I_{B_2}$ and using the fact the linear isomorphisms (1) and (2) are inverse one can verify with some calculation that $\tilde{Q}\tilde{P} = I_{B_3}$. This implies $A = \{b \in B_3 \mid \psi_3(b) = b \otimes 1\}$ and (ψ_3, B_3) satisfies (1) in the definition of extension.

Let $B_1 \otimes B_2$ have the comodule structure induced by $(I \otimes \psi_2)$. Then for $x \in B_1 \otimes B_2$ and $a \in A$, $x(1 \otimes a) = \sum_{(x)} (x_{(1)} \cdot a) x_{(0)}$ since B_2 is an extension and satisfies (4). This implies (ψ_3, B_3) satisfies (3) in the definition of extension; thus is an extension of A by H.

We remark that if $T: B_2 \to \tilde{B}_2$ is a morphism of extensions T induces a morphism of extensions from the product of B_1 with B_2 to the product of B_1 with $\tilde{B}_2$. If suitable P and γ exist for B_2 instead of B_1 a similar argument shows that the product of B_1 and B_2 is an extension. The product of B_1 and B_2 is naturally isomorphic as an extension to the product of B_2 and B_1.

8. **Crossed products, cleft extensions, equivalence classes and $H^2(H, A)$.** We now introduce crossed products. Suppose $\sigma: H \otimes H \to A$ where A is a commutative H-module algebra. Recall in $A \# H$ the multiplication is given by $(a \# g)(b \# h)$ $\sum_{(g)} a(g_{(1)} \cdot b) \# g_{(2)} h$. We alter this multiplication by σ which will usually be a 2-cocycle in $\operatorname{Reg}_+^{\cdot}(H, A)$.

DEFINITION. $A \#_\sigma H$ is the vector space $A \otimes H$ with multiplication defined by setting

$$(a \#_\sigma g)(b \#_\sigma h) = \sum_{(g),(h)} a(g_{(1)} \cdot b)\sigma(g_{(2)} \otimes h_{(1)}) \#_\sigma g_{(3)} h_{(2)}.$$

Note that when $\sigma = \mu_A(\varepsilon \otimes \varepsilon)$ then $A \#_\sigma H$ is precisely $A \# H$.

LEMMA 8.1. (a) *The multiplication in $A \#_\sigma H$ is associative if and only if* $[\psi(I \otimes \sigma)] * [\sigma(I \otimes m)] = [\sigma(m \otimes I)] * [\sigma \otimes \varepsilon]$.

(b) $1 \#_\sigma 1$ *is the unit in $A \#_\sigma H$ if and only if $\sigma(g \otimes h) = \mu_A \varepsilon(gh)$ whenever g or h lie in k.*

Proof. (a) Suppose $A \#_\sigma H$ is associative, let $f, g, h \in H$. Then $((1 \#_\sigma f)(1 \#_\sigma g)) \cdot (1 \#_\sigma h) = (1 \#_\sigma f)((1 \#_\sigma g)(1 \#_\sigma h))$. The left hand side equals,

$$\left(\sum_{(f),(g)} \sigma(f_{(1)} \otimes g_{(1)}) \#_\sigma f_{(2)} g_{(2)}\right)(1 \#_\sigma h)$$

$$(*) \qquad = \sum_{(f),(g),(h)} \sigma(f_{(1)} \otimes g_{(1)}) \sigma(f_{(2)} g_{(2)} \otimes h_{(1)}) \#_\sigma f_{(3)} g_{(3)} h_{(2)}$$

$$= \sum_{(f),(g),(h)} [\sigma(f_{(1)} \otimes g_{(1)}) \varepsilon(h_{(1)})][\sigma(f_{(2)} g_{(2)} \otimes h_{(2)})] \#_\sigma f_{(3)} g_{(3)} h_{(3)}.$$

Similarly the right hand side equals,

$$(**) \qquad \sum_{(f),(g),(h)} [f_{(1)} \cdot \sigma(g_{(1)} \otimes h_{(1)})][\sigma(f_{(2)} \otimes g_{(2)} h_{(2)})] \#_\sigma f_{(3)} g_{(3)} h_{(3)}.$$

Applying $I \otimes \varepsilon$ (or $I \#_\sigma \varepsilon$) to (*) and (**) and equating shows σ satisfies the identity in (a). Similar calculations which we leave to the reader show that if σ satisfies the identity in (a) then $A \#_\sigma H$ is associative.

(b) Suppose $1 \#_\sigma 1$ is the identity of $A \#_\sigma H$ and $h \in H$. Then

$$1 \#_\sigma h = (1 \#_\sigma 1)(1 \#_\sigma h) = \sum_{(h)} \sigma(1 \otimes h_{(1)}) \#_\sigma h_{(2)}.$$

Applying $I \#_\sigma \varepsilon$ shows $\mu_A \varepsilon(h) = \sigma(1 \otimes h)$. Similarly $\sigma(h \otimes 1) = \mu_A \varepsilon(h)$. Conversely, if σ satisfies the identity in (b) then one easily verifies that $1 \#_\sigma 1$ is the identity of $A \#_\sigma H$. Q.E.D.

$\psi_\sigma: A \#_\sigma H \to A \#_\sigma H \otimes H$, $a \#_\sigma h \to \sum_{(h)} a \#_\sigma h_{(1)} \otimes h_{(2)}$ gives $A \#_\sigma H$ the structure of a right H-comodule and is a morphism of multiplicative systems. We identify A with $A \#_\sigma k \subset A \#_\sigma H$. The map $(I \#_\sigma \varepsilon \otimes I)\psi_\sigma: A \#_\sigma H \to A \otimes H$, $a \#_\sigma h \to a \otimes h$ can be used to show that $A = \{b \in A \#_\sigma H \mid \psi_\sigma(b) = b \otimes 1\}$. If σ satisfies the conditions of Lemma 8.1 then $A \#_\sigma H$ satisfies conditions (1) and (2) in the definition of an extension. One easily verifies condition (3). Thus $(\psi_\sigma, A \#_\sigma H)$ is an extension of A by H. Whenever we consider $(\psi_\sigma, A \#_\sigma H)$ as an extension of A by H we always mean it has the structure just presented. Thus the copy of A in $A \#_\sigma H$—as an extension—is always $A \#_\sigma k$. We call $A \#_\sigma H$ a *crossed product* (*extension*) when σ satisfies the conditions of Lemma 8.1.

DEFINITION. A map $S \in \operatorname{End} H$ is called an *antipode* for H if S is the 2-sided inverse to $I \in \operatorname{End} H$ with respect to convolution (*).

S is necessarily unique being defined as an inverse. When such S exists H is called a Hopf algebra with antipode. H being a Hopf algebra with antipode is equivalent to $I \in \operatorname{Reg}(H, H)$.

EXAMPLE 8.1. Suppose G is a group. Then $S: kG \to kG$, $g \to g^{-1}$ is an antipode.

EXAMPLE 8.2. Suppose K is a connected Hopf algebra, (see §6). By Lemma 6.3 $I \in \operatorname{Reg}(K, K)$ so that K is a Hopf algebra with antipode. Since (restricted) universal enveloping algebras of (restricted) Lie algebras are connected they have antipodes.

In this case the antipode applied to an element of the (restricted) Lie algebra is negative-the-element.

For general Hopf algebras an antipode is an algebra antimorphism, a coalgebra antimorphism and has period 2 if the Hopf algebra is commutative or cocommutative, [10, §1, Lemma 1].

DEFINITION. An extension (ψ, B) of A by H is called *cleft* if there is a comodule morphism in $\operatorname{Reg}(H, B)$ and H has an antipode.

EXAMPLE 8.3. H is a right H-comodule and contains a copy of k and may be viewed as an extension of k by H. $I: H \to H$ is a comodule morphism which is invertible if H has an antipode. In this case H is a cleft extension of k by H.

LEMMA 8.2. *Suppose H has an antipode S, A is an H-module algebra and (ψ_i, B_i) are extensions of A by H, for $i=1, 2$.*

(a) *If $T: B_1 \to B_2$ is a morphism of extensions and (ψ_1, B_1) is cleft then so is (ψ_2, B_2).*

(b) *If $\gamma \in \operatorname{Reg}(H, B_1)$ is a comodule morphism then $\psi_1\gamma^{-1} = (\gamma^{-1} \otimes S)\Delta$.*

(c) *If $(\psi_\sigma, A \#_\sigma H)$ is a crossed product extension then the comodule morphism $\gamma_\sigma: H \to A \#_\sigma H$, $h \to 1 \#_\sigma h$ is invertible if $\sigma \in \operatorname{Reg}^2(H, A)$. The inverse is given by $h \to \sum_{(h)} \sigma^{-1}(S(h_{(1)}) \otimes h_{(2)}) \#_\sigma S(h_{(3)})$.*

(d) *S is a coalgebra morphism.*

Proof. (a) If $\gamma \in \operatorname{Reg}(H, B_1)$ is a comodule morphism then $T\gamma \in \operatorname{Reg}(H, B_2)$—has inverse $T\gamma^{-1}$—and is a comodule morphism. Thus (ψ_2, B_2) is cleft.

(b) Since γ is a comodule morphism it satisfies $\psi_1\gamma = (\gamma \otimes I)\Delta$. One easily verifies that $\psi_1\gamma$ and $\psi_1\gamma^{-1}$ are inverse in $\operatorname{Reg}(H, B \otimes H)$ as are $(\gamma \otimes I)\Delta$ and $(\gamma^{-1} \otimes S)\Delta$. By uniqueness of inverses we are done.

(c), (d) By (b) and Example 8.3 S is a coalgebra morphism. Using this fact one easily computes that the map given in (c) is the left inverse to γ_σ. Using the fact that $\sum_{(h)} h_{(1)} \cdot (S(h_{(2)}) \cdot a) = a$ for all $a \in A$, $h \in H$ and that S is a coalgebra morphism one easily computes that $H \to A \#_\sigma H$, $h \to \sum_{(h)} S(h_{(1)} \cdot \sigma^{-1}(h_{(2)} \otimes S(h_{(3)})) \#_\sigma S(h_{(4)})$ is a right inverse to γ_σ. Thus the two inverses are equal and γ_σ is invertible. Q.E.D.

LEMMA 8.3. *Let (ψ, B) be a cleft extension of A by H and $\gamma \in \operatorname{Reg}(H, B)$ a comodule morphism.*

(a) *The map*

$$A \otimes H \to B, \qquad a \otimes h \to a\gamma(h)$$

is a linear isomorphism.

(b) *If P_γ is the map $B \to B$, $b \to \sum_{(b)} b_{(0)}\gamma^{-1}(b_{(1)})$ then $\operatorname{Im} P_\gamma \subset A$ and the map*

$$B \to A \otimes H, \qquad b \to \sum_{(b)} P_\gamma(b_{(0)}) \otimes b_{(1)}$$

is the inverse isomorphism to the isomorphism given in (a).

Proof. In the proof we never need use that (ψ, B) satisfies the 3rd condition in the definition of an extension.

$$\begin{aligned}\psi P_\gamma(b) &= \psi\Big(\sum_{(b)} b_{(0)}\gamma^{-1}(b_{(1)})\Big) = \sum_{(b)} \psi(b_{(0)})\psi\gamma^{-1}(b_{(1)}) \\ &= \sum_{(b)} b_{(0)}\gamma^{-1}(b_{(2)}) \otimes b_{(1)}S(b_{(3)}) \text{ by cocommutativity} \\ &= \sum_{(b)} b_{(0)}\gamma^{-1}(b_{(1)}) \otimes 1, \quad \text{for all } b \in B.\end{aligned}$$

Thus $\operatorname{Im} P_\gamma \subset A$. Similar types of calculation show the linear maps in (a) and (b) are inverse; hence, are isomorphisms. Q.E.D.

The above lemma is similar in spirit to [18, p. 221, Proposition 2.6].

LEMMA 8.4. *Let (ψ, B) be a cleft extension of A by H and $\gamma \in \operatorname{Reg}(H, B)$ a comodule morphism.*

(a) *The image of the map $\sigma(\gamma) \equiv [m(\gamma \otimes \gamma)] * [\gamma^{-1}m]: H \otimes H \to B$ lies in A and $\sigma(\gamma)$ is a 2-cocycle in $\operatorname{Reg}^2_+(H, A)$.*

(b) *$T_\gamma: A \#_{\sigma(\gamma)} H$, $a \#_{\sigma(\gamma)} h \to a\gamma(h)$ is an isomorphism of extensions.*

Proof. The map $\sigma(\gamma)$ is given by $g \otimes h \to \sum_{(g),(h)} \gamma(g_{(1)})\gamma(h_{(1)})\gamma^{-1}(g_{(2)}h_{(2)})$. A calculation shows $\psi(\sigma(\gamma)(g \otimes h)) = [\sigma(\gamma)(g \otimes h)] \otimes 1$ which implies $\operatorname{Im}\sigma(\gamma) \subset A$.

A further calculation—involving the 3rd condition in the definition of extension—shows that T_γ is a multiplicative morphism; i.e., $T_\gamma(xy) = T_\gamma(x)T_\gamma(y)$. Lemma 8.3 implies T_γ is bijective and thus $A \#_{\sigma(\gamma)} H$ is an associative algebra with unit $1 \#_{\sigma(\gamma)} 1$. Thus $\sigma(\gamma)$ satisfies the conditions of Lemma 8.1. $\sigma(\gamma)$ has inverse $[\gamma m] * [m(\gamma^{-1} \otimes \gamma^{-1})]$. As with $\sigma(\gamma)$ one checks that $\operatorname{Im}\sigma(\gamma)^{-1} \subset A$. Now $\sigma(\gamma) \in \operatorname{Reg}^2(H, A)$ and satisfies the conditions of Lemma 8.1 is equivalent to $\sigma(\gamma)$ being a 2-cocycle in $\operatorname{Reg}^2_+(H, A)$.

We have already pointed out that T_γ is an algebra isomorphism. Clearly $T_\gamma | A = I_A$ and T_γ is a morphism of right H-comodules. Thus it is an isomorphism of extensions. Q.E.D.

LEMMA 8.5. *Let (ψ_i, B_i) be extensions of A by H for $i = 1, 2$ and let $T: B_1 \to B_2$ be a morphism of extensions. T is an isomorphism if (ψ_1, B_1) is cleft.*

Proof. Suppose (ψ_1, B_1) is cleft and $\gamma \in \operatorname{Reg}(H, B_1)$ is a comodule morphism. Then $T\gamma \in \operatorname{Reg}(H, B_2)$ is a comodule morphism and $\sigma(\gamma) = \sigma(T\gamma)$. Clearly the diagram,

$$\begin{tikzcd} A \#_{\sigma(\gamma)} H \arrow[r, "T_\gamma"] \arrow[d, "T_{T\gamma}"'] & B_1 \arrow[dl, "T"] \\ B_2 & \end{tikzcd}$$

is commutative. By Lemma 8.4 the horizontal and vertical maps are isomorphisms which imply T is an isomorphism. Q.E.D.

DEFINITION. If (ψ_i, B_i) are extensions of A by H for $i=1, 2$, we write $(\psi_1, B_1) \sim (\psi_2, B_2)$ (or simply $B_1 \sim B_2$ where ψ_1 and ψ_2 are implicit) if there is a morphism of extensions from B_1 to B_2.

By Lemma 8.5 " $\sim$ " is an equivalence relation amongst cleft extensions and by Lemma 8.4 every cleft extension " $\sim$ " a crossed product extension.

THEOREM 8.6. *If H has an antipode there is a bijective correspondence between the equivalence classes of cleft extensions of A by H and $H^2(H, A)$. The correspondence is gotten by choosing a crossed product from the equivalence class and passing to the homology class of the 2-cocycle determining the crossed product.*

Proof. As mentioned above each cleft extension " $\sim$ " a crossed product so that a crossed product lies in each equivalence class. The next lemma implies the theorem.

LEMMA 8.7. *$A \#_\sigma H \sim A \#_\tau H$ if and only if σ and τ are homologous 2-cocycles in $\mathrm{Reg}^2_+ (H, A)$; i.e., $\sigma * \tau^{-1} = D^1_+(e)$ for $e \in \mathrm{Reg}^1_+ (H, A)$.*

Proof. If $\sigma * \tau^{-1} = D^1_+(e)$ for $e \in \mathrm{Reg}^1_+ (H, A)$ we define $T: A \#_\sigma H \to A \#_\tau H$, $a \#_\sigma h \to \sum_{(h)} ae(h_{(1)}) \#_\tau h_{(2)}$. A calculation shows that this is a morphism of extensions so that $A \#_\sigma H \sim A \#_\tau H$.

Conversely, suppose $T: A \#_\sigma H \to A \#_\tau H$ is a morphism of extensions. Define $e: H \to A$ to be the composite $(I \#_\tau \varepsilon)T\gamma_\sigma$. (Recall $\gamma_\sigma: H \to A \#_\sigma H$, $h \to 1 \#_\sigma h$.) One easily checks that $T(a \#_\sigma h) = \sum_{(h)} ae(h_{(1)}) \#_\tau h_{(2)}$. Thus

$$(*)\qquad \begin{aligned} T[(1 \#_\sigma g)(1 \#_\sigma h)] &= T\Big(\sum_{(g),(h)} \sigma(g_{(1)} \otimes h_{(1)}) \#_\sigma g_{(2)}h_{(2)}\Big) \\ &= \sum_{(g),(h)} \sigma(g_{(1)} \otimes h_{(1)})e(g_{(2)}h_{(2)}) \#_\tau g_{(3)}h_{(3)}. \end{aligned}$$

$$(**)\qquad \begin{aligned} T(1 \#_\sigma g)T(1 \#_\sigma h) &= \Big(\sum_{(g)} e(g_{(1)}) \#_\tau g_{(2)}\Big)\Big(\sum_{(h)} e(h_{(1)}) \#_\tau h_{(2)}\Big) \\ &= \sum_{(g),(h)} e(g_{(1)})(g_{(2)} \cdot e(h_{(1)}))\tau(g_{(3)} \otimes h_{(2)}) \#_\tau g_{(4)}h_{(3)}. \end{aligned}$$

Equating (*) and (**) and applying $I \#_\tau \varepsilon$ implies $\sigma * [em] = [e \otimes \varepsilon] * [\psi(I \otimes e)]\tau$. Also $e(1) = 1$. Thus if we show $e \in \mathrm{Reg}\,(H, A)$ it follows $e \in \mathrm{Reg}^1_+ (H, A)$ and $D^1_+(e) = \sigma * \tau^{-1}$.

Since $T(1 \#_\sigma h) = \sum_{(h)} e(h_{(1)}) \#_\tau h_{(2)}$ we have that $T\gamma_\sigma = e * \gamma_\tau$ or $[T\gamma_\sigma] * \gamma_\tau^{-1} = e$. Thus $e^{-1} = \gamma_\tau * [T\gamma_\tau^{-1}]$. A calculation shows $\psi_\tau e^{-1}(h) = h \otimes 1$ so that $\mathrm{Im}\, e^{-1} \subset A$. Q.E.D.

In §7 the product of extensions is defined. This induces a product structure on the equivalence classes of cleft extensions. One can show that the product of the extensions $A \#_\sigma H$ and $A \#_\tau H$ is isomorphic to $A \#_{\sigma * \tau} H$ so the correspondence given in Theorem 8.6 is a group isomorphism. The equivalence class of $A \# H$ corresponds to the identity of $H^2(H, A)$.

9. **The Brauer group over** k. Let H be a cocommutative Hopf algebra. An element $h \in H$ is called grouplike if $\Delta(h) = h \otimes h$ and $h \neq 0$. For such h, $\varepsilon(h) = 1$ and if H has an antipode S then $I * S = \varepsilon = S * I$ implies $S(h) = h^{-1}$. Let $G(H)$ denote the set of grouplike elements of H. If $g, h \in G(H)$ then $gh \in G(H)$; also, $1 \in G(H)$. If A is an H-module algebra the map $\pi(g)\colon A \to A$, $a \to g \cdot a$ is a homomorphism when $g \in G(H)$.

THEOREM 9.1. *Let A be a finite normal field extension of k which is an H-module algebra. If $A^H = k$, $[A:k] = \dim_k H$ and $\{\pi(g)\colon A \to A \mid g \in G(H)\}$ includes all automorphisms of A over k then $A \#_\sigma H$ is a central simple k-algebra for any 2-cocycle σ in* $\mathrm{Reg}^2_+(H, A)$. *The unit in $A \#_\sigma H$ is $1 \#_\sigma 1$, $A \#_\sigma k \cong A$ is a maximal commutative subalgebra and $A \#_\sigma H$ has splitting field A.*

Proof. Since σ is a 2-cocycle in $\mathrm{Reg}^2_+(H, A)$ it follows from Lemma 8.1 that $A \#_\sigma H$ is associative with unit $1 \#_\sigma 1$.

Since A is an H-module there is the associated representation $\pi\colon H \to \mathrm{End}\, A$. A is a left A-module under left translation which gives a representation $\iota\colon A \to \mathrm{End}\, A$. We claim $\tau\colon A \# H \to \mathrm{End}\, A$, $a \# h \to \iota(a)\pi(h)$ is an algebra isomorphism.

$$\iota(a)\pi(h)\iota(b)\pi(\tilde{h}) = \sum_{(h)} \iota(a(h_{(1)} \cdot b))\pi(h_{(2)}\tilde{h})$$

for $a, b \in A$, $h, \tilde{h} \in H$ and thus τ is an algebra morphism. Since $\dim_k A \# H = [A:k]^2 = \dim_k \mathrm{End}\, A$ it suffices to show that τ is surjective. This is implied by [14, p. 22, Theorem 2] whose hypotheses we show are satisfied. $\mathrm{Im}\, \tau$ is a subring of $\mathrm{End}\, A$ since τ is an algebra morphism. $\iota\colon A \to \mathrm{End}\, A$ gives $\mathrm{End}\, A$ a vector space structure over A, where $a \cdot f \equiv \iota(a)f$. $\mathrm{Im}\, \tau$ is a finite dimensional A subspace. Finally $\{x \in A \mid f(xy) = xf(y)$ for all $y \in A$, $f \in \mathrm{Im}\, \tau\} = k$; in fact, $\{x \in A \mid f(x) = xf(1)$ for all $f \in \mathrm{Im}\, \pi\} = k$ because $A^H = k$.

In particular $\pi\colon H \to \mathrm{End}\, A$ is an injective algebra morphism and the elements $\{\pi(g) \mid g \in G(H)\}$ are distinct homomorphisms of A which are automorphisms since A is a finite field extension. Since automorphisms of a finite field extension have finite period, if $g \in G(H)$ then $\pi(g)^n = \pi(g)^{-1}$ for some $0 < n \in Z$. Since π is injective and $G(H)$ is closed under multiplication, $g^n = g^{-1}$ and $G(H)$ is a group.

The elements $1 \#_\sigma g$ where $g \in G(H)$ have left inverse $\sigma^{-1}(g^{-1} \otimes g) \#_\sigma g^{-1}$; thus to show that $A \#_\sigma H$ is simple it suffices to show that any nonzero 2-sided ideal of $A \#_\sigma H$ contains an element of the form $1 \#_\sigma g$, for $g \in G(H)$.

$A \#_\sigma H$ has a left $A \otimes A$-module structure where $(a \otimes b) \cdot (c \#_\sigma h)$ is defined to be $(a \#_\sigma 1)(c \#_\sigma h)(b \#_\sigma 1) = \sum_{(h)} ac(h_{(1)} \cdot b) \#_\sigma h_{(2)}$, for $a, b, c \in A$, $h \in H$. Any 2-sided ideal in $A \#_\sigma H$ is an $A \otimes A$ submodule. Thus showing that the simple $A \otimes A$ submodules are of the form $A \#_\sigma kg$ for $g \in G(H)$ implies that $A \#_\sigma H$ is simple.

We consider both $A \#_\sigma H$ and $A \otimes A$ as vector spaces over A by having A act on the left factor. Then $A \otimes A$ is an A-algebra (the scalar extension of A from k to A) and $A \#_\sigma H$ is a module for $A \otimes A$ over A; that is, the elements of $A \otimes A$ act A-linearly. We have the A-linear map $\alpha\colon A \#_\sigma H \to \mathrm{Hom}_A(A \otimes A, A)$ where

$\langle \alpha(a \#_\sigma h), b \otimes c\rangle = ab(h\cdot c)$. The fact that τ is injective implies α is injective and thus by dimension α is an A-linear isomorphism. By means of α we identify $A \#_\sigma H$ with $\mathrm{Hom}_A(A \otimes A, A)$. Under this identification the given module structure on $A \#_\sigma H$ corresponds to the contragredient structure to $A \otimes A$ acting on itself by left translation. Indeed,

$$\begin{aligned}\langle (a \otimes b)\cdot(c \#_\sigma h), d \otimes e\rangle &= \sum_{(h)} \langle ac(h_{(1)}\cdot b) \#_\sigma h_{(2)}, d \otimes e\rangle \\ &= \sum_{(h)} acd(h_{(1)}\cdot b)(h_{(2)}\cdot e) = acd(h\cdot(be)) \\ &= \langle c \#_\sigma h, ad \otimes be\rangle,\end{aligned}$$

for $a, b, c, d, e \in A$, $h \in H$. Thus the simple submodules of $A \#_\sigma H$ are the annihilators (considering $A \#_\sigma H = \mathrm{Hom}_A(A \otimes A, A)$) of the maximal ideals of $A \otimes A$.

For $g \in G(H)$, $(a \otimes b)(1 \#_\sigma g) = a(g\cdot b) \#_\sigma g$ and thus $A \#_\sigma kg$ has A-dimension 1 and is a simple $A \otimes A$ submodule. By [14, p. 25, Theorem 3] $\{\pi(g) \mid g \in G(H)\}$ is k-linearly independent in End A and thus $G(H)$ is a k-linearly independent set. This implies $\{A \#_\sigma kg \mid g \in G(H)\}$ consists of distinct simple submodules. To show this set contains all the $A \otimes A$ simple submodules it suffices to show that $A \otimes A$ contains not more maximal ideals than the cardinality of $G(H)$.

Let M be a maximal ideal in $A \otimes A$ and let Ω be an algebraic closure of A. Since $A \otimes A$ is an A-algebra $(A \otimes A)/M$ is an extension field of A and there is an A-linear algebra morphism $\gamma\colon A \otimes A \to \Omega$ with kernel M. This shows that there are not more maximal ideals in $A \otimes A$ than there are A-linear algebra morphisms from $A \otimes A$ to Ω. $A \to A \otimes A$, $a \to 1 \otimes a$ induces a bijection $\mathrm{Hom}_A(A \otimes A, \Omega) \to \mathrm{Hom}(A, \Omega)$ and thus there are not more maximal ideals in $A \otimes A$ then there are k-linear algebra morphisms from A to Ω. A is a normal extension implies any algebra morphism from A to Ω has image in A and thus corresponds to an automorphism of A. By hypothesis every k-automorphism of A can be realized as $\pi(g)$ for some $g \in G(H)$. Thus $A \#_\sigma H$ is simple.

The above also implies $A \#_\sigma k$ is a maximal commutative subalgebra in $A \#_\sigma H$. Since if $N = \mathrm{Ker}(A \otimes A \xrightarrow{m} A)$ then the centralizer of $A \#_\sigma k$ in $A \#_\sigma H$ is the submodule S of $A \#_\sigma H$ on which the maximal ideal acts trivially. By the "contragredience" of the module, S is the annihilator of N (considering $A \#_\sigma H = \mathrm{Hom}_A(A \otimes A, A)$). Thus S is a simple submodule and must equal $A \#_\sigma k$ since it contains $A \#_\sigma k$.

The preceding paragraph implies that the center of $A \#_\sigma H$ lies in $A \#_\sigma k$. If $a \#_\sigma 1 \in A \#_\sigma k$ and $a \notin k$ we can choose $h \in H$ where $h\cdot a \neq \varepsilon(h)a$. Then

$$(1 \#_\sigma h)(a \#_\sigma 1) = \sum_{(h)} (h_{(1)}\cdot a) \#_\sigma h_{(2)} \quad \text{and} \quad (a \#_\sigma 1)(1 \#_\sigma h) = a \#_\sigma h.$$

Applying $I \#_\sigma \varepsilon$ to the right-hand sides yields $h\cdot a \neq \varepsilon(h)a$ and thus $a \#_\sigma 1$ does not lie in the center of $A \#_\sigma H$. Thus the center of $A \#_\sigma H$ is $k \#_\sigma k = k$.

By what we have already shown that $A \#_\sigma H$ is central simple over k with

maximal commutative subalgebra $A \#_\sigma k = A$ it follows from [4, p. 119, Proposition 7] that A is a splitting field. Q.E.D.

COROLLARY 9.2 (TO THE PROOF OF THEOREM 9.1). *Under the hypothesis of Theorem* 9.1 *except that* σ *need not be a* 2-*cocycle*, (*but still* $\sigma \in \mathrm{Reg}_+^2\ (H, A)$), *then* $A \#_\sigma H$ *is a nonassociative algebra which contains no nontrivial* 2-*sided ideals.*

Proof. As before the elements $1 \#_\sigma g$ have left inverse $\sigma^{-1}(g^{-1} \otimes g) \#_\sigma g^{-1}$ for $g \in G(H)$ and it suffices to show any nontrivial 2-sided ideal in $A \#_\sigma H$ contains $1 \#_\sigma g$ for some $g \in G(H)$. For $a, b, c \in A$, $h \in H$ we have $((a \#_\sigma 1)(c \#_\sigma h))(b \#_\sigma 1) = (a \#_\sigma 1)((c \#_\sigma h)(b \#_\sigma 1))$ and thus $A \#_\sigma H$ is an $A \otimes A$-module as before. The rest of the proof goes exactly as before. Q.E.D.

COROLLARY 9.3 (TO THE PROOF OF THEOREM 9.1). *Let* A *be a finite normal field extension of* k *which is an* H-*module algebra and assume* $A^H = k$, $[A:k] = \dim_k H$ *and* $\{\pi(g): A \to A \mid g \in G(H)\}$ *includes all automorphisms of* A *over* k. *Then the minimal nonzero subcoalgebras of* H *are of the form* kg *where* $g \in G(H)$.

Proof. Let σ be any 2-cocycle in $\mathrm{Reg}_+^2\ (H, A)$. If C is a subcoalgebra of H then $A \#_\sigma C$ is an $A \otimes A$ submodule of $A \#_\sigma H$. Thus $A \#_\sigma C$ contains $A \#_\sigma kg$ for some $g \in G(H)$ which implies $kg \subset C$. Q.E.D.

Corollary 9.3 implies that the simple subcoalgebras of H are 1-dimensional. By the remarks preceding Theorem 8 in [10, §3] it follows that $H = \bigoplus_{g \in G(H)} D_g$ where each D_g is a connected subcoalgebra of H whose grouplike element is g. If B is an algebra then $\mathrm{Hom}\,(H, B)$ is naturally isomorphic as an algebra to the direct product of $\{\mathrm{Hom}\,(D_g, B)\}_{g \in G(H)}$. Thus an element $f \in \mathrm{Hom}\,(H, B)$ is invertible if and only if $f | D_g \in \mathrm{Hom}\,(D_g, B)$ is invertible for all $g \in G(H)$. By Lemma 6.3 we have that f is invertible if and only if $f(G(H)) \subset B^r$. In the proof of Theorem 9.1 we observed $G(H)$ is a group. Thus $I \in \mathrm{Reg}\,(H, H)$ and H has an antipode.

DEFINITION. If A is a finite normal field extension of k which is an H-module algebra, $A^H = k$, $[A:k] = \dim_k H$ and $\{\pi(g): A \to A \mid g \in G(H)\}$ includes all automorphisms of A over k then we call H a Galois-Hopf algebra (G-H algebra) of the extension A over k.

In general there is not a unique G-H algebra of A over k. When A is separable and normal the G-H algebra of the extension is unique and is the group algebra of the Galois group. (In other words $H = kG(H)$.)

DEFINITION. Let B be an arbitrary algebra containing D which is an H-module algebra. We say that the action of H on D is *B-inner* if there is $f \in \mathrm{Reg}\,(H, B)$ where $h \cdot d = \sum_{(h)} f(h_{(1)})\, d f^{-1}(h_{(2)})$ for all $h \in H$, $d \in D$. We say such f gives the B-inner action.

If there were $f, g \in \mathrm{Hom}\,(H, B)$ such that $h \cdot d = \sum_{(h)} f(h_{(1)})\, d g(h_{(2)})$ then letting $d = 1$ and using $h \cdot 1 = \varepsilon(h) 1$ shows that g is a right inverse to f.

Suppose the action of H on D is B-inner and given by $f \in \mathrm{Reg}\,(H, B)$. Then

$$\sum_{(h)} (h_{(1)} \cdot d) f(h_{(2)}) = \sum_{(h)} f(h_{(1)})\, d f^{-1}(h_{(2)}) f(h_{(3)}) = f(h)\, d.$$

Conversely if $f \in \operatorname{Reg}(H, B)$ where for all $h \in H$, $d \in D$, $f(h)\, d = \sum_{h)} (h_{(1)} \cdot d) f(h_{(2)})$ then

$$h \cdot d = \sum_{(h)} (h_{(1)} \cdot d) f(h_{(2)}) f^{-1}(h_{(3)}) = \sum_{(h)} f(h_{(1)})\, d f^{-1}(h_{(2)}).$$

Note that if $g \in G(H)$ then $g \cdot d = f(g)\, d f^{-1}(g)$ and it is easily shown that $f^{-1}(g)$ is just the inverse to $f(g)$ in B^r. Thus g acts as a classical inner automorphism. If $l \in H$ and $\Delta(l) = 1 \otimes l + l \otimes 1$ then l acts as a derivation on B. One easily checks that $\varepsilon(l) = 0$ and that if $f(1) = 1$ then $f^{-1}(l) = -f(l)$. In this case $l \cdot d = f(l)\, d - d f(l)$ so that l acts as a classical inner derivation. If $1 = h_0, h_1 \cdots h_t \in H$ and $\Delta(h_n) = \sum h_i \otimes h_{n-i}$ then $f(h_n)\, d = \sum (h_i \cdot d) f(h_{n-i})$ for $n = 0, \ldots, t$. Thus f is inner in the sense of [13, p. 224].

EXAMPLE 9.1. Let A be a commutative algebra which is an H-module and let $\sigma \in \operatorname{Reg}^2_+(H, A)$. Recall we have $\gamma_\sigma: H \to A \#_\sigma H$, $h \to 1 \#_\sigma h$. For $a \in A$

$$\begin{aligned} \gamma_\sigma(h)(a \#_\sigma 1) &= (1 \#_\sigma h)(a \#_\sigma 1) = \sum_{(h)} (h_{(1)} \cdot a \#_\sigma h_{(2)}) \\ &= \sum_{(h)} (h_{(1)} \cdot a \#_\sigma 1) \gamma_\sigma(h_{(2)}). \end{aligned}$$

If we identify A with $A \#_\sigma k$ this becomes $\gamma_\sigma(h) a = \sum_{(h)} (h_{(1)} \cdot a) \gamma_\sigma(h_{(2)})$. Thus when H has an antipode the action of H on A is $A \#_\sigma H$—inner as given by γ_σ, since $\gamma_\sigma \in \operatorname{Reg}(H, A \#_\sigma H)$ by Lemma 8.2.

PROPOSITION 9.4. *Let H be a G-H algebra of the extension A over k and let $\sigma, \beta \in \operatorname{Reg}^2_+(H, A)$ be 2-cocycles. There is a homomorphism $T: A \#_\sigma H \to A \#_\beta H$ which is the identity restricted to A if and only if σ and β are homologous 2-cocycles; i.e., $\sigma * \beta^{-1} = D^1_+(e)$ for $e \in \operatorname{Reg}^1_+(H, A)$.*

Proof. By Lemma 8.7 it suffices to show that any such T is a morphism of extensions. Since T is an algebra morphism and $T|A = I_A$ it suffices to show that T is a morphism of right H-comodules.

Consider $e: H \to A \#_\beta H$, $e = (T\gamma_\sigma) * \gamma_\beta^{-1}$. We shall show $\operatorname{Im} e \subset A$ by showing $\operatorname{Im} e$ centralizes the maximal commutative subring A $(= A \#_\beta k)$. In the following computation we shall use the fact that $\sum_{(h)} \gamma_\sigma^{-1}(h_{(1)}) a \gamma_\sigma(h_{(2)}) = S(h) \cdot a$, $a \in A$ where S is the antipode for H. This can be computed directly using the expression for γ_σ^{-1} given in Lemma 8.2. For $a \in A$, $h \in H$

$$\begin{aligned} ae(h) &= \sum_{(h)} a[T\gamma_\sigma(h_{(1)})]\gamma_\beta^{-1}(h_{(2)}) \\ &= \sum_{(h)} [T(a\gamma_\sigma(h_{(1)}))]\gamma_\beta^{-1}(h_{(2)}) = \sum_{(h)} [T(\gamma_\sigma(h_{(1)}\gamma_\sigma^{-1}(h_{(2)}) a \gamma_\sigma(h_{(3)})))]\gamma_\beta^{-1}(h_{(4)}) \\ &= \sum_{(h)} [T(\gamma_\sigma(h_{(1)})[S(h_{(2)}) \cdot a])]\gamma_\beta^{-1}(h_{(3)}) = \sum_{(h)} T\gamma_\sigma(h_{(1)})[S(h_{(2)}) \cdot a]\gamma_\beta^{-1}(h_{(3)}) \\ &= \sum_{(h)} [T\gamma_\sigma(h_{(1)})]\gamma_\beta^{-1}(h_{(2)})\gamma_\beta(h_{(3)})[S(h_{(4)}) \cdot a]\gamma_\beta^{-1}(h_{(5)}) \\ &= \sum_{(h)} [T\gamma_\sigma(h_{(1)})]\gamma_\beta^{-1}(h_{(2)})[h_{(3)} \cdot [S(h_{(4)}) \cdot a]] \\ &= \sum_{(h)} T\gamma_\sigma(h_{(1)})\gamma_\beta^{-1}(h_{(2)}) a = e(h) a. \end{aligned}$$

Thus $\operatorname{Im} e \subset A$ and $T\gamma_\sigma = e * \gamma_\beta$. This implies $T(1 \#_\sigma h) = \sum_{(h)} e(h_{(1)}) \#_\beta h_{(2)}$ and thus $T(a \#_\sigma h) = \sum_{(h)} ae(h_{(1)}) \#_\beta h_{(2)}$ for all $a \in A$, $h \in H$. This implies T is a right H-comodule morphism. Q.E.D.

The next result guarantees that often an action is inner.

THEOREM 9.5. *Let H be a Hopf algebra whose simple subcoalgebras are of the form kg for $g \in G(H)$. Let B be a finite dimensional central simple k algebra which has a semisimple subalgebra D which is an H-module algebra. Then the action of H on D is B-inner. f: $H \to B$ giving the inner action can be chosen to satisfy $f(1) = 1$.*

Proof. The following proof is a generalization of the proof of [11, p. 480, Theorem 3]; thus, the theorem generalizes a result of Jacobson on inner derivations.

We consider $B \otimes H$ as a right D-module where $(a \otimes h)\, d = \sum_{(h)} a(h_{(1)} \cdot d) \otimes h_{(2)}$ and a left B-module where $a(b \otimes h) = ab \otimes h$, for $a, b \in B$, $d \in D$, $h \in H$. Thus $B \otimes H$ becomes a left $B \otimes D^*$-module where D^* is the opposite algebra to D. As follows from the standard results $B \otimes D^*$ is a semisimple algebra. Thus the submodule $B \otimes k(G(H))$ has a complement and there is a $B \otimes D^*$-module *projection* C: $B \otimes H \to B \otimes k(G(H))$.

For $g \in G(H)$ the map $D \to D$, $d \to g \cdot d$ is an automorphism of D with inverse $d \to g^{-1} \cdot d$. By [4, p. 111, Corollary] there is $N(g) \in B^r$ where $g \cdot d = N(g) d N(g)^{-1}$. We choose $N(1)$ to be equal to 1. As follows from the remarks following Corollary 9.3, the elements of $G(H)$ are linearly independent in H and thus N extends to a linear map N: $k(G(H)) \to B$. B has a natural left B-module and right D-module structure induced by multiplication and thus is naturally a left $B \otimes D^*$-module. Using the fact that $N(g)\, d = (g \cdot d) N(g)$ one easily verifies that M: $B \otimes k(G(H)) \to B$, $b \otimes g \to bN(g)$ is a morphism of $B \otimes D^*$-modules.

Let f: $H \to B$ be the composite $H \to B \otimes H \xrightarrow{MC} B$ where $h \to 1 \otimes h$ is the first map. Using the fact MC is a $B \otimes D^*$-module morphism we have for $h \in H$, $d \in D$,

$$f(h)d = (1 \otimes d^*) \cdot MC(1 \otimes h) = \sum_{(h)} MC(h_{(1)} \cdot d \otimes h_{(2)})$$
$$= \sum_{(h)} (h_{(1)} \cdot d \otimes 1^*) MC(1 \otimes h_{(2)}) = \sum_{(h)} (h_{(1)} \cdot d) f(h_{(2)}).$$

For $g \in G(H)$ we have $f(g) = MC(1 \otimes g) = N(g)$ since C is a projection. Thus $f(1) = 1$ and $f(G(H)) \subset B^r$. By the remarks following Corollary 9.3, $f(G(H)) \subset B^r$ implies that $f \in \operatorname{Reg}(H, B)$. Thus the action of H on D is B-inner and given by f. Q.E.D.

LEMMA 9.6. *Let H be a G-H algebra of the extension A over k and let B be a central simple k algebra with maximal commutative subalgebra A. Assume the action of H on A is B-inner given by $f \in \operatorname{Reg}(H, B)$ where $f(1) = 1$. If $\sigma = [m_B(f \otimes f)] * [f^{-1} m_H]$: $H \otimes H \to B$ then $\operatorname{Im} \sigma \subset A$ and σ is a 2-cocycle in $\operatorname{Reg}^2_+(H, A)$. The map T: $A \#_\sigma H \to B$, $a \#_\sigma h \to af(h)$ is an injective algebra morphism.*

Proof. We first must show that $\operatorname{Im} \sigma \subset A$. This involves much calculation.

We define $h \rightharpoonup a \equiv \sum_{(h)} f^{-1}(h_{(1)})af(h_{(2)})$ for $h \in H$, $a \in A$. Clearly $\sum_{(h)} h_{(1)} \cdot (h_{(2)} \rightharpoonup a) = a$. We must first show that $h \rightharpoonup a \in A$. If $b \in A$ then

$$\begin{aligned} b(h \rightharpoonup a) &= \sum_{(h)} bf^{-1}(h_{(1)})af(h_{(1)}) = \sum_{(h)} f^{-1}(h_{(1)})f(h_{(2)})bf^{-1}(h_{(3)})af(h_{(4)}) \\ &= \sum_{(h)} h_{(1)} \rightharpoonup ((h_{(2)} \cdot b)a) = \sum_{(h)} h_{(1)} \rightharpoonup (a(h_{(2)} \cdot b)) \\ &= \sum_{(h)} f^{-1}(h_{(1)})af(h_{(2)})bf^{-1}(h_{(3)})f(h_{(4)}) = (h \rightharpoonup a)b. \end{aligned}$$

The fact that A is a maximal commutative subalgebra now implies that $h \rightharpoonup a \in A$.

Again using the same technique if $h, \bar{h} \in H$, $a \in A$

$$\begin{aligned} a\sigma(h \otimes \bar{h}) &= \sum_{(h),(\bar{h})} af(h_{(1)})f(\bar{h}_{(1)})f^{-1}(h_{(2)}\bar{h}_{(2)}) \\ &= \sum_{(h),(\bar{h})} f(h_{(1)})(h_{(2)} \rightharpoonup a)f(\bar{h}_{(1)})f^{-1}(h_{(3)}\bar{h}_{(2)}) \\ &= \sum_{(h),(\bar{h})} f(h_{(1)})f(\bar{h}_{(1)})[\bar{h}_{(2)} \rightharpoonup (h_{(2)} \rightharpoonup a)]f^{-1}(h_{(3)}\bar{h}_{(3)}) \\ &= \sum_{(h),(\bar{h})} f(h_{(1)})f(\bar{h}_{(1)})f^{-1}(h_{(2)}\bar{h}_{(2)})(h_{(3)}\bar{h}_{(3)} \cdot [\bar{h}_{(4)} \rightharpoonup (h_{(4)} \rightharpoonup a)]) \\ &= \sum_{(h),(\bar{h})} f(h_{(1)})f(\bar{h}_{(1)})f^{-1}(h_{(2)}\bar{h}_{(2)})a. \end{aligned}$$

Thus $\operatorname{Im} \sigma \subset A$ since A is a maximal commutative subalgebra. σ has inverse $fm_H * [m_B t(f^{-1} \otimes f^{-1})]$ and a similar calculation to the above shows that $\operatorname{Im} \sigma^{-1} \subset A$. Thus $\sigma \in \operatorname{Reg}^2(H, A)$. Using $f(1)=1$ one easily verifies that $\sigma \in \operatorname{Reg}^2_+(H, A)$.

One easily checks that T is a multiplicative morphism; i.e. $T(xy)=T(x)T(y)$ for $x, y \in A \#_\sigma H$. T is not zero since $T|A=I_A$. Thus by Corollary 9.2 T is injective. Since B is associative T being injective implies $A \#_\sigma H$ is associative and thus by Lemma 8.1 (a) σ is a 2-cocycle. Q.E.D.

THEOREM 9.7. *Let H be a G-H algebra of the extension A over k. In the Brauer group over k let N be the normal subgroup consisting of the similarity classes of algebras which are split by A. There is a natural group isomorphism $N \to H^2(H, A)$.*

Proof. This proof follows the pattern found in the remarks in [11, pp. 486–487].

From each class in N choose an algebra which contains A as a maximal commutative subalgebra. Any two such representatives are isomorphic by an isomorphism leaving A fixed. By Lemma 9.6 each representative has a subalgebra isomorphic to $A \#_\sigma H$ for a 2-cocycle $\sigma \in \operatorname{Reg}^2_+(H, A)$ and the isomorphism leaves the elements of A fixed. By Theorem 9.1 $A \#_\sigma H$ has $A = A \#_\sigma k$ as maximal commutative subalgebra and thus the representative algebra is isomorphic to $A \#_\sigma H$. (This implies all the representatives have dimension $[A:k]^2$.) We map the similarity class of the representative algebra to the homology class of σ. By Proposition 9.4 this map from N to $H^2(H, A)$ is well defined and injective. Clearly it is surjective since for any 2-cocycle σ in $\operatorname{Reg}^2_+(H, A)$ the similarity class of $A \#_\sigma H$ maps to the homology class of σ.

We must show that the correspondence is a group morphism. Let σ, τ be two 2-cocycles in $\mathrm{Reg}^2_+(H, A)$. We consider $A \#_\sigma H$ as a vector space over A by $a(b \#_\sigma h) = ab \#_\sigma h$. Similarly for $A \#_\tau H$. The right translation action of $A \#_\sigma H$, $(A \#_\tau H)$, on itself is A-linear and thus $(A \#_\sigma H) \otimes_A (A \#_\tau H)$ has a natural right $(A \#_\sigma H) \otimes_k (A \#_\tau H)$-module structure. The ring of endomorphisms of $(A \#_\sigma H) \otimes_A (A \#_\tau H)$ which commutes with the action of $(A \#_\sigma H) \otimes_k (A \#_\tau H)$ is a representative—with A as maximal commutative subalgebra—of the similarity class of $(A \#_\sigma H) \otimes_k (A \#_\tau H)$, which is the product of the similarity classes of $A \#_\sigma H$ and $A \#_\tau H$. The left module action of $A \#_{\sigma * \tau} H$ on $(A \#_\sigma H) \otimes_A (A \#_\tau H)$ given by

$$(a \#_{\sigma * \tau} h) \cdot [(b \#_\sigma \bar{h}) \otimes_A (c \#_\tau \tilde{h})] = \sum_{(h)} [(a \#_\sigma h_{(1)})(b \#_\sigma \bar{h})] \otimes_A [(1 \#_\tau h_{(2)})(c \#_\tau \tilde{h})],$$

imbeds $A \#_{\sigma * \tau} H$ in the representative of the product of the similarity classes; i.e. the commuting ring of endomorphisms. Thus the product of the classes maps to the homology class of $\sigma * \tau$ which is the product of the homology class of σ with the homology class of τ. Q.E.D.

As we mentioned in Example 5.2 if A is a finite normal and modular extension of k then there exists a G-H algebra of the extension. It is shown in [23] that for any finite extension $\tilde{A}$ over k there is a unique minimal extension A over $\tilde{A}$ where A is finite normal and modular over k. Thus every central simple k algebra has a finite normal modular splitting field A over k. Thus the union of the subgroups N—as in Theorem 9.7—is the entire Brauer group over k.

Theorem 9.7 and Theorem 5.1 combine to give a group isomorphism between N and $H^2(A)$, the second Amitsur cohomology group.

Bibliography

1. H. Allen and M. Sweedler, *Forms of algebras*, (to appear).

2. S. Amitsur, *Simple algebras and cohomology groups of arbitrary fields*, Trans. Amer. Math. Soc. **90** (1959), 73–112.

3. E. Artin, C. Nesbitt and R. Thrall, *Rings with minimum condition*, Univ. of Michigan Press, Ann Arbor, Mich., 1944.

4. N. Bourbaki, *Algèbre*, Chapter 8, XXIII-Livre II, Hermann, Paris, 1958.

5. ———, *Groupes et algèbres de Lie*, Chapter 1, XXVI, Hermann, Paris, 1960.

6. H. Cartan and S. Eilenberg, *Homological algebra*, Princeton Univ. Press, Princeton, N. J., 1956.

7. A. Dold, *Homology of symmetric products and other functors*, Ann of Math. **68** (1958), 54–80.

8. S. Eilenberg and S. MacLane, *On the groups $H(\pi, n)$*. I, Ann. of Math. **58** (1953), 55–106.

9. V. Gugenheim, *On extensions of algebras, co-algebras and Hopf algebras*. I, Amer. J. Math. **84** (1962), 349–382.

10. R. Heyneman and M. Sweedler, *Affine Hopf algebras*, (to appear).

11. G. Hochschild, *Simple algebras with purely inseparable splitting fields of exponent* 1, Trans. Amer. Math. Soc. **79** (1955), 477–489.

12. N. Jacobson, *Lie algebras*, Interscience Tracts No. 10, Wiley, New York, 1962.

13. ———, *Generation of separable and central simple algebras*, J. Math. Pures Appl. Ser. 9, **36** (1957), 217–227.

14. ———, *Lectures in abstract algebra*, Vol. III, University Series, Van Nostrand, New York, 1964.

15. ———, *Abstract derivations and Lie algebras*, Trans. Amer. Math. Soc. **42** (1937), 206–224.

16. R. Larson, *Cocommutative Hopf algebras*, Canad. J. Math. **19** (1967), 350–360.

17. S. MacLane, *Homology*, Academic Press, New York, 1963.

18. J. Milnor and J. Moore, *On the structure of Hopf algebras*, Ann. of Math. (2) **81** (1965), 211–264.

19. A. Rosenberg and D. Zelinsky, *On Amitsur's complex*, Trans. Amer. Math. Soc. **97** (1960), 327–356.

20. J.-P. Serre, *Corps locaux, Université de Nancago*. VIII, Hermann, Paris, 1962.

21. M. Sweedler, *The Hopf algebra of an algebra applied to field theory*, J. Algebra (to appear).

22. ———, *Hopf algebras with one grouplike element*, Trans. Amer. Math. Soc. **127** (1967), 515–526.

23. ———, *Structure of inseparable extensions*, Ann. of Math. (to appear).

Massachusetts Institute of Technology,
Cambridge, Massachusetts