ELEMENTARY BIALGEBRA PROPERTIES OF GROUP RINGS AND ENVELOPING RINGS: AN INTRODUCTION TO HOPF ALGEBRAS

D. S. PASSMAN

Abstract. This is a slight extension of an expository paper I wrote a while ago as a supplement to my joint work with Declan Quinn on Burnside's theorem for Hopf algebras. It was never published, but may still be of interest to students and beginning researchers.

Let K be a field and let A be an algebra over K. Then the tensor product $A \otimes A = A \otimes_K A$ is also a K-algebra, and it is quite possible that there exists an algebra homomorphism $\Delta\colon A \to A \otimes A$. Such a map Δ is called a comultiplication, and the seemingly innocuous assumption on its existence provides A with a good deal of additional structure. For example, using Δ, one can define a tensor product on the collection of A-modules, and when A and Δ satisfy some rather mild axioms, then A is called a bialgebra. Classical examples of bialgebras include group rings $K[G]$ and Lie algebra enveloping rings $U(L)$. Indeed, most of this paper is devoted to a relatively self-contained study of some elementary bialgebra properties of these examples. Furthermore, Δ determines a convolution product on $\mathrm{Hom}_K(A, A)$ and this leads quite naturally to the definition of a Hopf algebra.

1. Tensor products and b-algebras

We start by reviewing some basic properties of tensor products. Let K be a field, fixed throughout this paper, and let V, W, X, Y be K-vector spaces. A map $\beta\colon V \times W \to X$ is said to be *bilinear* if

$$\beta(k_1v_1 + k_2v_2, w) = k_1\beta(v_1, w) + k_2\beta(v_2, w), \quad \text{and}$$
$$\beta(v, k_1w_1 + k_2w_2) = k_1\beta(v, w_1) + k_2\beta(v, w_2)$$

for all $v, v_1, v_2 \in V$, $w, w_1, w_2 \in W$ and $k_1, k_2 \in K$. Notice that, if $\gamma\colon X \to Y$ is a K-linear transformation, then the composite map $\gamma\beta\colon V \times W \to Y$ is also bilinear. This observation is the key to the *universal definition* of tensor product.

Let V and W be as above. Then a *tensor product* (T, θ) of V and W over K is a K-vector space T and a bilinear map $\theta\colon V \times W \to T$ such that any bilinear map from $V \times W$ factors uniquely through T. More precisely, if $\beta\colon V \times W \to X$ is bilinear, then there exists a unique linear transformation $\alpha\colon T \to X$ such that $\alpha\theta = \beta$. In other words, β is the composite map

$$V \times W \xrightarrow{\ \theta\ } T \xrightarrow{\ \alpha\ } X.$$

It is easy to prove that tensor products exist and are essentially unique. As usual, we denote the tensor product of V and W by $T = V \otimes_K W = V \otimes W$ and we let $v \otimes w$ denote the image under θ of $v \times w \in V \times W$.

2010 *Mathematics Subject Classification.* 16-02, 16S34, 16S30, 16T10.

It can be shown that $V \otimes W$ is spanned by all $v \otimes w$ with $v \in V$ and $w \in W$. Indeed, if $\{v_i \mid i \in \mathcal{I}\}$ and $\{w_j \mid j \in \mathcal{J}\}$ are bases for V and W respectively, then the set $\{v_i \otimes w_j \mid i \in \mathcal{I},\, j \in \mathcal{J}\}$ is a basis for $V \otimes W$. Alternately, every element of $V \otimes W$ is uniquely a finite sum $\sum_i v_i \otimes w'_i$ with $w'_i \in W$ and uniquely a finite sum $\sum_j v'_j \otimes w_j$ with $v'_j \in V$. As a consequence, if V' and W' are subspaces of V and W respectively, then $V' \otimes W'$ is contained naturally in $V \otimes W$. Finally, note that if $\sigma\colon V \to V''$ and $\tau\colon W \to W''$ are K-linear transformations, then they determine a K-linear transformation $\sigma \otimes \tau\colon V \otimes W \to V'' \otimes W''$ defined by $\sigma \otimes \tau\colon v \otimes w \mapsto \sigma(v) \otimes \tau(w)$. Indeed,

$$\ker(\sigma \otimes \tau) = (\ker \sigma) \otimes W + V \otimes (\ker \tau)$$

and if σ and τ are onto, then so is $\sigma \otimes \tau$. Note also that $K \otimes W \cong W$ via the maps $k \otimes w \mapsto kw$ and $w \mapsto 1 \otimes w$ for all $k \in K$ and $w \in W$.

Now suppose that A is an associative ring with 1. Then A is said to be a *K-algebra* if K is a central subring of A with the same 1. In particular, this implies that A is naturally a K-vector space. If B is a second K-algebra, then the tensor product $A \otimes B$ is, at the very least, a K-vector space. But $A \otimes B$ can be given an associative multiplication by defining $(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1a_2 \otimes b_1b_2$ for all $a_1, a_2 \in A$, $b_1, b_2 \in B$, and in this way, $A \otimes B$ becomes a K-algebra. Note that, if $\sigma\colon A \to A'$ and $\tau\colon B \to B'$ are K-algebra homomorphisms, then the map $\sigma \otimes \tau\colon A \otimes B \to A' \otimes B'$ is also a K-algebra homomorphism. Furthermore, if V and W are left modules for A and B respectively, then V and W are K-vector spaces and $V \otimes W$ becomes an $A \otimes B$-module by defining $(a \otimes b)(v \otimes w) = av \otimes bw$ for all $a \in A$, $b \in B$, $v \in V$ and $w \in W$. For convenience let us denote the *annihilator* of V in A by $\operatorname{ann}_A V = \{a \in A \mid aV = 0\}$. Then $\operatorname{ann}_A V$ is a two-sided ideal of A since it is the kernel of the algebra homomorphism $A \to \operatorname{End}_K(V)$ and we have

Lemma 1.1. *Let V be an A-module and let W be a B-module. Then*

$$\operatorname{ann}_{A\otimes B} V \otimes W = (\operatorname{ann}_A V) \otimes B + A \otimes (\operatorname{ann}_B W).$$

Proof. Write $I = \operatorname{ann}_A V$ and $J = \operatorname{ann}_B W$ and note that $I \otimes B + A \otimes J$ is the kernel of the natural algebra epimorphism $A \otimes B \to (A/I) \otimes (B/J)$. Thus, since V is a faithful A/I-module and W is a faithful B/J-module, it clearly suffice to prove that $V \otimes W$ is a faithful $(A/I) \otimes (B/J)$-module. In other words, we can now assume that $I = 0 = J$ and the goal is to show that $\operatorname{ann}_{A\otimes B} V \otimes W = 0$.

To this end, let $\gamma \in \operatorname{ann}_{A\otimes B} V \otimes W$ and write $\gamma = \sum_{i=1}^n a_i \otimes b_i$ with $a_i \in A$ and with $\{b_1, b_2, \ldots, b_n\}$ a K-linearly independent subset of B. Let $\lambda\colon V \to K$ be any K-linear functional and observe that $\lambda \otimes 1\colon V \otimes W \to K \otimes W \cong W$ given by $v \otimes w \mapsto \lambda(v)w$ is a linear transformation. Now, for all $v \in V$ and $w \in W$, we have

$$0 = \gamma(v \otimes w) = \sum_{i=1}^n a_iv \otimes b_iw$$

and hence, by applying $\lambda \otimes 1$, we conclude that

$$\sum_{i=1}^n \lambda(a_iv)b_iw = 0.$$

But, for fixed $v \in V$, this says that $\sum_1^n \lambda(a_iv)b_i \in \operatorname{ann}_B W = 0$, so since the b_i's are linearly independent, we must have $\lambda(a_iv) = 0$. Indeed, since this holds for all linear functionals λ, we have $a_i v = 0$ for all i and all $v \in V$. Thus $a_i \in \operatorname{ann}_A V = 0$ and we conclude that $\gamma = 0$ as required. □

Again, let A be a K-algebra and observe that the function $A \times A \to A$ given by $a \times b \mapsto ab$ is bilinear. Hence, the latter gives rise to the *multiplication* map $\mu\colon A \otimes A \to A$ defined by $a \otimes b \mapsto ab$. Now suppose that there exists a K-algebra homomorphism $\Delta\colon A \to A \otimes A$. Since this map is in the direction opposite to that of μ, it is appropriately called a *comultiplication* on A. The existence of such a comultiplication is the first step in the construction of a bialgebra structure on A and therefore we call such a pair (A, Δ) a *b-algebra*. This notation is nonstandard, but quite convenient for our purposes. With few exceptions, we will use Δ to denote the comultiplication of any b-algebra. The fact that $\Delta\colon A \to A \otimes A$ is a multiplicative homomorphism can be described by the commutative diagram

$$\begin{tikzcd} A \otimes A \arrow[r, "\Delta\otimes\Delta"] \arrow[d, "\mu"'] & (A \otimes A) \otimes (A \otimes A) \arrow[d, "\mu"] \\ A \arrow[r, "\Delta"'] & A \otimes A \end{tikzcd}$$

that intertwines both Δ and μ.

Observe that if C is a subalgebra of A, then C is a *b-subalgebra* if and only if, for the Δ map of A, we have $\Delta(C) \subseteq C \otimes C$. Furthermore, if A and B are b-algebras, then a *b-algebra homomorphism* $\theta\colon A \to B$ is a K-vector space homomorphism that is compatible with the two multiplications and the two comultiplications. Specifically, this means that the two diagrams

$$\begin{tikzcd} A \otimes A \arrow[r, "\theta\otimes\theta"] \arrow[d, "\mu"'] & B \otimes B \arrow[d, "\mu"] \\ A \arrow[r, "\theta"'] & B \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} A \arrow[r, "\theta"] \arrow[d, "\Delta"'] & B \arrow[d, "\Delta"] \\ A \otimes A \arrow[r, "\theta\otimes\theta"'] & B \otimes B \end{tikzcd}$$

are commutative. In the first diagram, the two composite maps from $A \otimes A$ to B are identical, and clearly this asserts that the image of a product is the product of the images and hence that θ is an algebra homomorphism. In the second diagram, the two composite maps from A to $B \otimes B$ are identical, and this is the comultiplication compatibility. We call the kernel of such a homomorphism θ a *b-ideal* of A and these are characterized as follows.

Lemma 1.2. *I is a b-ideal of the b-algebra A if and only if I is an ideal of A with $\Delta(I) \subseteq I \otimes A + A \otimes I$.*

Proof. Suppose first that I is the kernel of the map $\theta\colon A \to B$ as given above. Then certainly I is an ideal of A and since $\theta(I) = 0$, it follows from the commutative diagram that

$$\Delta(I) \subseteq \ker(\theta \otimes \theta) = I \otimes A + A \otimes I.$$

Conversely, suppose I is an ideal of A satisfying the preceding condition and let θ denote the natural algebra epimorphism $\theta\colon A \to A/I = B$. Since $\Delta(I) \subseteq \ker(\theta\otimes\theta)$, it follows that I maps to zero in the composite algebra homomorphism

$$A \xrightarrow{\Delta} A \otimes A \xrightarrow{\theta\otimes\theta} B \otimes B.$$

Thus this map factors through $B = A/I$. Specifically, this means that there exists an algebra homomorphism $\Delta' \colon B \to B \otimes B$ such that $(\theta \otimes \theta)\Delta = \Delta'\theta$. In other words, (B, Δ') is a b-algebra and θ is a b-algebra homomorphism with kernel I. $\square$

Now suppose that V and W are modules for the b-algebra A. Then $V \otimes W$ is a module for $A \otimes A$ and hence $V \otimes W$ becomes an A-module via the homomorphism $\Delta \colon A \to A \otimes A$. To be precise, the action of A on $V \otimes W$ is defined by $a(v \otimes w) = \Delta(a)(v \otimes w)$ for all $a \in A$, $v \in V$ and $w \in W$. If I is a b-ideal of A, then it is easy to see that the set of all A-modules V with $\operatorname{ann}_A V \supseteq I$ is closed under tensor product. Conversely, we have

Proposition 1.3. *Let $\mathcal{F}$ be a family of A-modules closed under tensor product. Then*

$$I = \bigcap_{V \in \mathcal{F}} \operatorname{ann}_A V$$

is a b-ideal of A.

Proof. Of course, I is an ideal of A. Now let $X = \oplus \sum_{V \in \mathcal{F}} V$ be the direct sum of the modules in $\mathcal{F}$. Then X is an A-module and $\operatorname{ann}_A X = \bigcap_{V \in \mathcal{F}} \operatorname{ann}_A V = I$. Furthermore, since $X \otimes X = \oplus \sum_{V,W \in \mathcal{F}} V \otimes W$ and since $V \otimes W \in \mathcal{F}$, it follows that I annihilates $X \otimes X$. In other words, by Lemma 1.1, we have

$$\Delta(I) \subseteq \operatorname{ann}_{A \otimes A} X \otimes X = I \otimes A + A \otimes I$$

and I is a b-ideal of A. $\square$

The assumption that $\mathcal{F}$ is closed under tensor product can be weakened somewhat in the above. Indeed, suppose that for each $V, W \in \mathcal{F}$ there exists $U \in \mathcal{F}$ with $\operatorname{ann}_A U \subseteq \operatorname{ann}_A V \otimes W$. The certainly $I \subseteq \operatorname{ann}_A U$ annihilates all $V \otimes W$, so I annihilates $X \otimes X$ and hence I is a b-ideal of A.

Our next goal is to interpret the associative law of multiplication in terms of tensor products and the multiplication map μ. To start with, if U, V and W are any K-vector spaces, then $U \otimes (V \otimes W)$ is naturally K-isomorphic to $(U \otimes V) \otimes W$ via the map $u \otimes (v \otimes w) \mapsto (u \otimes v) \otimes w$ for all $u \in U$, $v \in V$ and $w \in W$. We can therefore write multiple tensors without parentheses and in particular, $U \otimes V \otimes W$ is spanned by all triple tensors $u \otimes v \otimes w$. Now let A be a K-algebra and observe that associativity of multiplication is equivalent to the diagram

$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{\mu \otimes 1} & A \otimes A \\ {\scriptstyle 1 \otimes \mu}\big\downarrow & & \big\downarrow{\scriptstyle \mu} \\ A \otimes A & \xrightarrow[\mu]{} & A \end{array}$$

being commutative since

$$\mu(\mu \otimes 1)(a \otimes b \otimes c) = \mu(ab \otimes c) = (ab)c, \quad \text{and}$$
$$\mu(1 \otimes \mu)(a \otimes b \otimes c) = \mu(a \otimes bc) = a(bc)$$

for all $a, b, c \in A$.

In the same way, if (A, Δ) is a b-algebra, then we say that Δ is *coassociative* if the diagram

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes A \\ {\scriptstyle\Delta}\big\downarrow & & \big\downarrow{\scriptstyle 1\otimes\Delta} \\ A \otimes A & \xrightarrow[\Delta\otimes 1]{} & A \otimes A \otimes A \end{array}$$

is commutative or equivalently if $(\Delta \otimes 1)\Delta = (1 \otimes \Delta)\Delta$. If Δ is coassociative, then we usually say that A is a *coassociative b-algebra*. Note that, when this occurs then the tensor product of A-modules is also associative. Indeed, let U, V and W be A-modules and let $a \in A$. If $\Delta(a) = \sum_i b_i \otimes c_i \in A \otimes A$, then the action of a on $(U \otimes V) \otimes W$ is given by

$$\begin{aligned} a\big((u \otimes v) \otimes w\big) &= \Delta(a)\big((u \otimes v) \otimes w\big) = \sum_i b_i(u \otimes v) \otimes c_i w \\ &= \sum_i \Delta(b_i)(u \otimes v) \otimes c_i w = (\Delta \otimes 1)\Delta(a)(u \otimes v \otimes w) \end{aligned}$$

for all $u \in U$, $v \in V$ and $w \in W$. Similarly, $a \in A$ acts on $U \otimes (V \otimes W)$ by

$$a\big(u \otimes (v \otimes w)\big) = (1 \otimes \Delta)\Delta(a)(u \otimes v \otimes w)$$

and therefore coassociativity implies that these two actions are identical. In particular, the nth tensor power

$$V^{\otimes n} = V \otimes V \otimes \cdots \otimes V \quad (n \text{ times})$$

for any A-module V is well defined. Here $V^{\otimes 1} = V$ and $V^{\otimes m} \otimes V^{\otimes n} = V^{\otimes(m+n)}$ for all $m, n \geq 1$.

Corollary 1.4. *Let A be a coassociative b-algebra and let V be an A-module. If $\operatorname{ann}_A V$ contains no nonzero b-ideal, then $\mathcal{T}(V) = \oplus \sum_{n=1}^{\infty} V^{\otimes n}$ is a faithful A-module.*

Proof. Since A is coassociative, it follows that $\mathcal{F} = \{V^{\otimes n} \mid n = 1, 2, \ldots\}$ is a set of A-modules closed under tensor product. Thus, by the previous proposition,

$$I = \bigcap_{n=1}^{\infty} \operatorname{ann}_A V^{\otimes n} = \operatorname{ann}_A \mathcal{T}(V)$$

is a b-ideal of A. But $I \subseteq \operatorname{ann}_A V^{\otimes 1} = \operatorname{ann}_A V$, so the hypothesis implies that $I = 0$ and hence that $\mathcal{T}(V)$ is faithful. $\square$

Let V be a module for the associative algebra A. If J is an ideal of A contained in $\operatorname{ann}_A V$, then we can think of V as having been lifted from an A/J-module. In particular, V is faithful if and only if it is not lifted from any proper homomorphic image of A. Similarly, if A is a b-algebra, we might say that V is *b-faithful* if it is not lifted from any proper b-homomorphic image of A. In other words, V is b-faithful if and only if $\operatorname{ann}_A V$ contains no nonzero b-ideal of A. Thus Corollary 1.4 asserts that in a coassociative b-algebra, any b-faithful module V gives rise to the faithful *tensor module* $\mathcal{T}(V)$.

2. Semigroup Algebras

We now move on to consider some concrete examples. To start with, recall that a multiplicative *semigroup* G is a set having an associative multiplication and an identity element 1. Semigroups many contain a zero element $0 \neq 1$ satisfying $0g = g0 = 0$ for all $g \in G$, and for convenience we let $G^{\#} = G \setminus \{0\}$ denote the set of nonzero elements of G. Notice that the elements of any K-algebra A form a multiplicative semigroup which we denote by $\mathcal{S}(A)$. Of course, there is no reason to believe that every semigroup G is equal to some $\mathcal{S}(A)$, but it is true that each such G is a subsemigroup of some $\mathcal{S}(A)$. Indeed, an appropriate choice for A is the semigroup algebra $K[G]$.

Let K be a field and let G be a semigroup. Then the *semigroup algebra* $K[G]$ is a K-vector space with basis $G^{\#}$. In particular, each element α of $K[G]$ is a finite sum of the form $\alpha = \sum_{g \in G^{\#}} k_g g$ with $k_g \in K$. The addition in $K[G]$ is given by the vector space structure and the multiplication is defined distributively using the multiplication in G. Of course, the zero element in G, if it exists, is identified with the zero element of $K[G]$. The associativity of multiplication in G easily implies that $K[G]$ is an associative K-algebra and certainly G is a subsemigroup of $\mathcal{S}\big(K[G]\big)$. If G is a group, then $K[G]$ is called a *group algebra*. Notice that the usual polynomial ring $K[x]$ is the semigroup algebra of the infinite cyclic semigroup $X = \{1, x, x^2, \ldots\}$ and the ring $K[y, y^{-1}]$ of finite Laurent series is the group ring of the infinite cyclic group $Y = \{1, y^{\pm 1}, y^{\pm 2}, \ldots\}$.

If G and H are semigroups, then a *semigroup homomorphism* $\theta\colon G \to H$ is of course a map which preserves the multiplication. Furthermore, we insist that $\theta(1) = 1$ and $\theta(0) = 0$ if G contains a zero element. Now suppose that $\theta\colon G \to \mathcal{S}(A)$ is such a semigroup homomorphism. Then it is clear that θ extends uniquely to a K-algebra homomorphism $\theta\colon K[G] \to A$ satisfying

$$\theta\colon \sum_{g \in G^{\#}} k_g g \mapsto \sum_{g \in G^{\#}} k_g \theta(g).$$

In particular, it follows that there exists a K-algebra homomorphism $\Delta\colon K[G] \to K[G] \otimes K[G]$ defined by $\Delta(g) = g \otimes g$ for all $g \in G$. In this way, $K[G]$ becomes a b-algebra and in fact a coassociative b-algebra since

$$(1 \otimes \Delta)\Delta(g) = g \otimes g \otimes g = (\Delta \otimes 1)\Delta(g)$$

for all $g \in G$.

If (A, Δ) is an arbitrary b-algebra, then based upon the above considerations, we say that $g \in A$ is a *group-like element* if $\Delta(g) = g \otimes g$. Moreover, we let $\mathcal{G}(A)$ denote the set of all group-like elements of A.

Lemma 2.1. *Let A be a b-algebra and set $G = \mathcal{G}(A)$. Then G is a subsemigroup of $\mathcal{S}(A)$ and the elements of $G^{\#}$ are K-linearly independent. Thus the K-subalgebra of A generated by G is naturally isomorphic as a b-algebra to the semigroup algebra $K[G]$.*

Proof. Since $\Delta\colon A \to A \otimes A$ is an algebra homomorphism, it is clear that $G = \mathcal{G}(A)$ is closed under multiplication and that $0, 1 \in G$. Thus G is a subsemigroup of $\mathcal{S}(A)$. Now suppose, by way of contradiction, that $G^{\#}$ is a linearly dependent set and choose a dependence relation of minimal length. Then there exist distinct elements $g, h_1, h_2, \ldots, h_n \in G^{\#}$ with $\{h_1, h_2, \ldots, h_n\}$ linearly independent and with

$g = \sum_{i=1}^{n} k_i h_i$ for some $k_i \in K$. Applying Δ to the latter expression yields

$$\sum_{i=1}^{n} k_i(h_i \otimes h_i) = \sum_{i=1}^{n} k_i \Delta(h_i) = \Delta(g) = g \otimes g = g \otimes \sum_{i=1}^{n} k_i h_i$$

and therefore

$$\sum_{i=1}^{n} k_i(g - h_i) \otimes h_i = 0.$$

But the set $\{h_1, h_2, \dots, h_n\}$ is K-linearly independent, so it can be extended to a basis for A and thus, by uniqueness of expression, we have $k_i(g - h_i) = 0$ for all i. Since $g \neq h_i$, we conclude that $k_i = 0$ and hence that $g = 0$, a contradiction. Finally, note that the K-linear span in A of the elements of $G^{\#}$ is closed under multiplication and is therefore the subalgebra of A generated by G. The linear independence of $G^{\#}$ now implies that this subalgebra is isomorphic to $K[G]$. Indeed, since $G = \mathcal{G}(A)$, this is an isomorphism of b-algebras. □

As an immediate consequence, we have

Corollary 2.2. *If G is a semigroup, then every nonzero group-like element of $K[G]$ is contained in G.*

Proof. Let α be a nonzero group-like element of $K[G]$ and write $\alpha = \sum_{i=1}^{n} k_i g_i$ with the g_i distinct elements of $G^{\#}$ and with each k_i a nonzero element of K. By the preceding lemma, the nonzero group-like elements of $K[G]$ are linearly independent. Thus we must have $n = 1$, $k_1 = 1$ and $\alpha = g_1 \in G$. □

If H is a subsemigroup of G, then certainly $K[H]$ is a b-subalgebra of $K[G]$. On the other hand if $\theta\colon G \to H$ is a semigroup epimorphism, then we know that θ extends to a homomorphism $\theta\colon K[G] \to K[H]$ and the latter map is easily seen to be a b-algebra epimorphism. In particular, $I = \ker\theta$ is a b-ideal of $K[G]$. For the converse, we need

Lemma 2.3. *Let B be a b-subalgebra of A and let $\lambda\colon A \to K$ be any linear functional. If $\lambda \otimes 1\colon A \otimes A \to K \otimes A \cong A$ is defined by $\lambda \otimes 1\colon a \otimes c \mapsto \lambda(a)c$ for all $a, c \in A$, then $(\lambda \otimes 1)\Delta(B) \subseteq B$.*

Proof. Note that $\lambda \otimes 1$ is a well-defined linear transformation and hence so is the composite map $(\lambda \otimes 1)\Delta\colon A \to A$. Furthermore, since $\Delta(B) \subseteq B \otimes B$, it follows that $(\lambda \otimes 1)\Delta(B) \subseteq KB = B$. □

We can now prove

Proposition 2.4. *Let $K[G]$ be the semigroup algebra of G.*

i. If B is a b-subalgebra of the b-algebra $K[G]$, then $B = K[H]$ for some subsemigroup $H \subseteq G$.
ii. If I is a b-ideal of $K[G]$, then there is a semigroup epimorphism $\theta\colon G \to H$ with I the kernel of the extended algebra epimorphism $\theta\colon K[G] \to K[H]$.

Proof. (i) Let B be a b-subalgebra of $K[G]$ and let $H = G \cap B$. Then H is certainly a subsemigroup of G and $K[H] \subseteq B$. The goal is to show that the latter inclusion is an equality. To this end, let $\beta = \sum_g k_g g \in B$ and, for any $x \in G^{\#}$, let

$\lambda_x\colon K[G] \to K$ be the linear functional that reads off the coefficient of x. Then, using the notation of the previous lemma, we have

$$(\lambda_x \otimes 1)\Delta(\beta) = (\lambda_x \otimes 1)\Big(\sum_g k_g g \otimes g\Big) = \sum_g \lambda_x(k_g g)g = k_x x$$

and, by that lemma, we know that $(\lambda_x \otimes 1)\Delta(\beta) \in B$. In particular, if $k_x \neq 0$, then $x \in G \cap B = H$ and it follows that $\beta \in K[H]$, as required.

(ii) Now let I be a bideal of $K[G]$ and let θ be the b-algebra epimorphism $\theta\colon K[G] \to K[G]/I = C$. Then $H = \theta(G)$ is surely a subsemigroup of $\mathcal{S}(C)$ and, since θ is a b-algebra homomorphism, it is easy to see that H consists of group-like elements. In particular, we know by Lemma 2.1 that $H^\#$ is a linearly independent subset of C. Furthermore, since $G^\#$ spans $K[G]$, it follows that $H^\#$ spans C. It is now clear that $C = K[H]$ and the map $\theta\colon K[G] \to K[H]$ is the natural extension of the semigroup epimorphism $\theta\colon G \to H$. Since $I = \ker\theta$, the result follows. $\square$

By combining the previous proposition with Corollary 1.4, we obtain Steinberg's generalization of a classical result of Burnside [B, §226]. The original Burnside theorem concerned modules for the complex group algebra $\mathbb{C}[G]$ with $|G| < \infty$ and the proof used the character theory of finite groups. The argument in [St] is more transparent and, of course, it is more general. Even more general is the Hopf algebra extension given by Rieffel in [R] and also obtained later in [PQ]. The proof here is from [PQ] and shows precisely why the G-faithfulness assumption on the $K[G]$-module V is both natural and relevant.

Let G be a semigroup and let V be a $K[G]$-module. We say that G acts *faithfully* on V if for all distinct $g_1, g_2 \in G$ we have $(g_1 - g_2)V \neq 0$. Of course, if G is a group, then this condition is equivalent to $(g-1)V \neq 0$ for all $1 \neq g \in G$.

Theorem 2.5. *Let G be a semigroup and let G act faithfully on the $K[G]$-module V. Then $K[G]$ acts faithfully on the tensor module $\mathcal{T}(V) = \oplus\sum_{n=1}^{\infty} V^{\otimes n}$.*

Proof. Let I be a b-ideal contained in $\operatorname{ann}_{K[G]} V$. By Proposition 2.4(ii), there exists a semigroup epimorphism $\theta\colon G \to H$ such that I is the kernel of the corresponding algebra map $\theta\colon K[G] \to K[H]$. If $I \neq 0$, then θ cannot be one-to-one on G and hence there exist distinct $g_1, g_2 \in G$ with $\theta(g_1 - g_2) = 0$. In particular, this implies that $g_1 - g_2 \in I$, so $(g_1 - g_2)V = 0$ and this contradicts the fact that G is faithful on V. In other words, the G-faithfulness assumption implies that $\operatorname{ann}_{K[G]} V$ contains no nonzero b-ideal. Since $K[G]$ is coassociative, Corollary 1.4 now yields the result. $\square$

Finally, it is apparent that the semigroup algebra must satisfy some *universal property* with respect to G and K. Indeed, fix G and let us consider all pairs (A, θ) where A is a K-algebra and where $\theta\colon G \to \mathcal{S}(A)$ is a semigroup homomorphism. Observe that if $\sigma\colon A \to B$ is any K-algebra homomorphism, then the composite map $\sigma\theta\colon G \to \mathcal{S}(B)$ is also a semigroup homomorphism and therefore $(B, \sigma\theta)$ is an allowable pair. Based on this, it is natural to define a *universal enveloping algebra* for G to be a pair (U, θ) such that, for any other pair (B, ϕ), there exists a unique algebra homomorphism $\sigma\colon U \to B$ with $\phi = \sigma\theta$. Given such a definition, it is quite easy to prove that (U, θ) exists and that it is unique up to a suitable isomorphism.

The uniqueness part is essentially obvious. If (U, θ) and (U', θ') are two such universal enveloping algebras for G, then there exists $\sigma\colon U \to U'$ with $\theta' = \sigma\theta$ and there exists $\sigma' : U' \to U$ with $\theta = \sigma'\theta'$. Thus $\sigma'\sigma\colon U \to U$ with $\theta = (\sigma'\sigma)\theta$ and uniqueness implies that $\sigma'\sigma$ is the identity on U. Similarly, $\sigma\sigma'$ is the identity on U', so σ and σ' are the necessary isomorphisms.

For the existence, we start with the free K-algebra $F = K\langle X\rangle$, where X is a set of variables $X = \{x_g \mid g \in G\}$ indexed by the semigroup G. Next, we consider those ideals I in F such that the map $\theta\colon G \to \mathcal{S}(F/I)$ given by $\theta(g) = x_g + I$ is a semigroup homomorphism. Specifically, since $\theta(g)\theta(h) = \theta(gh)$, any such ideal I must contain all elements of the form $x_g x_h - x_{gh}$ with $g, h \in G$. Furthermore, since $\theta(1) = 1$ and $\theta(0) = 0$, if G has a zero element, we also require $1 - x_1$ and $0 - x_0$ to belong to I. In particular, if we let I_0 be the ideal of F generated by all of the above expressions, then $(F/I_0, \theta_0)$ is an allowable pair, where θ_0 is defined by $\theta_0(g) = x_g + I_0$ for all $g \in G$.

We show now that $(F/I_0, \theta_0)$ is a universal enveloping algebra for G. To this end, let (B, ϕ) be given with $\phi\colon G \to \mathcal{S}(B)$, and define the K-algebra homomorphism $\tau\colon F \to B$ by $\tau\colon x_g \mapsto \phi(g)$ for all $g \in G$. If $I = \ker\tau$, then $F/I \subseteq B$, so the map $g \mapsto \phi(g) = x_g + I$ is a semigroup homomorphism, and the comments of the previous paragraph imply that $I \supseteq I_0$. In particular, τ factors through F/I_0. In other words, there exists an algebra homomorphism $\sigma\colon F/I_0 \to B$ such that

$$\phi(g) = x_g + I = \sigma(x_g + I_0) = \sigma\theta_0(g)$$

for all $g \in G$. Furthermore, σ is uniquely determined by the equation $\phi = \sigma\theta_0$ since F/I_0 is generated as an algebra by $\theta_0(G)$.

Unfortunately, such an existence proof does not tell us much about the structure of $U_0 = F/I_0$. In particular, it does not even settle the simple question of whether the map $\theta_0\colon G \to \mathcal{S}(U_0)$ is one-to-one. But we know the answer because it is easy to see that $K[G]$, with the usual embedding of G, is a universal enveloping algebra for G. Thus, by uniqueness, $U_0 \cong K[G]$ and G does indeed embed in U_0.

3. Enveloping Algebras of Lie Algebras

Another example of interest is based on Lie algebras. Let K be a field and let L be a K-vector space. Then L is said to be a *Lie algebra* if it is endowed with a binary operation $[\,,\,]\colon L \times L \to L$ which is bilinear and satisfies both $[x, x] = 0$ for all $x \in L$ and

$$\big[[x, y], z\big] + \big[[y, z], x\big] + \big[[z, x], y\big] = 0$$

for all $x, y, z \in L$. The first condition above asserts that the *Lie product* $[\,,\,]$ is *skew-symmetric* since

$$[x, y] + [y, x] = [x + y, x + y] - [x, x] - [y, y] = 0$$

and thus $[y, x] = -[x, y]$ for all $x, y \in L$. The second axiom is a form of associativity known as the *Jacobi identity.* As usual, if L' is a subspace of L, then L' is said to be a *Lie subalgebra* if $[L', L'] \subseteq L'$. When this occurs, then certainly L' becomes a Lie algebra in its own right using the restriction of the Lie product of L. Furthermore, a map $\theta\colon L \to L''$ between two Lie algebras is a *Lie homomorphism* if θ is a K-linear transformation with $\theta([x, y]) = [\theta(x), \theta(y)]$ for all $x, y \in L$.

Now let A be an associative K-algebra and define the map $[\,,\,]\colon A \times A \to A$ by $[a, b] = ab - ba$ for all $a, b \in A$. Then it is easy to verify that $[\,,\,]$ is bilinear, skew-symmetric and satisfies the Jacobi identity. Thus, in this way, the elements of A form a Lie algebra which we denote by $\mathcal{L}(A)$. Note that if $\sigma\colon A \to B$ is an algebra homomorphism, then the same map determines a Lie homomorphism $\sigma\colon \mathcal{L}(A) \to \mathcal{L}(B)$. Of course, if L is an arbitrary Lie algebra, then there is no reason to believe that L is equal to some $\mathcal{L}(A)$. However, it is true that each such L is a Lie subalgebra of some $\mathcal{L}(A)$ and in some sense, the largest choice of A, with A generated by L, is the universal enveloping algebra $U(L)$.

The construction of $U(L)$ starts with its universal definition. Let L be a fixed Lie algebra and consider the set of all pairs (A,θ) where A is a K-algebra and where $\theta\colon L\to\mathcal{L}(A)$ is a Lie homomorphism. As usual, if $\sigma\colon A\to B$ is an algebra homomorphism, then the composite map $\sigma\theta\colon L\to\mathcal{L}(B)$ is a Lie homomorphism and hence $(B,\sigma\theta)$ is an allowable pair. A *universal enveloping algebra* for L is therefore defined to be a pair (U,θ) such that, for any other pair (B,ϕ), there exists a unique algebra homomorphism $\sigma\colon U\to B$ with $\phi=\sigma\theta$. As in the case of semigroups, it is fairly easy to prove that (U,θ) exists and that it is unique up to a suitable isomorphism. Of course, the existence proof itself does not tell us what U really looks like. In particular, without a good deal of work, it does not settle the question of whether $\theta\colon L\to\mathcal{L}(U)$ is one-to-one. In fact, θ is one-to-one, and this is the important Poincaré-Birkhoff-Witt theorem which we state below, but do not prove. See [J, §V.2] for additional details.

Theorem 3.1. *If L is a Lie algebra and if (U,θ) is a universal enveloping algebra for L, then $\theta\colon L\to\mathcal{L}(U)$ is one-to-one.*

There is one family of Lie algebras for which Theorem 3.1 follows quite easily, namely the Lie algebras that have trivial *center* $\mathbb{Z}(L)=\{x\in L\mid [x,L]=0\}$. To start with, for each $x\in L$, define the linear transformation $D(x)\colon L\to L$ by $D(x)\colon \ell\mapsto D(x)\ell=[x,\ell]$ for all $\ell\in L$. Then $D(x)$ is contained in the K-algebra $E=\operatorname{End}_K(L)$. Furthermore, for all $x,y,\ell\in L$ we have

$$\begin{aligned}[D(x),D(y)]\ell &= D(x)D(y)\ell - D(y)D(x)\ell\\ &= D(x)[y,\ell]-D(y)[x,\ell]\\ &= \big[x,[y,\ell]\big]-\big[y,[x,\ell]\big]\end{aligned}$$

where, of course, $[D(x),D(y)]$ is the Lie product in $\mathcal{L}(E)$. Thus, using skew-symmetry and the Jacobi identity, we obtain

$$\begin{aligned}[D(x),D(y)]\ell &= \big[[\ell,y],x\big]+\big[[x,\ell],y\big]\\ &= \big[[x,y],\ell\big]=D([x,y])\ell.\end{aligned}$$

In other words, $[D(x),D(y)]=D([x,y])$ and $D\colon L\to\mathcal{L}(E)$ is a Lie algebra homomorphism. Furthermore, we have $D(x)=0$ if and only if $[x,L]=0$ and therefore $\ker D=\{x\in L\mid [x,L]=0\}=\mathbb{Z}(L)$. Hence, if we assume that $\mathbb{Z}(L)=0$, then D is one-to-one. Finally, since (U,θ) is a universal enveloping algebra for L, there must exist an algebra homomorphism $\sigma\colon U\to E$ with $D=\sigma\theta$. But D is one-to-one and therefore θ must also be one-to-one.

In view of Theorem 3.1, it follows that by suitable identification, we can assume that $L\subseteq U$. In this case, we call $U=U(L)$ *the universal enveloping algebra* of L, with the understanding that $\theta\colon L\to\mathcal{L}(U)$ is the natural embedding. Notice that the universal property of $U(L)$ now asserts that if B is any K-algebra and if $\phi\colon L\to\mathcal{L}(B)$ is a Lie homomorphism, then ϕ extends uniquely to an algebra homomorphism $\phi\colon U(L)\to B$. In due time, we will determine the structure of U. For now, let us observe that since L is a Lie subalgebra of $\mathcal{L}(U)$, the Lie products of L and of $\mathcal{L}(U)$ are identical on L. Nevertheless, to avoid confusion, we will sometimes write $[\ ,\ ]_L$ for the Lie product in L. With this understanding, we have

$xy - yx = [x, y] = [x, y]_L$, for all $x, y \in L$, where xy and yx indicate multiplication in U and where $[\,,\,]$ is the Lie product in $\mathcal{L}(U)$. Furthermore, suppose U' is the K-subalgebra of U generated by L. Since any homomorphism $\sigma\colon U \to B$ restricts to a homomorphism $\sigma\colon U' \to B$, it is easy to see that U' is also a universal enveloping algebra for L. Thus, by uniqueness, U and U' are isomorphic via a K-isomorphism which is the identity on L. But U' is generated by L and hence the same must be true for U. To summarize, we have shown

Lemma 3.2. *If $U(L)$ is the universal enveloping algebra of L, then $U(L)$ is generated as a K-algebra by L and $xy - yx = [x, y]_L \in L$ for all $x, y \in L$.*

Surprisingly, without obtaining any further information on the structure of the enveloping algebra, we are still able to prove that $U(L)$ is a b-algebra. To this end, and to avoid unnecessary repetition, we first observe

Lemma 3.3. *Let A be a K-algebra and define the K-linear transformation $\delta\colon A \to A \otimes A$ by $\delta(a) = 1 \otimes a + a \otimes 1$ for all $a \in A$. Then*

$$\delta(a)\delta(b) - \delta(b)\delta(a) = \delta(ab - ba)$$

for all $a, b \in A$. Thus $\delta\colon \mathcal{L}(A) \to \mathcal{L}(A \otimes A)$ is a Lie homomorphism. Furthermore, if the field K has characteristic $p > 0$, then $\delta(a)^p = \delta(a^p)$.

Proof. This follows by direct computation. Indeed,

$$\begin{aligned}\delta(a)\delta(b) &= (1 \otimes a + a \otimes 1)(1 \otimes b + b \otimes 1)\\ &= 1 \otimes ab + ab \otimes 1 + a \otimes b + b \otimes a\end{aligned}$$

and thus

$$\begin{aligned}\delta(a)\delta(b) - \delta(b)\delta(a) &= 1 \otimes ab + ab \otimes 1 - 1 \otimes ba - ba \otimes 1\\ &= 1 \otimes (ab - ba) + (ab - ba) \otimes 1\\ &= \delta(ab - ba).\end{aligned}$$

Finally, if $\operatorname{char} K = p > 0$, then since $1 \otimes a$ and $a \otimes 1$ commute in $A \otimes A$, we have

$$\begin{aligned}\delta(a)^p = (1 \otimes a + a \otimes 1)^p &= (1 \otimes a)^p + (a \otimes 1)^p\\ &= 1 \otimes a^p + a^p \otimes 1 = \delta(a^p)\end{aligned}$$

and the lemma is proved. □

Of course, the above map δ is never an algebra homomorphism, because $\delta(1)$ is not the identity of $A \otimes A$. Nevertheless, we can use it to show

Lemma 3.4. *Let L be a Lie algebra and set $U = U(L)$. Then the map $\Delta\colon L \to U \otimes U$, given by $\Delta(x) = 1 \otimes x + x \otimes 1$ for all $x \in L$, extends to a unique algebra homomorphism $\Delta\colon U \to U \otimes U$. In this way, $U = U(L)$ becomes a coassociative b-algebra.*

Proof. It follows from the preceding two lemmas that the map $\Delta\colon L \to U \otimes U$ is a Lie homomorphism from L to $\mathcal{L}(U \otimes U)$. Thus, we conclude from the universal property of $U = U(L)$, that Δ extends to a unique algebra homomorphism $\Delta\colon U \to U \otimes U$

and therefore U is a b-algebra. Finally note that, since $\Delta(1) = 1 \otimes 1$, we have for any $x \in L$,

$$\begin{aligned}(1 \otimes \Delta)\Delta(x) &= (1 \otimes \Delta)(1 \otimes x + x \otimes 1)\\ &= 1 \otimes (1 \otimes x + x \otimes 1) + x \otimes (1 \otimes 1)\\ &= 1 \otimes 1 \otimes x + 1 \otimes x \otimes 1 + x \otimes 1 \otimes 1\end{aligned}$$

and similarly this expression is also equal to $(\Delta \otimes 1)\Delta(x)$. Thus the algebra homomorphisms $(1 \otimes \Delta)\Delta$ and $(\Delta \otimes 1)\Delta$ from U to $U \otimes U \otimes U$ agree on the generating set $L \subseteq U$ and hence they must agree on all of U. In other words, $(1 \otimes \Delta)\Delta = (\Delta \otimes 1)\Delta$ and $U(L)$ is coassociative. □

As we will see in the next section, the above b-algebra structure of $U(L)$ meshes quite nicely with the Lie algebra structure of L provided K has characteristic 0. But for fields of characteristic $p > 0$, analogous results exist only in the context of restricted Lie algebras and their restricted enveloping algebras. Fortunately, the restricted situation is close enough to the ordinary one, so that we can treat this new material in a rather cursory fashion.

Let L be a vector space over a field K of characteristic $p > 0$. Then L is a *restricted Lie algebra* if L is a Lie algebra with Lie product $[\ ,\ ]$ and if L has an additional unary operation ${}^{[p]}\colon L \to L$, the *pth power map*, which satisfies certain technical axioms (see [J, §V.7]). For example, if A is a K-algebra, then the elements of A form a restricted Lie algebra $\mathcal{L}_p(A)$ by defining $[a, b] = ab - ba$, as before, and $a^{[p]} = a^p$ for all $a, b \in A$. Of course, if L and L' are restricted Lie algebras, then a map $\theta\colon L \to L'$ is a *restricted Lie homomorphism* if it is a K-linear transformation which preserves both the Lie product and the pth power map. In other words, we must have $\theta([x, y]) = [\theta(x), \theta(y)]$ and $\theta(x^{[p]}) = \theta(x)^{[p]}$ for all $x, y \in L$.

Now fix a restricted Lie algebra L and consider all pairs (A, θ) with A a K-algebra and with $\theta\colon L \to \mathcal{L}_p(A)$ a restricted Lie homomorphism. Then the pair (U_p, θ) is said to be a *restricted universal enveloping algebra* for L, if for any other pair (B, ϕ) there exists a unique algebra homomorphism $\sigma\colon U_p \to B$ such that $\phi = \sigma\theta$. As before, (U_p, θ) exists and is unique up to an appropriate isomorphism. Furthermore, the restricted analog of the Poincaré-Birkhoff-Witt theorem exists and is a result of Jacobson (see [J, §V.8]) which we quote below, but do not prove.

Theorem 3.5. *If L is a restricted Lie algebra over a field K of characteristic $p > 0$ and if (U_p, θ) is a restricted universal enveloping algebra for L, then $\theta\colon L \to \mathcal{L}_p(U_p)$ is one-to-one.*

Thus we can assume that L is embedded in U_p and, with this understanding, we write $U_p = U_p(L)$. Note that the more standard notation is $U_p = u(L)$. In any case, the restricted analog of Lemma 3.2 is obviously

Lemma 3.6. *If $U_p(L)$ is the restricted universal enveloping algebra of L, then $U_p(L)$ is generated as a K-algebra by L. Furthermore, $xy - yx = [x, y]_L \in L$ and $x^p = x^{[p]} \in L$ for all $x, y \in L$.*

Finally, the pth power aspect of Lemma 3.3 and the proof of Lemma 3.4 yield

Lemma 3.7. *Let L be a restricted Lie algebra and set $U_p = U_p(L)$. Then the map $\Delta\colon L \to U_p \otimes U_p$, given by $\Delta(x) = 1 \otimes x + x \otimes 1$ for all $x \in L$, extends to a unique algebra homomorphism $\Delta\colon U_p \to U_p \otimes U_p$. In this way, $U_p(L)$ becomes a coassociative b-algebra.*

We now move on to study these algebras in more detail.

4. Primitive Elements

Let A be an arbitrary b-algebra with comultiplication $\Delta\colon A \to A \otimes A$. Then based on the b-algebra structures given in Lemmas 3.4 and 3.7, we say that $x \in A$ is a *primitive element* if $\Delta(x) = 1 \otimes x + x \otimes 1$. Moreover, we let $\mathcal{P}(A)$ denote the set of all primitive elements of A. Note that $\mathcal{P}(A)$ contains no nonzero group-like elements and, in particular, $1 \notin \mathcal{P}(A)$. Furthermore, it is an easy exercise to verify that if $K[G]$ is a semigroup algebra with the usual comultiplication, then $\mathcal{P}(K[G]) = 0$.

Lemma 4.1. *If A is a b-algebra over the field K, then $\mathcal{P}(A)$ is a Lie subalgebra of $\mathcal{L}(A)$. Furthermore, if $\operatorname{char} K = p > 0$, then $\mathcal{P}(A)$ is a restricted Lie subalgebra of $\mathcal{L}_p(A)$.*

Proof. Since Δ is a K-linear map, it is clear that $\mathcal{P}(A)$ is a K-subspace of A. Furthermore, using the notation of Lemma 3.3, we see that $a \in A$ is primitive if and only if $\Delta(a) = \delta(a)$. It now follows immediately from that lemma and from the fact that Δ is an algebra homomorphism that if $a, b \in \mathcal{P}(A)$, then

$$\begin{aligned}\Delta([a,b]) &= \Delta(ab - ba) = [\Delta(a), \Delta(b)] \\ &= [\delta(a), \delta(b)] = \delta([a,b]).\end{aligned}$$

Thus $[a,b] = ab - ba \in \mathcal{P}(A)$ and $\mathcal{P}(A)$ is a Lie subalgebra of $\mathcal{L}(A)$. Furthermore, if $\operatorname{char} K = p > 0$ and if $a \in \mathcal{P}(A)$, then Lemma 3.3 also implies that $a^p \in \mathcal{P}(A)$ and we conclude that $\mathcal{P}(A)$ is a restricted Lie subalgebra of $\mathcal{L}_p(A)$. $\square$

Since enveloping algebras of Lie algebras are generated by primitive elements, it is necessary for us to understand the comultiplication applied to a product of primitives. The following result is just a version of the binomial theorem. For convenience, let $\mathbb{N}$ denote the set of nonnegative integers and let $\mathbb{N}^m$ denote the set of all m-tuples over $\mathbb{N}$ with the usual componentwise addition.

Lemma 4.2. *Let (A, Δ) be a b-algebra, let $x_1, x_2, \ldots, x_m \in \mathcal{P}(A)$ and write $\mathbf{x}^{\mathbf{e}} = x_1^{e_1} x_2^{e_2} \cdots x_m^{e_m}$ where $\mathbf{e} = (e_1, e_2, \ldots, e_m) \in \mathbb{N}^m$. Then*

$$\Delta(\mathbf{x}^{\mathbf{e}}) = \sum_{\mathbf{i}+\mathbf{j}=\mathbf{e}} \binom{\mathbf{e}}{\mathbf{i}} \mathbf{x}^{\mathbf{i}} \otimes \mathbf{x}^{\mathbf{j}}$$

where $\mathbf{i} = (i_1, i_2, \ldots, i_m)$ and $\mathbf{j} = (j_1, j_2, \ldots, j_m)$ both belong to $\mathbb{N}^m$ and where

$$\binom{\mathbf{e}}{\mathbf{i}} = \binom{e_1}{i_1}\binom{e_2}{i_2} \cdots \binom{e_m}{i_m}$$

is a product of binomial coefficients.

Proof. First let $x \in \mathcal{P}(A)$ and let e be a nonnegative integer. Since $1 \otimes x$ and $x \otimes 1$ commute in $A \otimes A$, we have

$$\begin{aligned}\Delta(x^e) &= \Delta(x)^e = (1 \otimes x + x \otimes 1)^e \\ &= \sum_{i+j=e} \binom{e}{i} (1 \otimes x)^j (x \otimes 1)^i = \sum_{i+j=e} \binom{e}{i} x^i \otimes x^j.\end{aligned}$$

Thus, by again using the multiplicative property of Δ, we obtain

$$\begin{aligned}\Delta(\mathbf{x}^{\mathbf{e}}) &= \Delta(x_1^{e_1})\Delta(x_2^{e_2})\cdots\Delta(x_m^{e_m})\\ &= \prod_{k=1}^{m}\Big(\sum_{i_k+j_k=e_k}\binom{e_k}{i_k}\,x_k^{i_k}\otimes x_k^{j_k}\Big)\\ &= \sum_{\mathbf{i}+\mathbf{j}=\mathbf{e}}\binom{\mathbf{e}}{\mathbf{i}}\,\mathbf{x}^{\mathbf{i}}\otimes\mathbf{x}^{\mathbf{j}}\end{aligned}$$

where $\prod_{k=1}^{m}$ indicates the product in the natural order. □

Now let A be a K-algebra and let $\mathfrak{B}$ be a subset of A endowed with a linear ordering $\prec$. Then an *ordered monomial* in the elements of $\mathfrak{B}$ is a product

$$\eta = x_1^{e_1}x_2^{e_2}\cdots x_m^{e_m}$$

with $x_1, x_2, \ldots, x_m \in \mathfrak{B}$, $x_1 \prec x_2 \prec \cdots \prec x_m$ and $e_i \in \mathbb{N}$. If $\operatorname{char} K = p > 0$, we say that η is an *ordered p-monomial* if the preceding conditions are satisfied and if, in addition, $0 \le e_i < p$ for all i. In any case, we let $e_1 + e_2 + \cdots + e_m = \operatorname{fdeg}\eta$ be the *formal degree* of η. Of course, it is quite possible that η can be written as a different ordered monomial and have an entirely different formal degree. In other words, the formal degree really depends upon the explicit expression for η.

Lemma 4.3. *Let A be a K-algebra, let L be a Lie subalgebra of $\mathcal{L}(A)$ and let B denote the K-subalgebra of A generated by L. Choose a spanning set $\mathfrak{B}$ for L and linearly order its elements.*

i. B is spanned by the ordered monomials in the elements of $\mathfrak{B}$.
ii. If $\operatorname{char} K = p > 0$ and if L is a restricted Lie subalgebra of $\mathcal{L}_p(A)$, then B is spanned by the ordered p-monomials in the elements of $\mathfrak{B}$.

Proof. Let L^n denote the K-linear subspace of A spanned by all products of at most n elements of L. Then certainly B is the ascending union $B = \bigcup_{n=0}^{\infty} L^n$ and we show, by induction on n, that each L^n is spanned by ordered monomials of formal degree $\le n$ in the elements of $\mathfrak{B}$. Since $\mathfrak{B}$ spans L, this is certainly true for $n = 0$ and 1. Furthermore, for arbitrary n, we see that L^n is spanned by all products of at most n elements of $\mathfrak{B}$.

Assume that the inductive result holds for $n-1$ and let $\xi = y_1y_2\cdots y_n$ be a product of n elements of $\mathfrak{B}$. Since L is a Lie subalgebra of $\mathcal{L}(A)$, we know that $ab = ba + [a,b]$ for all $a, b \in L$ and that $[a,b] \in L$. It therefore follows that if ξ' is obtained from ξ by interchanging two adjacent factors, then $\xi \equiv \xi' \bmod L^{n-1}$. In particular, via a finite sequence of such interchanges, we see that $\xi \equiv \eta \bmod L^{n-1}$ where $\eta = x_1^{e_1}x_2^{e_2}\cdots x_m^{e_m}$ is an ordered monomial of formal degree n in the elements of $\mathfrak{B}$. Thus these ordered monomial span L^n modulo L^{n-1}, and the inductive result is proved.

Finally, if $\operatorname{char} K = p > 0$ and if L is a restricted Lie subalgebra of $\mathcal{L}_p(A)$, then L is closed under pth powers. In particular, if some $e_i \ge p$ in the above expression for η, then using $x_i^p \in L$, we see that $\eta \equiv 0 \bmod L^{n-1}$ and the result follows. □

Now suppose that A is a b-algebra, let $\mathfrak{B}$ be an ordered subset of $\mathcal{P}(A)$ and let

$$\eta = x_1^{e_1}x_2^{e_2}\cdots x_m^{e_m}$$

be an ordered monomial in the elements of $\mathfrak{B}$. If η is the empty word, that is if $\eta = 1$, then certainly $\Delta(\eta) = \eta\otimes 1 = 1\otimes\eta = 1\otimes 1$. On the other hand, if $\operatorname{fdeg}\eta \ge 1$, then Lemma 4.2 asserts that $\Delta(\eta)$ is an integer linear combination of tensors $\alpha\otimes\beta$ where each α and β is an ordered monomial and where $\operatorname{fdeg}\alpha + \operatorname{fdeg}\beta = \operatorname{fdeg}\eta$. Notice that the terms with $\operatorname{fdeg}\alpha = 0$ or $\operatorname{fdeg}\beta = 0$ are equal to $1\otimes\eta$ and $\eta\otimes 1$ respectively, and each occurs with coefficient 1. In addition, the $\alpha = x_i$ contribution to $\Delta(\eta)$ is equal to

$$x_i \otimes \partial_i(\eta) = x_i \otimes e_i\, x_1^{e_1}\cdots x_i^{e_i-1}\cdots x_m^{e_m},$$

where the ∂_i notation was chosen because the right-hand expression above looks so much like the partial derivative with respect to x_i. By combining all this information, we conclude that

$$(*)\qquad \Delta(\eta) = 1\otimes\eta + \eta\otimes 1 + \Big(\sum_{i=1}^{m} x_i\otimes\partial_i(\eta)\Big) + \gamma$$

where γ is an integer linear combination of tensors $\alpha\otimes\beta$ with each α and β an ordered monomial satisfying $\operatorname{fdeg}\alpha \ge 2$, $\operatorname{fdeg}\beta\ge 1$ and $\operatorname{fdeg}\alpha + \operatorname{fdeg}\beta = \operatorname{fdeg}\eta$. Of course, if $\operatorname{char} K = p > 0$ and if η is an ordered p-monomial, then so are all the other monomials above.

With this, we can prove

Proposition 4.4. *Let A be a b-algebra over the field K, let L be a Lie subalgebra of $\mathcal{P}(A)$ and let B be the K-subalgebra of A generated by L. Choose a basis $\mathfrak{B}$ for L and linearly order its elements.*

i. If $\operatorname{char} K = 0$, then the ordered monomials in the elements of $\mathfrak{B}$ form a K-basis for B.
ii. If $\operatorname{char} K = p > 0$ and if L is a restricted Lie subalgebra of $\mathcal{P}(A)$, then the ordered p-monomials in the elements of $\mathfrak{B}$ form a K-basis for B.

Proof. By the preceding lemma we know that the appropriate monomials span B. For linear independence, we first assume that $\operatorname{char} K = 0$ and we show, by induction on n, that the ordered monomials of formal degree $\le n$ are linearly independent. This is clear for $n = 0$ and for $n = 1$ since $\mathfrak{B}$ is a basis for L and since $1\notin L$. Suppose now that $n\ge 2$ and that the inductive result holds for $n-1$. Let $0 = \sum_{j=0}^{t} k_j\eta_j$ be a dependence relation satisfied by the distinct ordered monomials $1 = \eta_0, \eta_1, \ldots, \eta_t$, each of formal degree $\le n$. We can of course assume that the monomials involve just the elements $x_1, x_2, \ldots, x_m \in \mathfrak{B}$ with $x_1 \prec x_2 \prec \cdots \prec x_m$.

By applying Δ to the above relation, we obtain $0 = \sum_{j=0}^{t} k_j\Delta(\eta_j)$ and we consider this expression in detail. To start with, we know that even when $j = 0$, each $\Delta(\eta_j)$ involves the term $\eta_j\otimes 1$. But these terms contribute

$$\sum_{j=0}^{t} k_j(\eta_j\otimes 1) = \Big(\sum_{j=0}^{t} k_j\eta_j\Big)\otimes 1 = 0\otimes 1 = 0$$

to the sum, and thus they can be ignored. Once we do this, it follows that the relation $0 = \sum_{j=0}^{t} k_j\Delta(\eta_j)$ can be written as a K-linear combination of tensors $\alpha\otimes\beta$ with α and β ordered monomials and with $\operatorname{fdeg}\alpha < n$. In particular, by the inductive assumption, the α's that occur here are linearly independent and hence are contained in a basis for A. Thus if we write

$$\sum_{j=0}^{t} k_j\Delta(\eta_j) = \sum_{\alpha} \alpha\otimes\alpha'$$

where the α's are distinct ordered monomials, each of formal degree less than n and where each $\alpha' \in A$, then the uniqueness of expression in $A \otimes A$ implies that all α' are zero. Since $n \geq 2$, we can take $\alpha = x_i$ and conclude from $(*)$ that $0 = \sum_{j=1}^{t} k_j \partial_i(\eta_j)$. Observe that this sum starts with $j = 1$ since the term $\Delta(\eta_0) = \eta_0 \otimes 1$ has already been accounted for.

Now note that if x_i is involved in η_j then $\partial_i(\eta_j) \neq 0$ since $\operatorname{char} K = 0$. Furthermore, these $\partial_i(\eta_j)$ are nonzero scalar multiples of distinct ordered monomials each of formal degree less than n. Thus, by the inductive assumption again, these monomials are linearly independent and hence $\partial_i(\eta_j) \neq 0$ implies that $k_j = 0$. But for any $j \geq 1$, we have $\eta_j \neq 1$ and hence some x_i must be involved in η_j. With this, we conclude that $k_j = 0$ for all $j \geq 1$ and, since the original dependence relation now reduces to $0 = k_0\eta_0 = k_0 1$, we also have $k_0 = 0$.

The characteristic $p > 0$ argument is similar, but of course now we must consider ordered p-monomials rather than just ordered monomials. Furthermore, if x_i is involved in η_j then, by assumption, the exponent $e_{i,j}$ of x_i in η_j satisfies $0 < e_{i,j} < p$. Thus $e_{i,j} \not\equiv 0 \bmod p$ and $\partial_i(\eta_j) \neq 0$. With this observation, the result follows. $\square$

The preceding proposition has numerous consequences of interest, some of which we list below. To start with, we have the more precise versions of the Poincaré-Birkhoff-Witt theorem and of Jacobson's theorem.

Corollary 4.5. *Let L be a Lie algebra over a field K and let $\mathfrak{B}$ be an ordered basis for L.*

i. If $\operatorname{char} K = 0$, then the ordered monomials in the elements of $\mathfrak{B}$ form a basis for $U(L)$.

ii. If $\operatorname{char} K = p > 0$ and if L is a restricted Lie algebra, then the ordered p-monomials in the elements of $\mathfrak{B}$ form a basis for $U_p(L)$.

Part (i) clearly follows since L is a Lie subalgebra of $\mathcal{P}(U(L))$ and part (ii) is similarly true. Now let M be a Lie subalgebra of L and choose a basis $\mathfrak{B}$ for L compatible with the inclusion $M \subseteq L$. In other words, $\mathfrak{B} \cap M$ is a basis for M and $\mathfrak{B} \setminus (\mathfrak{B} \cap M)$ determines a basis for the vector space L/M. Then it is easy to see from the above that the subalgebra of $U(L)$ generated by M is naturally isomorphic to $U(M)$. The analogous restricted result of course also holds. More generally, we can combine Proposition 4.4 and Corollary 4.5 to obtain

Corollary 4.6. *Let A be a b-algebra over a field K, let L be a Lie subalgebra of $\mathcal{P}(A)$ and let B be the K-subalgebra of A generated by L.*

i. If $\operatorname{char} K = 0$, then B is naturally isomorphic to $U(L)$.

ii. If $\operatorname{char} K = p > 0$ and if L is a restricted Lie subalgebra of $\mathcal{P}(A)$, then B is naturally isomorphic to $U_p(L)$.

Note that if L is an ordinary Lie algebra in characteristic $p > 0$, then the usual proof of the Poincaré-Birkhoff-Witt theorem shows that $U(L)$ also has the structure described in Corollary 4.5(i). Furthermore, we know that $U(L)$ is a b-algebra and that L is a Lie subalgebra of $\hat{L} = \mathcal{P}(U(L))$. Thus, since $\hat{L}$ is a restricted Lie algebra and $\hat{L}$ generates $U(L)$, the preceding corollary implies that $U(L) \cong U_p(\hat{L})$ as b-algebras.

The next observation is due to Friedrichs [F, page 19].

Corollary 4.7. *Suppose that $A = U(L)$ if K has characteristic 0 and that $A = U_p(L)$ if K has characteristic $p > 0$. Then $\mathcal{P}(A) = L$.*

Proof. Let $\operatorname{char} K = 0$, choose an ordered basis $\mathfrak{B}'$ of L and extend it to an ordered basis $\mathfrak{B}$ of $\mathcal{P}(A)$. Suppose, by way of contradiction, that $\mathfrak{B}$ is properly larger than $\mathfrak{B}'$ and let $x \in \mathfrak{B} \setminus \mathfrak{B}'$. Since $x \in U(L)$, we can write x as a K-linear combination of ordered monomials in the elements of $\mathfrak{B}'$. But this yields a nontrivial linear dependence among the ordered monomials in the elements of $\mathfrak{B}$, a contradiction by Proposition 4.4. Thus $\mathfrak{B} = \mathfrak{B}'$ and $\mathcal{P}(A) = L$. The characteristic $p > 0$ case follows in a similar manner. $\square$

Let L be a Lie algebra over a field K of characteristic 0. If M is a Lie subalgebra of L, then certainly $U(M)$ is a b-subalgebra of $U(L)$. On the other hand, if $\theta\colon L \to M$ is a Lie algebra epimorphism, then the universal property of $U(L)$ implies that θ extends to a unique algebra epimorphism $\theta\colon U(L) \to U(M)$. Furthermore, since the latter map is a b-algebra epimorphism, it follows that $I = \ker \theta$ is a b-ideal of $U(L)$. Conversely, we have

Proposition 4.8. *Let L be a Lie algebra over a field K of characteristic 0.*

i. If B is a b-subalgebra of $U(L)$, then $B = U(M)$ for some Lie subalgebra $M \subseteq L$.
ii. If I is a b-ideal of $U(L)$, then there is a Lie algebra epimorphism $\theta\colon L \to M$ with I the kernel of the extended algebra epimorphism $\theta\colon U(L) \to U(M)$.

Proof. (i) Let B be a b-subalgebra of $U(L)$ and set $M = L \cap B$. Then M is certainly M is a Lie subalgebra of L and $U(M) \subseteq B$. For the reverse inclusion, choose an ordered basis $\mathfrak{B}$ for L that is compatible with the containment $M \subseteq L$. We show, by induction on n, that if $\beta = \sum_{j=1}^{t} k_j \eta_j \in B$ is a K-linear combination of distinct ordered monomials η_j with $0 \neq k_j \in K$ and $\operatorname{fdeg} \eta_j \leq n$ for all j, then each η_j is an ordered monomial in $\mathfrak{B} \cap M$ and hence $\beta \in U(M)$. Suppose first that $n = 1$ so that β is a K-linear combination of 1 and elements of $\mathfrak{B}$. Since 1 and $\mathfrak{B} \cap M$ are contained in $U(M) \subseteq B$, it clearly suffices to delete all such terms and assume that $\beta \in B$ is a K-linear combination of terms in $\mathfrak{B} \setminus (\mathfrak{B} \cap M)$. But $\beta \in B \cap L = M$ and $\mathfrak{B} \setminus (\mathfrak{B} \cap M)$ is linearly independent modulo M. Thus we conclude that $\beta = 0 \in U(M)$ and the $n = 1$ case is proved.

Suppose now that $n \geq 2$ and that the inductive result holds for $n - 1$. Again let $\beta = \sum_{j=1}^{t} k_j \eta_j \in B$ with $\operatorname{fdeg} \eta_j \leq n$ for all j. We can of course assume that each η_j is an ordered monomial in the elements $x_1, x_2, \ldots, x_m \in \mathfrak{B}$ with $x_1 \prec x_2 \prec \cdots \prec x_m$, and that no η_j is the empty product 1. Since each element α of $U(L)$ can be written uniquely as a K-linear combination of ordered monomials in the elements of $\mathfrak{B}$, we can let $\lambda_i(\alpha)$ be the coefficient of the monomial x_i in such an expression for α. Clearly $\lambda_i\colon U(L) \to K$ is a K-linear functional and, since B is a b-subalgebra of $U(L)$, Lemma 2.3 implies that $(\lambda_i \otimes 1)\Delta(\beta) \subseteq B$. Furthermore, $(\lambda_i \otimes 1)\Delta(\eta_j) = \partial_i(\eta_j)$ by equation $(*)$, and thus

$$\sum_{j=1}^{t} k_j \partial_i(\eta_j) = (\lambda_i \otimes 1)\Delta(\beta) \in B,$$

for all $i = 1, 2, \ldots, m$. For fixed i, the nonzero $\partial_i(\eta_j)$'s all involve distinct ordered monomials in the elements of $\mathfrak{B}$ and each has formal degree $< n$. Thus, by induction, if $\partial_i(\eta_j) \neq 0$, then this element involves only those x_k's that are contained in the subset $\mathfrak{B} \cap M$.

Finally, consider a fixed monomial $\eta = \eta_j$ and write $\eta = x_1^{e_1} x_2^{e_2} \cdots x_m^{e_m}$. Then, for all i, we have $\partial_i(\eta) = e_i\, x_1^{e_1} \cdots x_i^{e_i - 1} \cdots x_m^{e_m}$ and, in particular, if $e_i \neq 0$ then $\partial_i(\eta) \neq 0$. Furthermore, when this occurs, then $\partial_i(\eta)$ involves only those x_k's in $\mathfrak{B} \cap M$. Suppose now that $\operatorname{fdeg} \eta \geq 2$. If $e_i \geq 2$ then x_i occurs in $\partial_i(\eta)$ and hence $x_i \in \mathfrak{B} \cap M$. On the other hand, if $e_i = 1$ then, since $\operatorname{fdeg} \eta \geq 2$, there exists $i' \neq i$ with $e_{i'} \geq 1$. But then x_i occurs in $\partial_{i'}(\eta)$, so again we conclude that $x_i \in \mathfrak{B} \cap M$. In other words, all such η's of formal degree ≥ 2 are contained in $U(M) \subseteq B$, and we can therefore delete these from β. But then β is a K-linear combination of monomials of formal degree ≤ 1 and, since this case has already been settled, the result follows.

(ii) Now let I be a b-ideal of $U(L)$ and let θ be the b-algebra epimorphism $\theta\colon U(L) \to U(L)/I = C$. Then $M = \theta(L)$ is surely a Lie subalgebra of $\mathcal{L}(C)$ and, in fact, $M \subseteq \mathcal{P}(C)$. But C is generated by $\theta(L) = M$ and hence Corollary 4.6(i) implies that $C = U(M)$. In other words, $\theta\colon U(L) \to U(M)$ is the unique algebra epimorphism which extends the Lie algebra map $\theta\colon L \to M$. Since $I = \ker \theta$, the proposition is proved. □

In a similar manner, we obtain

Proposition 4.9. *Suppose that L is a restricted Lie algebra over a field K of characteristic $p > 0$.*

i. If B is a b-subalgebra of $U_p(L)$, then $B = U_p(M)$ for some restricted Lie subalgebra $M \subseteq L$.

ii. If I is a b-ideal of $U_p(L)$, then there is a restricted Lie algebra epimorphism $\theta\colon L \to M$ such that I is the kernel of the extended algebra epimorphism $\theta\colon U_p(L) \to U_p(M)$.

Now let A be a K-algebra and let L be a Lie subalgebra of $\mathcal{L}(A)$. If V is an A-module, then we say that L acts *faithfully* on V if $\ell V \neq 0$ for all $0 \neq \ell \in L$. The following is the Lie analog of Theorem 2.5.

Theorem 4.10. *Suppose $A = U(L)$ when $\operatorname{char} K = 0$, and that $A = U_p(L)$ when $\operatorname{char} K = p$ and L is a restricted Lie algebra. If L acts faithfully on the A-module V, then A acts faithfully on the tensor module $\mathcal{T}(V) = \oplus \sum_{n=1}^{\infty} V^{\otimes n}$.*

Proof. Suppose first that $\operatorname{char} K = 0$ and let I be a b-ideal of $A = U(L)$ contained in $\operatorname{ann}_A V$. By Proposition 4.8(ii), there exists a Lie algebra epimorphism $\theta\colon L \to M$ such that I is the kernel of the corresponding algebra map $\theta\colon U(L) \to U(M)$. If $I \neq 0$, then θ cannot be one-to-one on L and hence there exists $0 \neq \ell \in L$ with $\theta(\ell) = 0$. In particular, $\ell \in I \subseteq \operatorname{ann}_A V$, so $\ell V = 0$ and this contradicts the fact that L is faithful on V. In other words, the L-faithfullness assumption implies that $\operatorname{ann}_A V$ contains no nonzero b-ideal. Since $U(L)$ is coassociative, Corollary 1.4 now yields the result. The characteristic $p > 0$ argument is of course similar. □

The following nice consequence is due to Harish-Chandra [H, Theorem 1]. Unfortunately, the proof we offer is not self contained, but rather requires that we quote a basic theorem from the study of Lie algebras. Recall that a K-algebra A is *residually finite* if the collection of its ideals I with $\dim_K A/I < \infty$ has intersection equal to 0. In other words, these algebras are precisely the subdirect products of finite dimensional K-algebras.

Corollary 4.11. *If L is a finite dimensional Lie algebra over a field K of characteristic 0, then $U(L)$ is residually finite.*

Proof. By Ado's theorem (see [J, §VI.2]), $A = U(L)$ has a finite K-dimensional module V on which L acts faithfully. Thus, the preceding theorem implies that $0 = \operatorname{ann}_A \mathcal{T}(V) = \bigcap_{n=1}^{\infty} I_n$, where $I_n = \operatorname{ann}_A V^{\otimes n}$. But each $V^{\otimes n}$ is a finite dimensional A-module, so $I_n = \operatorname{ann}_A V^{\otimes n}$ is an ideal of A of finite codimension and hence the result follows. □

The characteristic $p > 0$ analog of the above is trivial. Indeed, if L is a finite dimensional restricted Lie algebra, then its restricted enveloping algebra $U_p(L)$ is also finite dimensional. On the other hand, infinite dimensional analogs of the above in all characteristics can be found in [Mi]. Finally, we remark that $U(L)$ and $U_p(L)$ have no group-like elements other than 0 or 1. This is an easy exercise using Lemma 4.2 and Proposition 4.4.

5. Free Algebras

Let $F = K\langle X\rangle$ denote the free K-algebra on the set of variables X. Then the *universal mapping property* for F asserts that if A is any K-algebra and if $\theta\colon X \to A$ is any map at all, then θ extends to a unique algebra homomorphism $\theta\colon F \to A$. Because of this, it is a simple matter to give F various b-algebra structures, and in this section, we briefly discuss two examples of interest.

To start with, let us define $\Delta'\colon F \to F \otimes F$ by $\Delta'\colon x \mapsto x \otimes x$ for all $x \in X$. Then obviously Δ' defines a b-algebra structure on F with each x being a group-like element. In fact, if G is the subsemigroup of $\mathcal{S}(F)$ generated by X, then Lemma 2.1 and Corollary 2.2 imply that $G = \mathcal{G}(F)^{\#}$ and that F is the semigroup algebra $K[G]$. This comes as no surprise since we know that the distinct words in X form a K-basis for F. Furthermore, it is clear that G is the *free semigroup* generated by the set X.

A more interesting b-algebra structure for F occurs when we define $\Delta\colon F \to F$ by $\Delta\colon x \mapsto 1 \otimes x + x \otimes 1$. Then each $x \in X$ is a primitive element of F and we have

Proposition 5.1. *Let K be a field of characteristic 0, let $F = K\langle X\rangle$ be the free K-algebra on the variables X and let L be the Lie subalgebra of $\mathcal{L}(F)$ generated by X. Then $F = U(L)$ and L is the free Lie algebra generated by X.*

Proof. We use the b-algebra structure for F given above. Then L is a Lie subalgebra of $\mathcal{P}(F)$ and L generates F as an algebra. Thus, by Corollary 4.6(i), $F = U(L)$. Finally, let M be any Lie algebra over K and let $\theta\colon X \to M$ be any map. Then $\theta\colon X \to U(M)$, so the universal property for F implies that θ extends to a unique algebra homomorphism $\theta\colon F \to U(M)$. Furthermore, since L is the Lie subalgebra of $\mathcal{L}(F)$ generated by X, it is clear that $\theta(L)$ is contained in the Lie subalgebra of $\mathcal{L}(U(M))$ generated by $\theta(X) \subseteq M$. Thus $\theta(L) \subseteq M$ and it is clear that θ is a Lie homomorphism. In other words, we have shown that any map $\theta\colon X \to M$ extends to a Lie homomorphism $\theta\colon L \to M$ which is certainly uniquely determined, and therefore L is the free Lie algebra generated by X. □

In a similar manner, one can prove

Proposition 5.2. *Let K be a field of characteristic $p > 0$, let $F = K\langle X\rangle$ be the free K-algebra on the variables X and let L be the restricted Lie subalgebra of $\mathcal{L}_p(F)$*

generated by X. Then $F = U_p(L)$ and L is the free restricted Lie algebra generated by the set X.

6. Bialgebras and Hopf Algebras

Now we return to more general theory. Let (A, Δ) be a b-algebra, let B be a K-algebra and, as usual, let $\mathrm{Hom}_K(A, B)$ denote the K-vector space of all K-linear transformations from A to B. Suppose $f, g \in \mathrm{Hom}_K(A, B)$ and observe that the map $\sigma\colon A \times A \to B$ given by $\sigma\colon a \times a' \mapsto f(a)g(a') \in B$ is bilinear. Thus σ gives rise to a linear transformation $\bar{\sigma}\colon A \otimes A \to B$ and, via composition with $\Delta\colon A \to A \otimes A$, we obtain the map $f * g = \bar{\sigma}\Delta \in \mathrm{Hom}_K(A, B)$ called the *convolution product* of f and g. Specifically, $(f * g)(a) = \sum_i f(a_i)g(a'_i)$ where $\Delta(a) = \sum_i a_i \otimes a'_i$.

In other words, if A is a b-algebra, then $\mathrm{Hom}_K(A, B)$ has a convolution multiplication along with its K-vector space structure. Indeed, with these operations, $\mathrm{Hom}_K(A, B)$ is quite close to being a K-algebra in its own right. All that is missing is associativity of multiplication and an identity element. Furthermore, associativity holds if we assume that Δ is coassociative. The argument for this is quite straightforward, but the right sort of notation makes it even easier to understand.

To start with, let $V_1, V_2, \ldots, V_n$ be K-vector spaces and, using the associativity of $\otimes$, observe that the n-fold tensor product $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ makes sense. Furthermore, suppose that X is any K-vector space and let $\beta\colon V_1 \times V_2 \times \cdots \times V_n \to X$ be any *multilinear map*. This means that β is linear in each variable or equivalently, for each subscript i, we have

$$\begin{aligned} &\beta(v_1, v_2, \ldots, kv_i + k'v'_i, \ldots, v_n) \\ &\qquad = k\,\beta(v_1, v_2, \ldots, v_i, \ldots, v_n) + k'\,\beta(v_1, v_2, \ldots, v'_i, \ldots, v_n) \end{aligned}$$

for all $v_j \in V_j$, $v'_i \in V_i$ and $k, k' \in K$. It then follows from the universal mapping property for n-fold tensor products that β determines a unique linear transformation $V_1 \otimes V_2 \otimes \cdots \otimes V_n \to X$ given by $v_1 \otimes v_2 \otimes \cdots \otimes v_n \mapsto \beta(v_1, v_2, \ldots, v_n)$.

Now let A be a coassociative b-algebra. Then, as we will see, the coassociativity of Δ implies that any choice of composite maps built up from 1 and Δ determines the same algebra homomorphism from the algebra A to the n-fold tensor power $A^{\otimes n} = A \otimes A \otimes \cdots \otimes A$. For example, with $n = 4$, the composite maps

$$\begin{aligned} &A \xrightarrow{\ \Delta\ } A \otimes A \xrightarrow{1\otimes\Delta} A \otimes A \otimes A \xrightarrow{1\otimes\Delta\otimes 1} A \otimes A \otimes A \otimes A, \\ &A \xrightarrow{\ \Delta\ } A \otimes A \xrightarrow{\Delta\otimes 1} A \otimes A \otimes A \xrightarrow{1\otimes 1\otimes\Delta} A \otimes A \otimes A \otimes A, \end{aligned}$$

and even

$$A \xrightarrow{\ \Delta\ } A \otimes A \xrightarrow{\Delta\otimes\Delta} A \otimes A \otimes A \otimes A$$

are identical. Of course, in the latter we could apply the Δ's in $\Delta \otimes \Delta$ one at a time, with the right-hand Δ first, to obtain the clearly equivalent sequence

$$A \xrightarrow{\ \Delta\ } A \otimes A \xrightarrow{1\otimes\Delta} A \otimes A \otimes A \xrightarrow{\Delta\otimes 1\otimes 1} A \otimes A \otimes A \otimes A.$$

We sketch a quick proof of this uniqueness.

Lemma 6.1. *Let A be a coassociative b-algebra. Then, for each integer n, all maps $\delta\colon A \to A^{\otimes n}$ built, as above, from 1 and Δ are identical.*

Proof. We proceed by induction on n. When $n = 1$ we have $\delta = 1$, and when $n = 2$ we must have $\delta = \Delta$. For $n = 3$ the only possibilities are $\delta = (1 \otimes \Delta)\Delta$ or $\delta = (\Delta \otimes 1)\Delta$, and these are equal by coassociativity. Furthermore, as in the preceding $n = 4$ example, we can certainly apply the Δ maps one at a time. In other words, we can assume that $\delta = \delta_{n-1}\delta_{n-2}\cdots\delta_1$, where each δ_i maps $A^{\otimes i}$ to $A^{\otimes(i+1)}$ and has the form $1 \otimes \cdots \otimes \Delta \otimes \cdots \otimes 1$ with precisely one copy of Δ.

Suppose now that $n \geq 4$ and that the result holds for $n-1$. Then by induction, the product $\delta_{n-2}\delta_{n-3}\cdots\delta_1$ is uniquely determined independent of the particular choices for the various δ_i's that occur. We can therefore clearly assume that $\delta_i = 1^{\otimes(i-1)} \otimes \Delta$ for $i = 1, 2, \ldots, n-3$, and δ_{n-2} can be taken to be either $1^{\otimes(n-3)} \otimes \Delta$ or $\Delta \otimes 1^{\otimes(n-3)}$. If δ_{n-1} is of the form $1 \otimes \alpha$, then by taking all the remaining δ_i equal to $1^{\otimes(i-1)} \otimes \Delta$, we see that $\delta = (1 \otimes \delta')\Delta$, where $\delta' \colon A \to A^{\otimes(n-1)}$. By induction, δ' is uniquely determined and hence so is δ.

Finally, suppose $\delta_{n-1} = \Delta \otimes 1^{\otimes(n-2)} = \Delta \otimes 1 \otimes 1^{\otimes(n-3)}$. Then, by taking δ_{n-2} to be $\Delta \otimes 1^{\otimes(n-3)}$, and by applying coassociativity, we see that

$$\begin{aligned}\delta_{n-1}\delta_{n-2} &= (\Delta \otimes 1 \otimes 1^{\otimes(n-3)})(\Delta \otimes 1^{\otimes(n-3)}) \\ &= (1 \otimes \Delta \otimes 1^{\otimes(n-3)})(\Delta \otimes 1^{\otimes(n-3)}).\end{aligned}$$

In other words, we can replace δ_{n-1} by $1 \otimes \Delta \otimes 1^{\otimes(n-3)}$ and, by so doing, we are reduced to the preceding case where δ_{n-1} is of the form $1 \otimes \alpha$. With this, the result clearly follows. □

For any n, we can now denote the unique map from A to $A^{\otimes n}$ by Δ^{n-1}. Clearly $\Delta^0 = 1$, $\Delta^1 = \Delta$, and $\Delta^n = (1 \otimes \Delta^{(n-1)})\Delta$ for all $n \geq 2$. Now, if $a \in A$ then, following Heyneman and Sweedler, we write $\Delta^{n-1}(a)$ symbolically as

$$\Delta^{n-1}(a) = \sum_{(a)} a_1 \otimes a_2 \otimes \cdots \otimes a_n$$

so that a_i denotes a typical ith tensor factor in the expansion for $\Delta^{n-1}(a)$. Notice that if $\beta \colon A^{\times n} \to V$ is any multilinear map, then

$$\beta\big(\Delta^{n-1}(a)\big) = \sum_{(a)} \beta(a_1, a_2, \ldots, a_n)$$

makes sense. Notice also that, since

$$(1 \otimes \cdots \otimes \Delta \otimes \cdots 1)\Delta^{n-1}(a) = \Delta^n(a),$$

we have

$$\sum_{(a)} a_1 \otimes \cdots \otimes \Delta(a_i) \otimes \cdots \otimes a_n = \sum_{(a)} a_1 \otimes \cdots \otimes a_i \otimes a_{i+1} \otimes \cdots \otimes a_{n+1}$$

for all i. We can, of course, view the preceding operation as fixing $a_1, a_2, \ldots, a_{i-1}$, replacing a_i by $a_i \otimes a_{i+1}$ and shifting the subscripts of $a_{i+1}, \ldots, a_n$ up by 1. It takes some practice and a certain leap of faith to understand and appreciate this notation, but once one does, computations become almost routine.

For example, let us show that convolution multiplication is associative in this context. To this end, let $f, g, h \in \operatorname{Hom}_K(A, B)$ and let $a \in A$. Then

$$\big(f * (g * h)\big)(a) = \sum_{(a)} f(a_1)(g * h)(a_2) = \sum_{(a)} f(a_1)\big(g(a_2)h(a_3)\big)$$

and similarly

$$\big((f * g) * h\big)(a) = \sum_{(a)} (f * g)(a_1)h(a_2) = \sum_{(a)} \big(f(a_1)g(a_2)\big)h(a_3).$$

Thus, since multiplication in B is associative, we conclude that $f*(g*h) = (f*g)*h$. Throughout the remainder of this paper, we will assume that Δ is a coassociative comultiplication and we will freely use the Heyneman-Sweedler notation.

Finally, we need a convolution identity in $\mathrm{Hom}_K(A,B)$ and we would like to achieve this, for all B, by adding just one additional structure to A. In particular, when $B = K$, this structure must yield an identity element in $\mathrm{Hom}_K(A,K)$. In other words, at the very least, we seem to need a certain linear functional $\varepsilon\colon A \to K$. Now we expect $\mathrm{Hom}_K(A,K)$ to be the duel or "co" of A, so its identity should be the "co" of the identity of A. Since the idea of comultiplication in A comes from multiplication by reversing the arrows, it is reasonable to expect that ε might come from properties of the natural unit embedding of K into A also by reversing the direction of the arrows. As we will see, this is indeed the case.

First, let us note that the embedding $u\colon K \to A$ is an algebra homomorphism known as the *unit map* since $u(k) = k1$ for all $k \in K$. Next, u is related to the multiplication map $\mu\colon A \otimes A \to A$ by the fact that the compositions

$$A \xrightarrow{\ \cong\ } K \otimes A \xrightarrow{u\otimes 1} A \otimes A \xrightarrow{\ \mu\ } A$$

and

$$A \xrightarrow{\ \cong\ } A \otimes K \xrightarrow{1\otimes u} A \otimes A \xrightarrow{\ \mu\ } A$$

are both equal to the identity. Here, of course, $A \cong K \otimes A$ via the maps $a \mapsto 1 \otimes a$ and $k \otimes a \mapsto ka$ for all $a \in A$ and $k \in K$. This leads us to define a *counit* $\varepsilon\colon A \to K$ to be a K-algebra epimorphism such that the compositions

$$A \xrightarrow{\ \Delta\ } A \otimes A \xrightarrow{\varepsilon\otimes 1} K \otimes A \xrightarrow{\ \cong\ } A$$

and

$$A \xrightarrow{\ \Delta\ } A \otimes A \xrightarrow{1\otimes \varepsilon} A \otimes K \xrightarrow{\ \cong\ } A$$

are both equal to the identity. Equivalently, the preceding conditions assert that

$$\sum_{(a)} \varepsilon(a_1)a_2 = a = \sum_{(a)} a_1\varepsilon(a_2)$$

for all $a \in A$.

Putting this all together, we say that the triple (A, Δ, ε) is a *bialgebra* if A is a K-algebra, $\Delta\colon A \to A \otimes A$ is a coassociative comultiplication, and $\varepsilon\colon A \to K$ is a counit. Not surprisingly, we have

Lemma 6.2. *Suppose that the triple (A, Δ, ε) is a bialgebra and that B is any K-algebra. Then $\mathrm{Hom}_K(A,B)$, with convolution multiplication, is an associative K-algebra with identity ε.*

Proof. We already know that $\mathrm{Hom}_K(A,B)$ has a K-vector space structure along with an associative and distributive convolution multiplication. All that remains is to show that $\varepsilon\colon A \to K \subseteq B$ plays the role of the identity element. For this, let $f \in \mathrm{Hom}_K(A,B)$ and let $a \in A$. Then

$$(\varepsilon * f)(a) = \sum_{(a)} \varepsilon(a_1)f(a_2) = f\Big(\sum_{(a)} \varepsilon(a_1)a_2\Big) = f(a)$$

so $\varepsilon * f = f$. In a similar manner, we have $f * \varepsilon = f$. $\square$

Two remarks are now in order. First, the definition of a bialgebra is really symmetric with respect to its multiplicative and comultiplicative structures. While this is not apparent from the information given here, it is not too hard to prove. Second, the convolution product in $\mathrm{Hom}_K(A,B)$ uses the multiplication in B and just the comultiplication in A. Thus it is usually defined when A is merely assumed to be a *coalgebra*, that is a vector space with an appropriate coassociative comultiplication and an appropriate counit.

If g is a nonzero group-like element in the bialgebra A, then $\Delta(g) = g \otimes g$ implies that $g = \varepsilon(g)g$. Thus since $\varepsilon(g) \in K$ and $g \neq 0$, we must have $\varepsilon(g) = 1$. In particular, since ε is an algebra homomorphism, it follows that the nonzero group-like elements of A are closed under multiplication. On the other hand, if x is a primitive element of A, then $\Delta(x) = 1 \otimes x + x \otimes 1$ and $\varepsilon(1) = 1$ imply that $x = \varepsilon(1)x + \varepsilon(x)1 = x + \varepsilon(x)$, so $\varepsilon(x) = 0$. Conversely, we have

Lemma 6.3. *Let K be a field.*

- *i. If G is a semigroup without 0, then the semigroup algebra $K[G]$ is a bialgebra with counit $\varepsilon\colon \sum_g k_g g \mapsto \sum_g k_g$.*
- *ii. If $\operatorname{char} K = 0$ and L is a K-Lie algebra, then the enveloping algebra $U(L)$ is a bialgebra with counit ε the unique algebra epimorphism $U(L) \to K$ determined by $\varepsilon(L) = 0$.*
- *iii. If $\operatorname{char} K = p > 0$ and L is a restricted Lie algebra over K, then the restricted enveloping algebra $U_p(L)$ is a bialgebra with counit ε the unique algebra epimorphism $U_p(L) \to K$ determined by $\varepsilon(L) = 0$.*

Proof. (i) The map $G \to 1 \in K$ extends to an algebra epimorphism $\varepsilon\colon K[G] \to K$. Since $\Delta(g) = g \otimes g$ for all $g \in G$, we have $\sum_{(g)} \varepsilon(g_1)g_2 = g = \sum_{(g)} g_1\varepsilon(g_2)$ and, by linearity, ε is a counit.

(ii) The map $L \to 0 \in K$ is certainly a Lie algebra homomorphism and hence it extends uniquely to an algebra homomorphism $\varepsilon\colon U(L) \to K$. Furthermore, it is clear that $\sum_{(x)} \varepsilon(x_1)x_2 = x = \sum_{(x)} x_1\varepsilon(x_2)$ for all $x \in L$. Finally, identify $K \otimes U(L)$ and $U(L) \otimes K$ with $U(L)$ and observe that the algebra homomorphisms $(\varepsilon \otimes 1)\Delta\colon U(L) \to U(L)$ and $(1 \otimes \varepsilon)\Delta\colon U(L) \to U(L)$ agree with the identity map on L. Thus, since L generates $U(L)$ as a K-algebra, we conclude that $(\varepsilon \otimes 1)\Delta = 1 = (1 \otimes \varepsilon)\Delta$, as required. Part(iii) follows in a similar fashion. $\square$

Now suppose that (A, Δ, ε) is a bialgebra and consider the *convolution algebra* $\mathrm{Hom}_K(A,A)$. This algebra contains the identity map $1\colon A \to A$, but of course this is different from the convolution identity ε. Nevertheless, in the most important bialgebras, 1 is at least a unit in $\mathrm{Hom}_K(A,A)$ and its unique convolution inverse is called the *antipode* of A and is denoted by S. Thus the linear transformation $S\colon A \to A$ is the antipode of A if $S * 1 = \varepsilon = 1 * S$ or equivalently if

$$\sum_{(a)} S(a_1)a_2 = \varepsilon(a) = \sum_{(a)} a_1 S(a_2)$$

for all $a \in A$. A bialgebra with antipode is said to be a *Hopf algebra*.

If g is a group-like element of the Hopf algebra A, then $\Delta(g) = g \otimes g$ and $\varepsilon(g) = 1$ imply that $S(g)g = 1 = gS(g)$, so g is invertible and $g^{-1} = S(g)$. In particular, $S(1) = 1$. Furthermore, $S(g)$ is also group-like since $\Delta\big(S(g)\big) = \Delta(g)^{-1} = (g \otimes g)^{-1} = S(g) \otimes S(g)$. On the other hand, if x is a primitive element of A, then $\Delta(x) = 1\otimes x + x\otimes 1$ and $\varepsilon(x) = 0$ imply that $0 = S(1)x + S(x)1 = x + S(x)$, so $S(x) = -x$. Conversely, we have

Lemma 6.4. *Let K be a field.*

i. If G is a group, then the group algebra $K[G]$ is a Hopf algebra with antipode $S\colon \sum_g k_g g \mapsto \sum_g k_g g^{-1}$.
ii. If $\operatorname{char} K = 0$ and L is a K-Lie algebra, then the enveloping algebra $U(L)$ is a Hopf algebra with antipode S being the unique algebra antiautomorphism $S : U(L) \to U(L)$ determined by $S(\ell) = -\ell$ for all $\ell \in L$.
iii. If $\operatorname{char} K = p > 0$ and L is a restricted K-Lie algebra, then the restricted enveloping algebra $U_p(L)$ is a Hopf algebra with antipode S being the unique algebra antiautomorphism $S : U_p(L) \to U_p(L)$ determined by $S(\ell) = -\ell$ for all $\ell \in L$.

Proof. (i) The map $S\colon K[G] \to K[G]$ given by $S\colon \sum_g k_g g \mapsto \sum_g k_g g^{-1}$ is certainly a well-defined linear transformation. Moreover, since $\Delta(g) = g\otimes g$ for all $g \in G$, we have $\sum_{(g)} S(g_1)g_2 = \varepsilon(g) = \sum_{(g)} g_1 S(g_2)$ and, by linearity, S is an antipode.

(ii) Let A^{op} denote the opposite ring of $A = U(L)$. Then the map $S\colon L \to \mathcal{L}(A^{\mathrm{op}})$ given by $\ell \mapsto -\ell$ is easily seen to be a Lie algebra homomorphism. Hence this map extends to a unique algebra homomorphism $S\colon A \to A^{\mathrm{op}}$. Furthermore, since $A^{\mathrm{op}} = A$ as sets, we can view S as a map from A to A and, as such, it is clearly the unique antihomomorphism extending $S(\ell) = -\ell$ for all $\ell \in L$. It follows that $S^2\colon A \to A$ is a homomorphism extending the identity map on L, so uniqueness implies that $S^2 = 1$ and hence that S is an antiautomorphism of A.

Set

$$B = \{a \in A \mid (S * 1)(a) = \varepsilon(a) = (1 * S)(a)\}$$

so that B is clearly a K-subspace of A. Furthermore, let $a, b \in B$ and note that

$$\begin{aligned}\Delta(ab) = \Delta(a)\Delta(b) &= \Big(\sum_{(a)} a_1 \otimes a_2\Big)\Big(\sum_{(b)} b_1 \otimes b_2\Big)\\ &= \sum_{(a),(b)} a_1 b_1 \otimes a_2 b_2.\end{aligned}$$

Thus, since S is an antihomomorphism, we have

$$\begin{aligned}(S * 1)(ab) &= \sum_{(a),(b)} S(a_1 b_1) a_2 b_2 = \sum_{(a),(b)} S(b_1) S(a_1) a_2 b_2\\ &= \sum_{(b)} S(b_1)\Big(\sum_{(a)} S(a_1) a_2\Big) b_2.\end{aligned}$$

But $\sum_{(a)} S(a_1)a_2 = \varepsilon(a)$ and $\sum_{(b)} S(b_1)b_2 = \varepsilon(b)$ since $a, b \in B$, so it follows that

$$(S * 1)(ab) = \sum_{(b)} S(b_1)\varepsilon(a) b_2 = \varepsilon(a)\varepsilon(b) = \varepsilon(ab).$$

Similarly, $(1 * S)(ab) = \varepsilon(ab)$ and we conclude that $ab \in B$.

In other words, we have shown that B is a subalgebra of A. But it is clear that B contains the generating set L. Thus $B = A$ and S is indeed an antipode for A. Part (iii) follows in a similar fashion. $\square$

Notice that the antipodes defined above are all algebra antiautomorphisms satisfying $S^2 = 1$. As it turns out, these properties are actually forced upon us. To start with, it can be shown that the antipode S of an arbitrary Hopf algebra A is at least an algebra antihomomorphism. While S need not be one-to-one or onto in general, certain situations imply the even stronger condition $S^2 = 1$. For example, this occurs when A is commutative and also when A is *cocommutative*. By definition, the latter means that $\Delta = T\Delta$ where $T\colon A \otimes A \to A \otimes A$ is the *twist map* given by $a \otimes a' \mapsto a' \otimes a$. Equivalently, A is cocommutative if and only if

$$\sum_{(a)} a_1 \otimes a_2 = \sum_{(a)} a_2 \otimes a_1$$

for all $a \in A$. Since Δ is an algebra homomorphism, it clearly suffices to check cocommutativity on a set of generators for A. With this, it is easy to see that group algebras and enveloping algebras are all cocommutative and thus S^2 must equal 1 for these algebras.

Finally, there is an important theorem due to Kostant (see [Sw, Theorems 8.1.5 and 13.0.1] that characterizes cocommutative Hopf algebras over an algebraically closed field of characteristic 0. Indeed, every such algebra is an "extension" of an enveloping algebra by a group algebra. In particular, these algebras are generated by their primitive and group-like elements.

7. Biideals and Hopf Ideals

Let (A, Δ, ε) be a bialgebra. If C is a subalgebra of A, then C is said to be a *bisubalgebra* if C is a bialgebra in its own right using the restrictions of Δ and ε. For this to occur, it is clear that only the condition $\Delta(C) \subseteq C \otimes C$ need be checked. Thus C is a bisubalgebra if and only if it is a b-subalgebra. Next, if $(B, \Delta', \varepsilon')$ is a bialgebra, than a *bialgebra homomorphism* $\theta\colon A \to B$ is an algebra homomorphism compatible with the two comultiplications and the two counits. In other words, θ must be a b-algebra homomorphism such that the composite map

$$A \xrightarrow{\ \theta\ } B \xrightarrow{\ \varepsilon'\ } K$$

is equal to $\varepsilon\colon A \to K$. Equivalently, the latter occurs if and only if the diagram

$$\begin{array}{ccc} A & \xrightarrow{\ \theta\ } & B \\ {\scriptstyle\varepsilon}\downarrow & & \downarrow{\scriptstyle\varepsilon'} \\ K & = & K \end{array}$$

is commutative. The kernel of such a homomorphism θ is called a *biideal* of A. It is easy to see that I is a biideal of A if and only if I is a b-ideal with $\varepsilon(I) = 0$.

Now suppose that A is a Hopf algebra with the above structure and with antipode S. If C is a subalgebra of A, then C is a *Hopf subalgebra* if it is a Hopf algebra in its own right using the restrictions of the various maps defined on A. It is clear that this occurs if and only if C is a bisubalgebra of A with $S(C) \subseteq C$. Again, if $(B, \Delta', \varepsilon', S')$ is a Hopf algebra, then a *Hopf algebra homomorphism* $\theta\colon A \to B$ is a bialgebra homomorphism compatible with the two antipodes. To be precise, the latter condition requires that the diagram

$$\begin{array}{ccc} A & \xrightarrow{\theta} & B \\ {\scriptstyle S}\big\downarrow & & \big\downarrow{\scriptstyle S'} \\ A & \xrightarrow[\theta]{} & B \end{array}$$

is commutative, or equivalently that $S'\theta = \theta S$. The kernel of such a homomorphism is called a *Hopf ideal* of A. Clearly, any Hopf ideal must be a biideal. Furthermore, the preceding commutative diagram implies that $S(I) \subseteq I$. Conversely, if I is a biideal with $S(I) \subseteq I$, then I maps to 0 under the composition

$$A \xrightarrow{S} A \xrightarrow{\theta} A/I.$$

Therefore S determines a map $S' \colon A/I \to A/I$, and S' is easily seen to play the role of the antipode in A/I. To reiterate, we have shown

Lemma 7.1. *Let (A, Δ, ε) be a bialgebra, let C be a subalgebra of A, and let I be an ideal of A.*

i. C is a bisubalgebra of A if and only if $\Delta(C) \subseteq C \otimes C$. Furthermore, I is a biideal of A if and only if $\Delta(I) \subseteq A \otimes I + I \otimes A$ and $\varepsilon(I) = 0$.

ii. Now suppose that A is a Hopf algebra with antipode S. Then C is a Hopf subalgebra of A if and only if it is a bisubalgebra with $S(C) \subseteq C$. Moreover, I is a Hopf ideal of A if and only if it is a biideal with $S(I) \subseteq I$.

Our goal now is to extend Proposition 1.3 and Corollary 1.4 to the context of bialgebras and Hopf algebras. To start with, if A is a bialgebra, then the homomorphism $\varepsilon \colon A \to K$ determines a 1-dimensional A-module, the so-called *principal module*. Specifically, let K_ε be a copy of K and use ${}_\varepsilon \colon K \to K_\varepsilon$ to denote the given K-algebra isomorphism. Then K_ε becomes an A-module by defining $ak_\varepsilon = \varepsilon(a)k_\varepsilon$ for all $a \in A$ and $k \in K$. A basic property of this module is that it acts like the identity with respect to tensor product. To be precise, we have

Lemma 7.2. *If A is a bialgebra, then for all A-modules V*

$$K_\varepsilon \otimes V \cong V \cong V \otimes K_\varepsilon$$

as A-modules. Furthermore, K_ε is the unique A-module satisfying this condition.

Proof. We know that the map $\tau \colon V \to K_\varepsilon \otimes V$ given by $v \mapsto 1_\varepsilon \otimes v$ is a K-vector space isomorphism. Furthermore, if $a \in A$ and $v \in V$, then

$$\begin{aligned} a\tau(v) &= \sum_{(a)} a_1 1_\varepsilon \otimes a_2 v = \sum_{(a)} \varepsilon(a_1) 1_\varepsilon \otimes a_2 v \\ &= 1_\varepsilon \otimes \Big(\sum_{(a)} \varepsilon(a_1) a_2\Big) v = 1_\varepsilon \otimes av = \tau(av). \end{aligned}$$

Thus τ is an A-module isomorphism and the rest is clear. □

If V is any A-module then, in view of the above, it is natural to define the 0th tensor power of V to be $V^{\otimes 0} = K_\varepsilon$. We can now quickly obtain

Proposition 7.3. *Let (A, Δ, ε) be a bialgebra.*

i. If $\mathcal{F}$ is a family of A-modules closed under tensor product and containing K_ε, then $\bigcap_{V \in \mathcal{F}} \operatorname{ann}_A V$ is a biideal of A.

ii. Suppose V is an A-module whose annihilator contains no nonzero biideal of A. Then $\mathcal{T}_0(V) = \oplus \sum_{n=0}^{\infty} V^{\otimes n}$ is a faithful A-module.

Proof. (i) By Proposition 1.3, $I = \bigcap_{V \in \mathcal{F}} \operatorname{ann}_A V$ is a b-ideal of A. Furthermore, $K_\varepsilon \in \mathcal{F}$ implies that $I \subseteq \operatorname{ann}_A K_\varepsilon = \ker \varepsilon$. Thus $\varepsilon(I) = 0$ and I is a biideal.

(ii) Set $\mathcal{F} = \{V^{\otimes n} \mid n = 0, 1, \ldots\}$ so that $\mathcal{F}$ is closed under tensor product and contains $V^{\otimes 0} = K_\varepsilon$. By the above, $I = \bigcap_{n=0}^{\infty} \operatorname{ann}_A V^{\otimes n} = \operatorname{ann}_A \mathcal{T}_0(V)$ is a biideal of A contained in $\operatorname{ann}_A V$. Thus, by assumption, $I = 0$. □

In the remainder of this paper we will restrict our attention to finite dimensional algebras. The following is a special case of a surprising result due to Nichols [N, Theorem 1].

Lemma 7.4. *If A is a finite dimensional Hopf algebra, then any b-subalgebra of A is a Hopf subalgebra and any b-ideal of A is a Hopf ideal of A.*

Proof. Let B denote either a b-subalgebra of A or a b-ideal of A. Furthermore, let $E = \operatorname{Hom}_K(A, A)$ be the convolution algebra of A and set

$$F = \{f \in E \mid f(B) \subseteq B\}.$$

Certainly, F is a K-subspace of E and, in fact, F is closed under convolution multiplication. To see the latter, let $f, g \in F$. If B is a b-subalgebra of A, then $\Delta(B) \subseteq B \otimes B$ implies that

$$(f * g)(B) \subseteq f(B)g(B) \subseteq B^2 = B.$$

On the other hand, if B is a b-ideal, then $\Delta(B) \subseteq A \otimes B + B \otimes A$ implies that

$$(f * g)(B) \subseteq f(A)g(B) + f(B)g(A) \subseteq AB + BA = B$$

since $B \triangleleft A$.

Now observe that the identity map 1 is contained in F. Thus, by the above, F contains the convolution powers 1^{*n} of 1 for all $n > 0$. Furthermore, since A is finite dimensional, E is also finite dimensional and hence the map 1 is algebraic over K. In particular, for some $m \geq 1$, we can write 1^{*m} as a finite K-linear combination of the powers 1^{*i} with $i > m$. But 1 has a convolution inverse S, so multiplying the expression for 1^{*m} by S^{*m} and by $S^{*(m+1)}$ in turn, we deduce first that $\varepsilon = 1^{*0} \in F$ and then that $S = 1^{*(-1)} \in F$. In other words, $\varepsilon(B) \subseteq B$ and $S(B) \subseteq B$.

Finally, if B is a b-subalgebra, then $S(B) \subseteq B$ implies that B is a Hopf subalgebra. On the other hand, if B is a b-ideal of A, then $\varepsilon(B) \subseteq B \cap K = 0$. Thus, since $S(B) \subseteq B$, we conclude that B is a Hopf ideal of A. □

The preceding result is false in general for infinite dimensional Hopf algebras. Some rather complicated counterexamples appear in [N].

Theorem 7.5. *Let A be a finite dimensional Hopf algebra.*

i. If $\mathcal{F}$ is a family of A-modules that is closed under taking tensor products, then $\bigcap_{V \in \mathcal{F}} \operatorname{ann}_A V$ is a Hopf ideal of A.
ii. Suppose V is an A-module whose annihilator contains no nonzero Hopf ideal of A. Then $\mathcal{T}(V) = \oplus \sum_{n=1}^{\infty} V^{\otimes n}$ is a faithful A-module.

This follows immediately from Proposition 1.3, Corollary 1.4 and Lemma 7.4. We now obtain some consequences of interest. First, recall than an A-module V is *semisimple* if it is a finite direct sum of simple modules. Notice that if $I \triangleleft A$, then any A/I-module can be viewed as an A-module. Conversely, if V is an A-module with $\operatorname{ann}_A V \supseteq I$, then V can be viewed as an A/I-module.

Corollary 7.6. *If A is a finite dimensional Hopf algebra, then the set of semisimple A-modules is closed under tensor product if and only if the Jacobson radical* $\mathrm{Rad}(A)$ *is a Hopf ideal of A.*

Proof. Let $\mathcal{F}$ be the set of all semisimple A-modules. If $\mathcal{F}$ is closed under tensor product, then Theorem 7.5(i) implies that $\mathrm{Rad}(A) = \bigcap_{V\in\mathcal{F}} \operatorname{ann}_A V$ is a Hopf ideal of A. Conversely, if $\mathrm{Rad}(A)$ is a Hopf ideal, then $\mathcal{F}$ consists of all the modules for the Hopf algebra $A/\mathrm{Rad}(A)$ and therefore $\mathcal{F}$ is surely closed under tensor product. □

In a similar manner, we prove

Corollary 7.7. *Let A be a finite dimensional semisimple Hopf algebra and let $\mathcal{I}$ be a family of simple A-modules. Suppose that, for all $V, W \in \mathcal{I}$, every irreducible submodule of $V \otimes W$ is contained in $\mathcal{I}$. Then $I = \bigcap_{V\in\mathcal{I}} \operatorname{ann}_A V$ is a Hopf ideal of A, and $\mathcal{I}$ is the set of all simple A/I-modules.*

Proof. Let $\mathcal{F}$ be the set of all finite direct sums (allowing multiplicities) of members of $\mathcal{I}$. Since A is semisimple, the hypothesis implies that $\mathcal{F}$ is closed under tensor product. Hence, by Theorem 7.5(i), $I = \bigcap_{V\in\mathcal{I}} \operatorname{ann}_A V = \bigcap_{W\in\mathcal{F}} \operatorname{ann}_A W$ is a Hopf ideal of A. Furthermore, since A/I is semisimple, it follows that $\mathcal{I}$ must be the set of all simple A/I-modules. □

Our final consequence uses the fact that any finite dimensional Hopf algebra A is a Frobenius algebra [LS, §5] and hence that every simple A-module is isomorphic to a minimal left ideal of A.

Corollary 7.8. *Let A be a finite dimensional Hopf algebra and let V be an A-module whose left annihilator contains no nonzero Hopf ideal of A. Then every simple A-module is isomorphic to a submodule of $V^{\otimes n}$ for some $n \geq 1$.*

Proof. It follows from Theorem 7.5(ii) that $\mathcal{T}(V) = \oplus \sum_{n=1}^{\infty} V^{\otimes n}$ is a faithful A-module. Now let W be a simple A-module, so that W is isomorphic to a minimal left ideal $L \subseteq A$. Since $L \neq 0$, we have $L\mathcal{T}(V) \neq 0$ and hence $LV^{\otimes n} \neq 0$ for some $n \geq 1$. In particular, there exists $u \in V^{\otimes n}$ with $Lu \neq 0$. But then the minimality of L implies that $W \cong L \cong Lu \subseteq V^{\otimes n}$, as required. □

We remark in closing that the material discussed in this expository paper is, for the most part, quite classical and concrete. It affords an introduction to Hopf algebras, but is not really indicative of the subject as a whole. The interested reader should now go on to learn more about the general theory. Standard references include the books by Abe [A] and Sweedler [Sw]. We especially recommend the more recent monograph by Montgomery [Mo].

References

[A] E. Abe, *Hopf Algebras*, Cambridge Univ. Press, Cambridge, 1977.

[B] W. Burnside, *Theory of Groups of Finite Order*, (reprint of 2nd edition, 1911), Dover, New York, 1955.

[F] K. O. Friedrichs, *Mathematical aspects of the quantum theory of fields, Part V*, Comm. Pure Appl. Math., **6** (1953), 1–72.

[H] Harish-Chandra, *On representations of Lie algebras*, Ann. Math. (2), **50** (1949), 900–915.

[J] N. Jacobson, *Lie Algebras*, Interscience, New York, 1962.

[LS] R. G. Larson and M. E. Sweedler, *An associative orthogonal bilinear form for Hopf algebras*, Amer. J. Math., **91** (1969), 75–94.

[Mi] W. Michaelis, *Properness of Lie algebras and enveloping algebras, I*, Proc. AMS, **101** (1987), 17–23.

[Mo] S. Montgomery, *Hopf Algebras and Their Actions on Rings*, CBMS Conference Notes, Amer. Math. Soc., Providence, 1993.

[N] W. D. Nichols, *Quotients of Hopf algebras*, Comm. Algebra, **6** (1978), 1789-1800.

[PQ] D. S. Passman and D. Quinn, *Burnside's theorem for Hopf algebras*, Proc. AMS, **123** (1995), 327-333.

[R] M. A. Rieffel, *Burnside's theorem for representations of Hopf algebras*, J. Algebra, **6** (1967), 123–130.

[St] R. Steinberg, *Complete sets of representations of algebras*, Proc. AMS, **13** (1962), 746–747.

[Sw] M. E. Sweedler, *Hopf Algebras*, Benjamin, New York, 1969.

Department of Mathematics, University of Wisconsin-Madison, Madison, Wisconsin 53706, USA

E-mail address: passman@math.wisc.edu