COMODULE ALGEBRAS AND GALOIS EXTENSIONS RELATIVE TO
POLYNOMIAL ALGEBRAS, FREE ALGEBRAS, AND ENVELOPING
ALGEBRAS

ALLEN D. BELL

Abstract. This is a preprint version of a paper that will appear in Communications in Algebra 28 (2000) 337–362.

In this paper we study the question of when an $H$-comodule algebra is a faithfully flat Galois extension of its subalgebra of coinvariants for certain Hopf algebras $H$. We note that if $H$ is connected, a faithfully flat Galois extension must actually be cleft and hence a crossed product, and we show that with a different hypothesis, a faithfully flat Galois extension must be a smash product. We also describe faithfully flat Galois extensions when $H$ is pointed cocommutative. We give an explicit description of $H$-comodule algebras when $H$ is a polynomial algebra, a divided power Hopf algebra, a free algebra, or a shuffle algebra. We give necessary and sufficient conditions for an $H$-extension to be faithfully flat Galois in these cases and in the case where $H$ is the enveloping algebra of a Lie algebra; a key ingredient in our analysis is the existence and description of a total integral. In the case where $H = k[x]$, we give a simple example of a flat Galois extension that is not faithfully flat.

Throughout this paper, $k$ is a field, all algebras are $k$-algebras, all maps are $k$-linear, and $H$ is a Hopf algebra. In the first section, we prove some general results about faithfully flat $H$-Galois extensions for special Hopf algebras $H$; the key ingredient is a total integral. We then apply these results to the the case where $H = U(g)$ for a Lie algebra $g$. For example, we note that if $H$ is connected, then an $H$-extension $A \supseteq A^{coH}$ is faithfully flat Galois if and only if there is a total integral $\phi : H \to A$, and in this case, the extension is actually cleft, that is, $A \cong A^{coH} \# H$. We show that for any $H$, if there is a total integral $\phi : H \to A$ that is an algebra homomorphism, then the extension $A \supseteq A^{coH}$ is cleft with a trivial cocycle, so $A \cong A^{coH} \# H$. We then apply these results to the case where $H$ is the enveloping algebra of a Lie algebra and give necessary and sufficient conditions for an $H$-extension to be faithfully flat Galois or to be a smash product. Finally, we give necessary and sufficient conditions for an $H$-extension to be Galois or faithfully flat Galois when $H$ is pointed cocommutative.

In the second section, we study in detail the case where $H = k[x]$ or $H$ is a divided power Hopf algebra. We show that an $H$-comodule structure on an algebra $A$ is determined by a locally nilpotent iterative higher derivation in the first case and a a locally nilpotent derivation $f$ in the second case, and when $k$ has characteristic 0 (in which case $k[x]$ and the divided power Hopf algebra are identical), we show $A \supseteq A^{coH}$ is faithfully flat Galois if and only if there exists $\theta \in A$ with $f(\theta) = 1$. In this case, $A$ is isomorphic to the differential operator ring $A[f[\theta; \delta]$ for the derivation $\delta = \text{ad} \, \theta$, and $f$ corresponds to

1991 Mathematics Subject Classification. 16W30; Secondary 16S40.

Key words and phrases. Hopf algebra, Galois extension, comodule algebra, faithfully flat, locally nilpotent derivation.
the derivation \(d/d\theta\). We also give a simple example of a flat \(k[x]\)-Galois extension that is not faithfully flat.

In the third section and fourth sections, we consider first the case of a polynomial algebra in multiple variables and then the case where \(H\) is a free algebra (with primitive generators) or \(H\) is a shuffle algebra. The results are similar to those in Section 2, although they are naturally more complicated. We show among other things that if \(A\) is an \(H\)-comodule algebra and either \(A\) is commutative and \(H\) is a polynomial algebra or \(A\) is arbitrary and \(H\) is a free algebra, then \(A \supseteq A^{\co H}\) is faithfully flat Galois if and only if \(A\) is actually a smash product \(A^{\co H} \# H\).

For background material on Hopf algebras, we refer the reader to the books [7] and [10]. We will generally use [7] as our reference; however, many of the proofs in this book are omitted or only sketched, so whenever possible, we also provide a reference to an original source.

Some of the work for this paper was done while the author was visiting the University of California at Santa Barbara and the University of Washington, and he wishes to thank the mathematics departments at both institutions for their hospitality. He also wishes to thank Ken Goodearl for some stimulating conversations and for suggesting Example 2.4.

1. General Results

Let \(k\) be a field and let \(H\) be a Hopf algebra over \(k\). We begin by defining some of the terms that will occur in this paper. For more detail and discussion, we refer the reader to [7], particularly chapters 5, 7, and 8. When dealing with comodules we will always work on the right and when dealing with modules we will work on the left. Thus an \(H\)-comodule algebra is an algebra \(A\) that is a right \(H\)-comodule via a structure map \(\rho : A \rightarrow A \otimes_k H\) which is an algebra homomorphism. The subset of \(H\)-coinvariants is \(A^{\co H} = \{a \in A \mid \rho(a) = a \otimes 1\}\); it is a subalgebra and subcomodule. We refer to the extension \(A \supseteq A^{\co H}\) as an \(H\)-extension. The Galois map associated to this extension is the left \(A\)-module map \(\beta : A \otimes_{A^{\co H}} A \rightarrow A \otimes_k H\) defined by \(\beta(a \otimes b) = (a \otimes 1)\rho(b) = \sum (b) ab_{(0)} \otimes b_{(1)}\). Note that if \(A\) is commutative, then \(\beta\) is an algebra homomorphism. We say the extension \(A \supseteq A^{\co H}\) is Galois if \(\beta\) is a bijection.

Recall that an extension \(A \supseteq B\) of rings is right flat if whenever \(f : M \rightarrow N\) is a injective homomorphism of left \(B\)-modules, the induced homomorphism \(id_A \otimes f : A \otimes_B M \rightarrow A \otimes_B N\) is injective. The extension is right faithfully flat if \(f\) is injective if and only if \(id_A \otimes f\) is injective. Left flat and left faithfully flat extensions are defined in the obvious way. By [7, Theorem 8.5.6],[8, Theorem 1], if the extension \(A \supseteq A^{\co H}\) is Galois, then it is right faithfully flat if and only if it is left faithfully flat, and so we will simply speak of faithfully flat Galois extensions. Faithfully flat Galois extensions are of great interest due to the just-cited theorem of Schneider. He proves that if \(H\) has a bijective antipode, then an \(H\)-extension \(A \supseteq A^{\co H}\) is faithfully flat Galois if and only if the the functor \(\cdot \otimes_{A^{\co H}} A\) defines an equivalence from the category of right \(A^{\co H}\)-modules to the category of right \((H, A)\)-Hopf modules (simultaneous right \(A\)-modules and right \(H\)-comodules).

Suppose \(A\) is an \(H\)-comodule algebra. A total integral is an \(H\)-comodule map \(\phi : H \rightarrow A\) such that \(\phi(1) = 1\). (To say \(\phi\) is an \(H\)-comodule map is to say that \(\rho \circ \phi = (\phi \otimes id) \circ \Delta\).) We say the extension \(A \supseteq A^{\co H}\) is cleft if there is a total integral \(\phi : H \rightarrow A\) that is convolution invertible, i.e., such that there exists a linear map \(\psi : H \rightarrow A\) with \(\phi * \psi(h) = \psi * \phi(h) = \epsilon(h)1_A\) for all \(h \in H\). The extension \(A \supseteq A^{\co H}\) is cleft if and only
if $A \cong A^{coH} \#_{\sigma} H$ as $H$-comodule algebras for some crossed product $A^{coH} \#_{\sigma} H$: see [7, Theorem 7.2.2],[4, Theorem 11]. In this case $A \supseteq A^{coH}$ is a free Galois extension and so is faithfully flat: see [7, Theorem 8.2.4],[4, Theorem 9].

A Hopf algebra $H$ is said to be connected if every nonzero subcoalgebra of $H$ contains 1. Most of the results and examples in this paper concern connected Hopf algebras. The following well-known result gives us a large class of connected Hopf algebras. To state it, we first recall that an element $x \in H$ is said to be primitive if $\Delta(x) = x \otimes 1 + 1 \otimes x$. This in turn implies $\epsilon(x) = 0$ and $S(x) = -x$ (where $S$ is the antipode of $H$).

**Lemma 1.1.** Let $H$ be a Hopf algebra that is generated as an algebra by primitive elements. Then $H$ is connected.

**Proof.** This is part of [10, Section 11.0, Exercise 2]; it also follows from [7, Lemma 5.5.1] as in the proof of [7, Proposition 5.5.3(1)].

We now turn to the characterization of faithfully flat Galois extensions for connected Hopf algebras.

**Lemma 1.2.** Let $H$ be a connected Hopf algebra, let $A$ be an $H$-comodule algebra, and let $\phi : H \to A$ be a total integral. Then $\phi$ is convolution invertible.

**Proof.** This is a special case of [10, Lemma 9.2.3].

**Proposition 1.3.** Let $H$ be a connected Hopf algebra and $A$ an $H$-comodule algebra. Then the following statements are equivalent.

1. The extension $A \supseteq A^{coH}$ is faithfully flat Galois.
2. The extension $A \supseteq A^{coH}$ is cleft.
3. There is a total integral $\phi : H \to A$.

**Proof.** (3) $\Rightarrow$ (2) This follows from Lemma 1.2.

(2) $\Rightarrow$ (1) This follows from the remarks after the definition of cleft.

(1) $\Rightarrow$ (3) [7, Theorem 8.5.6],[8, Theorem 1] states that if $A \supseteq A^{coH}$ is faithfully flat Galois, then $A$ is an injective $H$-comodule. By [3, Theorem 1.6], this last condition is equivalent to the existence of a total integral $\phi : H \to A$.

Proposition 1.3 demonstrates the importance of a total integral. The next result shows that when a total integral of a special type exists, we get an even stronger conclusion.

**Proposition 1.4.** Let $H$ be a Hopf algebra with antipode $S$, let $A$ be an $H$-comodule algebra, and let $\phi : H \to A$ be a total integral that is an algebra homomorphism. Then $\phi$ is convolution invertible, $A$ is an $H$-module algebra via an action that makes $A^{coH}$ a submodule, and $A \cong A^{coH} \# H$ as $H$-comodule algebras. (This is an ordinary smash product with trivial cocycle.)

Conversely, if there is an action of $H$ that makes $A^{coH}$ into an $H$-module algebra such that $A \cong A^{coH} \# H$ as $H$-comodule algebras, then there is a total integral $\phi : H \to A$ that is an algebra homomorphism.

**Proof.** Assume $\phi : H \to A$ is a total integral and an algebra homomorphism, and set $\psi = \phi \circ S$. Then

$$\phi \ast \psi(h) = \sum_{(h)} \phi(h_{(1)})\phi(S(h_{(2)})) = \phi(\sum_{(h)} h_{(1)}S(h_{(2)})) = \phi(\epsilon(h)1_{H}) = \epsilon(h)1_{A}.$$
A similar calculation shows \( \psi \ast \phi(h) = \epsilon(h)1_A \), so \( \psi \) is the convolution inverse to \( \phi \).
By [7, Proposition 7.2.3],[4, Theorem 11], this implies \( A \cong A^{\text{co}H} \#_{\sigma} H \) where the cocycle \( \sigma : H \times H \rightarrow A \) is defined by

\[
\sigma(x, y) = \sum_{(x), (y)} \phi(x_{(1)})\phi(y_{(1)})\phi(S(x_{(2)}y_{(2)})) \\
= \sum_{(x)} \phi(x_{(1)})\left( \sum_{(y)} y_{(1)}S(y_{(2)}) \right)\phi(S(x_{(2)})) = \epsilon(y)\phi\left( \sum_{(x)} x_{(1)}S(x_{(2)}) \right) = \epsilon(x)\epsilon(y)1_A.
\]

This is the trivial cocycle and so \( A \cong A^{\text{co}H} \# H \). The action of \( H \) on \( A^{\text{co}H} \) is given by \( h.a = \sum_{(h)} \phi(h_{(1)})a\phi(S(h_{(2)})) \), and the reader may easily verify that this actually defines an \( H \)-module algebra action on \( A \).

We can prove an even stronger version of the converse. Suppose that \( B \) is an \( H \)-module algebra and we make \( B \# H \) into an \( H \)-comodule algebra via \( \text{id}_B \otimes \Delta \). (This is our situation, with \( A^{\text{co}H} = B \).) If \( \Phi : B \# H \rightarrow A \) is an \( H \)-comodule algebra homomorphism, then it is easy to see that \( \phi : H \rightarrow A \) defined by \( \phi(h) = \Phi(1\# h) \) is a total integral and an algebra homomorphism.

As an example, we apply the above results to the case where \( H \) is the enveloping algebra of a Lie algebra or a restricted Lie algebra.

**Proposition 1.5.** Let \( \mathfrak{g} \) be a Lie algebra over \( k \), let \( H = U(\mathfrak{g}) \) be its enveloping algebra, and let \( A \) be an \( H \)-comodule algebra. Then \( A \supseteq A^{\text{co}H} \) is faithfully flat Galois if and only if there is a map \( \lambda : \mathfrak{g} \rightarrow A \) such that \( \rho(\lambda(x)) = \lambda(x) \otimes 1 + 1 \otimes x \) for all \( x \in \mathfrak{g} \).

Suppose there is a map \( \lambda \) as above such that \( \lambda([x, y]) = \lambda(x)\lambda(y) - \lambda(y)\lambda(x) \) for all \( x, y \in \mathfrak{g} \). Then \( A \) becomes a \( U(\mathfrak{g}) \)-module algebra under the action \( x.a = \lambda(x)a - a\lambda(x) \) for \( x \in \mathfrak{g} \), and \( A^{\text{co}H} \) is a submodule. Moreover, \( A \cong A^{\text{co}H} \# U(\mathfrak{g}) \) as \( U(\mathfrak{g}) \)-comodule algebras.

**Proof.** \( H \) is connected by any of [7, Proposition 5.5.3], [10, Proposition 11.0.9], Lemma 1.1. Thus if \( A \) is an \( H \)-comodule algebra, Proposition 1.3 states that \( A \supseteq A^{\text{co}H} \) is faithfully flat Galois if and only if there exists a total integral \( \phi : U(\mathfrak{g}) \rightarrow A \). Suppose such a \( \phi \) exists and \( x \in \mathfrak{g} \). Then \( \rho(\phi(x)) = (\phi \otimes \text{id}) \circ \Delta(x) = \phi(x) \otimes 1 + 1 \otimes x \), so we may set \( \lambda = \phi|_{\mathfrak{g}} \).

Conversely, suppose there is a map \( \lambda : \mathfrak{g} \rightarrow A \) such that \( \rho(\lambda(x)) = \lambda(x) \otimes 1 + 1 \otimes x \) for all \( x \in \mathfrak{g} \). Then we claim \( \lambda \) extends to a total integral \( \phi : U(\mathfrak{g}) \rightarrow A \) and hence that \( A \supseteq A^{\text{co}H} \) is faithfully flat Galois and \( A \cong A^{\text{co}H} \#_{\sigma} U(\mathfrak{g}) \).

To see this, we need to introduce some notation. Let \( X \) be a basis for \( \mathfrak{g} \) and let \( \mathbf{n} \) be an \( X \)-multi-index. This means \( \mathbf{n} \) is a function from \( X \) to the non-negative integers with the property that \( \mathbf{n}(x) = 0 \) for all but finitely many \( x \in X \). We add and (when possible) subtract multi-indices in the obvious way, and we let \( \mathbf{0} \) denote the \( X \)-multi-index that is identically 0. Given two \( X \)-multi-indices \( \mathbf{n}, \mathbf{i} \), we define \( \mathbf{i} \leq \mathbf{n} \) if \( \mathbf{i}(x) \leq \mathbf{n}(x) \) for all \( x \in X \). We define \( \mathbf{n}! = \prod_{x \in X} \mathbf{n}(x)! \) and we define \( \binom{\mathbf{n}}{\mathbf{i}} \) to be \( \frac{\mathbf{n}!}{\mathbf{i}! \mathbf{n}!(\mathbf{n} - \mathbf{i})!} \) if \( \mathbf{i} \leq \mathbf{n} \) and 0 otherwise. Note that \( \binom{\mathbf{n}}{\mathbf{i}} = \prod_{x \in X} \binom{\mathbf{n}(x)}{\mathbf{i}(x)} \).

We let \( x^{\mathbf{n}} \) denote the monomial \( \prod_{x \in X} x^{\mathbf{n}(x)} \) (we fix an order on \( X \) and maintain that order in this product). The Poincaré-Birkhoff-Witt Theorem tells us that the monomials \( x^{\mathbf{n}} \) form a vector space basis for \( U(\mathfrak{g}) \). Using multi-index notation, we can express the comultiplication on \( U(\mathfrak{g}) \) as follows: \( \Delta(x^{\mathbf{n}}) = \sum_{0 \leq i \leq \mathbf{n}} \binom{\mathbf{n}}{\mathbf{i}} x^i \otimes x^{\mathbf{n} - \mathbf{i}} \).
We now define a map \( \phi : U(\mathfrak{g}) \rightarrow A \) by \( \phi(x^n) = \prod_{x \in X} \lambda(x)^{n(x)} \). Using the fact that \( \rho \) is an algebra homomorphism and that \( a \otimes 1 \) and \( 1 \otimes x \) commute (whence the Binomial Theorem is applicable), we obtain:

\[
\rho \circ \phi(x^n) = \prod_{x \in X} (\lambda(x) \otimes 1 + 1 \otimes x)^{n(x)} = \prod_{x \in X} \left( \sum_{i=0}^{n(x)} \binom{n(x)}{i} \lambda(x)^i \otimes x^{n(x)-i} \right) = \sum_{0 \leq i \leq n} \left( \prod_{x \in X} \lambda(x)^{n(x)} \right) \otimes x^{n-i} = (\phi \circ \text{id}) \circ \Delta(x^n)
\]

This shows \( \phi \) is a total integral.

Suppose that \( \lambda \) satisfies \( \lambda([x, y]) = \lambda(x)\lambda(y) - \lambda(y)\lambda(x) \) for all \( x, y \in \mathfrak{g} \). The universal property of \( U(\mathfrak{g}) \) implies that \( \lambda \) extends to an algebra homomorphism \( : U(\mathfrak{g}) \rightarrow A \). Since \( \mathfrak{g} \) is an algebra homomorphism, to check that \( \phi \) is a comodule map, it suffices to check that \( \rho \circ \phi = (\phi \otimes \text{id}) \circ \Delta \) holds on a set of algebra generators of \( U(\mathfrak{g}) \). Since \( \mathfrak{g} \) generates \( U(\mathfrak{g}) \) as an algebra, this is precisely our assumption on \( \lambda \). Thus \( \phi \) is a total integral. By Proposition 1.4, this implies that \( A \) becomes a \( U(\mathfrak{g}) \)-module algebra under the action \( x.a = \lambda(x)a - a\lambda(x) \) for \( x \in \mathfrak{g} \), with \( \mathfrak{g}^{\mathfrak{co} H} \) a submodule. Moreover, \( A \cong \mathfrak{g}^{\mathfrak{co} H} \# U(\mathfrak{g}) \) as \( U(\mathfrak{g}) \)-comodule algebras.

**Proposition 1.6.** Suppose \( \text{char } k = p > 0 \), let \( (\mathfrak{g}, [\cdot, \cdot]) \) be a restricted Lie algebra, and let \( H = u(\mathfrak{g}) \) be the corresponding restricted enveloping algebra (see [7, Definition 2.3.2],[9, Chapter 2] for details). Let \( A \) be an \( H \)-comodule algebra. Then \( A \cong \mathfrak{g}^{\mathfrak{co} H} \# U(\mathfrak{g}) \) is faithfully flat Galois if and only if there is a map \( \lambda : \mathfrak{g} \rightarrow A \) such that \( \rho(\lambda(x)) = \lambda(x) \otimes 1 + 1 \otimes x \) for all \( x \in \mathfrak{g} \).

Suppose the \( \lambda \) above has the additional properties that \( \lambda([x, y]) = \lambda(x)\lambda(y) - \lambda(y)\lambda(x) \) and \( \lambda(x^{[p]}) = \lambda(x)^p \) for all \( x, y \in \mathfrak{g} \). Then \( A \) is a \( u(\mathfrak{g}) \)-module algebra and \( A \cong \mathfrak{g}^{\mathfrak{co} H} \# u(\mathfrak{g}) \) as \( u(\mathfrak{g}) \)-comodule algebras.

**Proof.** The proof follows the same lines as the proof of Proposition 1.5.

We now wish to generalize Proposition 1.3. We begin by reviewing some background material; for more detail, see [7, Chapter 5]. Recall that \( g \in H \) is said to be grouplike if \( \Delta(g) = g \otimes g \) and \( \epsilon(g) = 1 \). We denote by \( G(H) \) the set of grouplike elements of \( H \); this is a multiplicative subgroup of \( H \). A Hopf algebra is said to be pointed if every simple subcoalgebra is 1-dimensional, that is, if every nonzero subcoalgebra contains a grouplike element.

For every \( g \in G(H) \), there is a maximal subcoalgebra \( H(g) \) containing \( g \). This is called the \( g \)-component of \( H \). The component \( H(1) \) is a Hopf subalgebra of \( H \). The sum of components \( H(g) \) for distinct \( g \) is always direct. If \( H \) is pointed cocommutative, then \( H = \bigoplus_{g \in G(H)} H(g) \), but this equality does not hold in general. If \( H = \bigoplus_{g \in G(H)} H(g) \), then this decomposition is a \( G(H) \)-grading of \( H \) as an algebra. (See [7, §5.6],)

Suppose that \( H = \bigoplus_{g \in G(H)} H(g) \) and that \( A \) is an \( H \)-comodule algebra. If we define \( A(g) = \{ a \in A \mid \rho(a) \in A \otimes H(g) \} \), then \( A(g) \) is a submodule of \( A \) and \( A = \bigoplus_{g \in G(H)} A(g) \) is a \( G(H) \)-grading of the algebra \( A \). Note that \( A(1) \) is an \( H(1) \)-comodule algebra and that \( A^{\mathfrak{co} H} = A(1)^{\mathfrak{co} H(1)} \). Recall that a \( G \)-graded algebra \( A = \bigoplus_{g \in G} A(g) \) is strongly graded if \( A(x)A(y) = A(xy) \) for all \( x, y \in G \).
Proposition 1.7. Retain the notation of the preceding paragraphs and let $H$ be a Hopf algebra with $H = \oplus_{g \in G(H)} H(g)$. Let $A$ be an $H$-comodule algebra, so $A$ is $G(H)$-graded. Then the following statements are true.

1. The extension $A \supseteq A^{coH}$ is $H$-Galois if and only if $A$ is strongly $G(H)$-graded and $A(1) \supseteq A(1)^{coH(1)}$ is $H(1)$-Galois.

2. The extension $A \supseteq A^{coH}$ is faithfully flat Galois if and only if $A$ is strongly $G(H)$-graded and there is a total integral $\phi : H(1) \to A(1)$ (equivalently, a total integral $\phi : H \to A$).

Proof. For convenience, set $B = A^{coH} = A(1)^{coH(1)}$ and let $\beta : A \otimes_B A \to A \otimes_k H$ be the Galois map. Set $G = G(H)$.

(1) We can decompose $A \otimes_B A$ as a direct sum of all $A(x) \otimes_B A(y)$ for $x, y \in G$ (each $A(x)$ is an $A(1)$-bimodule and hence a $B$-bimodule, so this makes sense); we can decompose $A \otimes_k H$ in a similar fashion. We have $\beta(A(x) \otimes_B A(y)) \subseteq A(xy) \otimes_k H(y)$, whence for any $x, y \in G$, $\beta$ restricts to a map $\beta_{x,y} : A(x) \otimes_B A(y) \to A(xy) \otimes_k H(y)$. The decompositions noted above show that $\beta$ is a bijection if and only if each restriction $\beta_{x,y}$ is a bijection.

Suppose first that $\beta$ is a bijection. Then $\beta_{1,1}$ is just the Galois map for $A(1)$ as an $H(1)$-comodule algebra, so by the previous paragraph, $A(1) \supseteq A(1)^{coH(1)}$ is Galois.

Next, let $x, y \in G$: we wish to show $A(x) \otimes_B A(y) = A(xy)$. We already know $A(x) \otimes_B A(y) \subseteq A(xy)$; let $a \in A(xy)$. By assumption, $\beta_{x,y}$ is a bijection, so there exist $r_1, \ldots, r_m \in A(x)$, $s_1, \ldots, s_n \in A(y)$ such that $a \otimes y = \beta(\sum_i r_i \otimes s_i) = \sum_i \sum_{(n)} r_i(s_i)(0) \otimes (s_i)(1)$. If we apply the map $id \otimes \epsilon$ to this equality, we obtain $a = \sum_i r_i s_i$. This shows $A$ is strongly $G$-graded.

Now suppose the converse is valid, that is, suppose $\beta_{1,1}$ is a bijection with inverse $\gamma_{1,1}$ and suppose $A$ is strongly $G$-graded. We wish to show each $\beta_{x,y}$ is a bijection. We begin by assuming $x = 1$. Since $A$ is strongly graded, there exist $r_1, \ldots, r_m \in A(y^{-1})$, $s_1, \ldots, s_m \in A(y)$ with $\sum_i r_i s_i = 1$. Define $\gamma_{1,y} : A(y) \otimes_k H(y) \to A(1) \otimes_B A(y)$ by

$$\gamma_{1,y}(a \otimes h) = \sum_i \sum_{(r_i)} a(r_i)(0) \otimes h(r_i)(1)(1 \otimes s_i) = \sum_i \gamma_{1,1}((a \otimes h)\rho(r_i))(1 \otimes s_i).$$

We will show $\gamma_{1,y}$ is the inverse of $\beta_{1,y}$.

Before proceeding, let us make an observation: if $t \in A \otimes_{A^{coH}} A$ and $a' \in A$, then $\beta(t(1 \otimes a')) = \beta(t)\rho(a')$. Now if $a \in A(y)$, $h \in H(y)$, our observation shows

$$\beta_{1,y} \circ \gamma_{1,y}(a \otimes h) = \sum_i \beta\left(\gamma_{1,1}((a \otimes h)\rho(r_i))\right)\rho(s_i)$$

$$= \sum_i (a \otimes h)\rho(r_i)\rho(s_i) = (a \otimes h)\rho\left(\sum_i r_i s_i\right) = (a \otimes h)(1 \otimes 1) = a \otimes h.$$ 

If $a' \in A(1), a \in A(y)$, then

$$\gamma_{1,y} \circ \beta_{1,y}(a' \otimes a) = \gamma_{1,y}(\sum_{(a)} a'a_{(0)} \otimes a_{(1)}) = \sum_i \gamma_{1,1}\left(\sum_{(a), (r_i)} a'a_{(0)}(r_i)(0) \otimes a_{(1)}(r_i)(1)\right)(1 \otimes s_i)$$

$$= \sum_i \gamma_{1,1}(\beta(a' \otimes ar_i))(1 \otimes s_i) = (a' \otimes a)(1 \otimes \sum_i r_i s_i) = a' \otimes a.$$

This shows $\beta_{1,y}$ and $\gamma_{1,y}$ are inverses.
Now let \( x, y \in G \) and recall the following standard fact about strong gradings: the multiplication map \( m_{x,y} : A(x) \otimes A(y) \rightarrow A(xy) \) is an isomorphism. (The inverse is the map \( a \mapsto \sum r_i \otimes s_i \) with \( r_1, \ldots, r_m, s_1, \ldots, s_n \) as above.) Since any \( \beta_{x,y} \) is a left \( A \)-module map, the diagram below commutes.

\[
\begin{array}{ccc}
A(x) \otimes A(1) & \xrightarrow{\text{id} \otimes \beta_{1,y}} & A(y) \\
\downarrow m_{x,1} \otimes \text{id} & & \downarrow m_{x,y} \otimes \text{id} \\
A(x) \otimes_B A(y) & \xrightarrow{\beta_{x,y}} & A(xy) \otimes_k H(y)
\end{array}
\]

As every map except possibly \( \beta_{x,y} \) in this diagram is a bijection, \( \beta_{x,y} \) must be a bijection.

This completes the proof that \( \beta \) is a bijection.

(2) Once we know that \( A \supseteq A^{co H} \) is Galois, [7, Theorem 8.5.6], [8, Theorem I] plus [3, Theorem 1.6] shows that \( A \supseteq A^{co H} \) is faithfully flat Galois if and only if there exists a total integral \( \phi : H \rightarrow A \), just as in the proof of (1) \( \Rightarrow \) (3) in Proposition 1.3. Furthermore, any total integral must take \( H(1) \) into \( A(1) \). Thus if \( A \supseteq A^{co H} \) is faithfully flat Galois, there is a total integral from \( H(1) \) to \( A(1) \) by Proposition 1.3.

Conversely, suppose there is a total integral \( \phi : H(1) \rightarrow A(1) \). Since \( H \) is a coalgebra direct sum of the \( H(g) \)'s, we may extend \( \phi \) to \( H \) by declaring the extension to be identically 0 on each \( H(g) \) with \( g \neq 1 \). This yields a total integral \( \phi : H \rightarrow A \).

\[
\begin{proof}
\end{proof}
\]

2. The Case Where \( H = k[x] \) or \( H \) is a Divided Power Hopf Algebra

In this section we will study \( H \)-comodule algebras and \( H \)-Galois extensions in case \( H = k[x] \) or \( H \) is a divided power Hopf algebra. When \( H = k[x] \), an \( H \)-comodule algebra is essentially an algebra \( A \) equipped with a locally nilpotent iterative higher derivation, and the extension \( A^{co H} \) is faithfully flat Galois if and only if there is an element of \( A \) taken to 1 by the first map in the higher derivation and to 0 by the higher maps. In this case, we show that \( A \) is isomorphic as an \( H \)-comodule algebra to a smash product \( A^{co H} \# H \), which is just a differential operator ring \( A^{co H}[\theta; \delta] \). We also give an example of a flat \( k[x] \)-Galois extension that is not faithfully flat.

When \( H \) is a divided power Hopf algebra, an \( H \)-comodule algebra is essentially an algebra \( A \) equipped with a locally nilpotent derivation \( f \). We give explicit conditions for an \( H \)-extension to be faithfully flat Galois: in case \( \text{char} \, k = 0 \), the extension is faithfully flat Galois precisely when \( f(a) = 1 \) for some \( a \in A \).

We begin with case \( H = k[x] \). To make \( k[x] \) into a Hopf algebra, we require that \( x \) be primitive; this implies that \( n x^n = \sum_{i=0}^{n} \binom{n}{i} x^i \otimes x^{n-i} \) for all \( n \).

Let \( C \) be an \( H \)-comodule. Then there are maps \( f_n : C ightarrow C \) for each non-negative integer \( n \) such that the comodule structure of \( C \) is defined by \( \rho_C(c) = \sum_{n=0}^{\infty} f_n(c) \otimes x^n \).

The counitary law implies that \( f_0 = \text{id}_C \) and the coassociative law \( (\text{id} \otimes \Delta) \circ \rho_C = (\rho_C \otimes \text{id}) \circ \rho_C \) implies that

\[
\sum_n \sum_{i=0}^{n} \binom{n}{i} f_n(c) \otimes x^i \otimes x^{n-i} = \sum_{i,j} f_i \circ f_j(c) \otimes x^i \otimes x^j.
\]

This equality is valid if and only if \( f_i \circ f_j = \binom{i+j}{i} f_{i+j} \) for all \( i, j \). When this composition law holds and \( f_0 = \text{id} \), we say the sequence \( f = (f_0, f_1, \ldots) \) is iterative. There is one other requirement: \( \rho_C(c) \) must be a finite sum, so the sequence \( f \) must be locally nilpotent in the
Proof. To the derivation $H$ an algebra, where $\rho(c) = \sum_{n=0}^{\infty} f_n(c) \otimes x^n$. 

It is easy to verify that if $(D, g)$ and $(C, f)$ are $H$-comodules, then a comodule map $\phi : D \to C$ is just a linear map satisfying $\phi \circ g_n = f_n \circ \phi$ for all $n$.

Now suppose $A$ is an algebra and $(A, f)$ is an $H$-comodule. In order for $A$ to be an $H$-comodule algebra, the comodule structure map $\rho$ defined from $f$ as above must be multiplicative. Let $a, b \in A$. Then

$$\rho(a) \rho(b) = \left(\sum_i f_i(a) \otimes x^i\right) \left(\sum_j f_j(b) \otimes x^j\right) = \sum_{i,j} f_i(a) f_j(b) \otimes x^{i+j} = \sum_n \left(\sum_{i+j=n} f_i(a) f_j(b)\right) \otimes x^n.$$ 

For this to equal $\rho(ab)$, we need $f_n(ab) = \sum_{i+j=n} f_i(a) f_j(b)$ for all $n$. A sequence $f$ with $f_0 = \id$ satisfying this last equality is called a higher derivation on $A$. Thus $H$-comodule algebras correspond to pairs $(A, f)$ where $A$ is an algebra and $f$ is a locally nilpotent iterative higher derivation on $A$. If we set $A^f = \bigcap_{n=0}^{\infty} \ker f_n$, then $A^{coH} = A^f$.

The map $f_1$ is always a derivation. If $\text{char} k = 0$, then an iterative higher derivation is determined uniquely by any derivation $f = f_1$ via the formula $f_i = f^i / i!$, where $f^i$ is the $i$-fold composition. In this case we generally write $(A, f)$ in place of $(A, f)$. Note then that $A^{coH} = A^f = \ker f$ and that $f$ is locally nilpotent if and only if $f$ is locally nilpotent in the usual sense.

**Proposition 2.1.** Let $H = k[x]$ and let $(A, f)$ be an $H$-comodule algebra, where $f$ is a locally nilpotent iterative higher derivation on $A$. Then the extension $A \supseteq A^{coH}$ is faithfully flat Galois if and only if there is an element $\theta \in A$ with $f_1(\theta) = 1$ and $f_n(\theta) = 0$ for $n \geq 2$.

If this is the case, then $A$ is an $H$-module algebra via the action $x.a = \text{ad} \theta(a)$, where $\text{ad} \theta(a) = \theta a - a \theta$. Moreover, $A$ is isomorphic as an $H$-comodule algebra to the differential operator ring $A^f[\theta; \text{ad} \theta]$.

**Proof.** Since $H = U(\mathfrak{g})$ where $\mathfrak{g} = kx$ is the unique one-dimensional Lie algebra, Proposition 1.5 implies $A \supseteq A^{coH}$ is faithfully flat Galois if and only if there is a $\theta \in A$ with $\rho(\theta) = \theta \otimes 1 + 1 \otimes x$. This holds if and only if $f_1(\theta) = 1$ and $f_n(\theta) = 0$ for $n \geq 2$.

Since $\mathfrak{g}$ is one-dimensional, the hypothesis in the second paragraph of Proposition 1.5 is satisfied whenever $\theta$ exists. Thus we have $A \cong A^f[\theta]$ and $A$ is isomorphic as an $H$-comodule algebra to the differential operator ring $A^f[\theta]$.

**Corollary 2.2.** Suppose $\text{char} k = 0$, let $H = k[x]$, and let $(A, f)$ be an $H$-comodule algebra, where $f$ is a locally nilpotent derivation on $A$. Then the extension $A \supseteq A^{coH}$ is faithfully flat Galois if and only if there is an element $\theta \in A$ with $f(\theta) = 1$. If this is the case, then $A$ is an $H$-module algebra via the action $x.a = \text{ad} \theta(a)$ and $A$ is isomorphic as an $H$-comodule algebra to the differential operator ring $A^f[\theta; \text{ad} \theta]$, with $f$ corresponding to the derivation $d/d\theta$.

**Remark 2.3.** If $\text{char} k = p > 0$, then $A = k[x]/(x^{pn})$ is a Hopf algebra quotient of $k[x]$. We can describe $H$-comodule algebras via iterative higher derivations $f$ on $A$ with $f_n = 0$ for all $n \geq p^n$. We get a result like Proposition 2.1: $A \supseteq A^{coH}$ is faithfully flat Galois if and only if there is a $\theta$ with $f_1(\theta) = 1$ and $f_n(\theta) = 0$ for $n \geq 2$. If $\theta^{p^{n}} = 0$, then
A \cong A^{\text{co}} \# H \cong A^f[\theta; \text{ad}\theta]/(\theta^p n). This example is discussed in [5, Example 3 in Sections 1&2], [3, Example 1.8(3)], where another condition is stated: \( A \supseteq A^{\text{co}} H \) is faithfully flat Galois if and only if there exists \( \theta \in A \) with \( f_{p^n-1}(a) = 1 \).

For the Hopf algebra \( H = k[x]/(x^p) \), an \( H \)-comodule algebra is determined by an algebra \( A \) equipped with a derivation \( f \) such that \( f^p = 0 \). This \( f \) uniquely determines the appropriate iterative higher derivation, and we obtain the analog of Corollary 2.2: \( A \supseteq A^{\text{co}} H \) is faithfully flat Galois if and only if there exists \( \theta \in A \) with \( f(\theta) = 1 \), and in this case \( A \cong A^{\text{co}} H \# H \).

The next example shows that a flat \( k[x] \)-Galois extension need not be faithfully flat.

**Example 2.4.** Let \( H = k[x] \) and let \( A = \mathcal{O}(SL_2) = k[a, b, c, d]/(ad - bc - 1) \); we will continue to denote the images of the variables \( a, b, c, d \) in \( A \) by \( a, b, c, d \). If \( \text{char } k = 0 \), make \( A \) into an \( H \)-comodule algebra via the locally nilpotent derivation \( f : A \rightarrow A \) defined by \( f(a) = c, f(b) = d, f(c) = f(d) = 0 \). For general \( k \), make \( A \) into an \( H \)-comodule algebra via the higher derivation \( f \) defined by \( f_n(a^i) = \binom{i}{n} a^{i-n} c^n \), \( f_n(b^i) = \binom{i}{n} b^{i-n} d^n \), \( f_n(c^i) = f_n(d^i) = 0 \) for all \( i, n \). (As usual, we set \( \binom{i}{n} = 0 \) if \( i < n \).) Then \( A \supseteq A^{\text{co}} H \) is a flat Galois extension that is not faithfully flat. We will only show this under the assumption that \( \text{char } k = 0 \). We leave the case \( \text{char } k = p > 0 \) to the interested reader; the only difference is in the proof of the equality \( A^{\text{co}} H = k[c, d] \), where it becomes necessary to apply the maps \( f_{p^n} \) for all \( n \) instead of just the map \( f \) in the proof below.

Clearly \( k[c, d] \subseteq A^f = A^{\text{co}} H \). We begin by showing equality holds. We can re-write the defining relation as \( ad = bc + 1 \); it is then easy to see (using for example, Bergman’s Diamond Lemma, [2, Theorem 1.2]) that a basis for \( A \) consists of all monomials in \( a, b, c, d \) that do not contain both \( a \) and \( d \). Explicitly, a basis is \( \{ a^i b^j c^k | i > 0, j, k \geq 0 \} \cup \{ b^i c^k d^l | j, k, l \geq 0 \} \). It makes sense to speak of the total degree of elements of \( A \): this degree defines a filtration on \( A \) that is preserved by \( f \).

Note that \( f(b^i c^k d^l) = j b^{i-1} c k d^{l+1} \) and if \( i > 0 \),

\[
f(a^i b^j c^k) = ia^{i-1} b^j c^{k+1} + ja^i b^{i-1} c d = a^{i-1} b^{i-1} c [i b c + j a d] = (i+j)a^{i-1} b^{i-1} c^{k+1} + ja^{i-1} b^{i-1} c^k.
\]

This shows that if \( M, M' \) are distinct monomials of degree \( n \) and \( f(M), f(M') \) are nonzero, then the terms of degree \( n \) in \( f(M), f(M') \) are distinct.

Now let \( p \in \text{ker } f \) have degree \( n \). Since \( f(p) = 0 \), this last observation shows that every term \( M \) of degree \( n \) occurring in \( p \) must be sent to \( 0 \) by \( f \). Thus if \( M = \lambda a^i b^j c^k \), we must have \( i + j = 0 \), and if \( M = \lambda b^i c^k d^l \), we must have \( j = 0 \). It follows that the terms of highest total degree in \( p \) are of the form \( \lambda c^k d^l \). Since such terms are in \( \text{ker } f \), we can conclude by induction on \( n \) that \( p \in k[c, d] \). This shows \( A^f = k[c, d] \).

We can write \( A = A^f[a, b]/(da - cb - 1) \), so by [6, Corollary 22.6], we know \( A \) is flat as an \( A^f \)-module. However, if \( I = cA^f + dA^f \triangleleft A^f \), then \( IA \) contains \( da - cb = 1 \), so \( IA = A \). Thus \( A^f / I \otimes_{A^f} A = 0 \); this shows that \( A \) is not faithfully flat as an \( A^f \)-module.

Finally, we need to show that the Galois map \( \beta : A \otimes_{A^f} A \rightarrow A \otimes_k H \cong A[x] \) is a bijection. By the universal property of polynomial rings, there is a unique algebra homomorphism \( \gamma : A \otimes_k k[x] \rightarrow A \otimes_{A^f} A \) such that \( \gamma(1 \otimes x) = a \otimes b - b \otimes a \) and \( \gamma(r \otimes 1) = r \otimes 1 \) for all \( r \in A \). This map is clearly a left \( A \)-module map. We will show that \( \beta \) and \( \gamma \) are inverses. As we noted when \( \beta \) was defined, \( \beta \) is always a left \( A \)-module map, and since \( A \) is commutative, \( \beta \) is an algebra homomorphism.
Since $A \otimes_k H$ is generated as an algebra and left $A$-module by $1 \otimes x$, to show $\beta \circ \gamma$ is the identity, it suffices to note
\[
\beta \circ \gamma(1 \otimes x) = \beta(a \otimes b - b \otimes a) = (a \otimes 1)(b \otimes 1 + d \otimes x) - (b \otimes 1)(a \otimes 1 + c \otimes x) = (ab - ba) \otimes 1 + (ad - bc) \otimes x = 1 \otimes x.
\]

Now $A \otimes_A A'$ is generated as an algebra and left $A$-module by $1 \otimes a$ and $1 \otimes b$, so to show $\gamma \circ \beta$ is the identity, it suffices to show it is on these two elements. Now
\[
\gamma \circ \beta(1 \otimes a) = \gamma(a \otimes 1 + c \otimes x) = a \otimes 1 + ca \otimes b - cb \otimes a = a \otimes 1 + a \otimes (ad - 1) - (ad - 1) \otimes a = a \otimes 1 + da \otimes a - a \otimes 1 - da \otimes a + 1 \otimes a = 1 \otimes a.
\]

Likewise, $\gamma \circ \beta(1 \otimes b) = 1 \otimes b$, so $\beta$ and $\gamma$ are inverses. This proves $A \supseteq A^{coH}$ is a Galois extension.

We now turn to the study of the divided power Hopf algebra $H$. This is often a more appropriate Hopf algebra than $k[x]$ when $\text{char } k = p > 0$. The (infinite) divided power Hopf algebra $H$ is defined as follows. Let $x^{(0)}, x^{(1)}, x^{(2)}, \ldots$ be a sequence of symbols, and set $1 = x^{(0)}$. These symbols form a basis for $H$. We make $H$ into a coalgebra by defining $\epsilon(x^{(i)}) = \delta_{i,0}$ and $\Delta(x^{(n)}) = \sum_{i+j=n} x^{(i)} \otimes x^{(j)}$, and we make $H$ into an algebra by defining $x^{(i)}x^{(j)} = \frac{(i+j)!}{i!j!} x^{(i+j)}$. This structure makes $H$ into a bialgebra and we can make $H$ into a Hopf algebra with antipode defined by $S(x^{(i)}) = (-1)^i x^{(i)}$: see [7, Example 5.6.8]. It is not hard to see that $H$ is connected; this fact is [10, Proposition 11.0.12]. Thus $H$ is a connected, commutative, cocommutative Hopf algebra.

If $k$ has characteristic 0, then taking $x^{(i)} = x^i/i!$ shows that $H = k[x]$. However, if $\text{char } k > 0$, then the polynomial algebra and the divided power Hopf algebra are distinct objects.

Let $H$ be the divided power Hopf algebra and let $C$ be an $H$-comodule. There are maps $f_n : C \to C$ for each non-negative integer $n$ such that the comodule structure of $C$ is defined by $\rho_C(c) = \sum_{n=0}^\infty f_n(c) \otimes x^{(n)}$. The counitary law implies that $f_0 = \text{id}_C$ and the coassociative law implies that $f_i \circ f_j = f_{i+j}$ for all $i, j$. It follows that if we let $f = f_1$, then $f_n = f^n$, and so $\rho_C(c) = \sum_{n=0}^\infty f_n(c) \otimes x^{(n)}$. As with $H = k[x]$, this must be a finite sum, so $f$ must be locally nilpotent (that is, for each $c \in C$, there must be an $n = n(c)$ with $f^n(c) = 0$). We will denote $H$-comodules by $(C, f)$.

It is easy to see that if $(D, g)$ and $(C, f)$ are $H$-comodules, then a comodule map $\phi : D \to C$ is just a linear map satisfying $\phi \circ g = f \circ \phi$.

Suppose $A$ is an algebra and $(A, f)$ is an $H$-comodule. In order for $A$ to be an $H$-comodule algebra, the comodule structure map $\rho$ defined from $f$ as above must be multiplicative. Let $a, b \in A$. Then
\[
\rho(a)\rho(b) = \left(\sum_i f^i(a) \otimes x^{(i)}\right)\left(\sum_j f^j(b) \otimes x^{(j)}\right)
\]
\[
= \sum_{i,j} f^i(a)f^j(b) \otimes \frac{(i+j)!}{i!j!} x^{(i+j)} = \sum_n \sum_{i=0}^n \binom{n}{i} f^i(a)f^{n-i}(b) \otimes x^{(n)}.
\]

For this to equal $\rho(ab)$, we need $f^n(ab) = \sum_{i=0}^n \binom{n}{i} f^i(a)f^{n-i}(b)$ for all $n$. Taking $n = 1$, this says $f(ab) = af(b) + f(a)b$, so a necessary condition for $\rho$ to be an algebra
homomorphism is that \( f \) be a derivation on \( A \). But if \( f \) is a derivation on \( A \), then the desired equality for any \( n \) is valid by Leibniz’s rule. Thus \((A, f)\) is an \( H\)-comodule algebra if and only if \( f \) is a derivation on \( A \). The subalgebra \( A^{\text{co}}H \) of coinvariants is just \( A^{f} = \ker f \).

**Proposition 2.5.** Let \( H \) be a divided power Hopf algebra and let \((A, f)\) be an \( H\)-comodule algebra, where \( f \) is a locally nilpotent derivation on \( A \). Then the extension \( A \supseteq A^{\text{co}}H \) is faithfully flat Galois if and only if there exist \( a_0 = 1, a_1, \ldots \) in \( A \) such that \( f(a_n) = a_{n-1} \) for all \( n \geq 1 \).

If there exists such a sequence with the property that \( a_i a_j = \frac{(i+j)!}{i!j!} a_{i+j} \) for all \( i, j \), then \( A \) is an \( H\)-module algebra via the action \( x^{(n)} a = \sum_{i+j=n} (-1)^j a_i a_{j} \), and \( A \) is isomorphic as an \( H\)-comodule algebra to \( A^{\text{co}}H \# H \).

**Proof.** Since \( H \) is connected, Proposition 1.3 implies that an \( H\)-extension \( A \supseteq A^{\text{co}}H \) is faithfully flat Galois if and only if there is a total integral \( \phi : H \to A \). The \( H\)-comodule structure on \( H \) is determined by the derivation \( g : H \to H \) defined by \( g(x^{(n)}) = x^{(n-1)} \), and \( \phi : H \to A \) is an \( H\)-comodule map if and only if \( \phi \circ g = f \circ \phi \). Set \( a_n = \phi(x^{(n)}) \); this last condition translates to \( a_{n-1} = f(a_n) \). We also require \( \phi(1) = 1 \) for a total integral, so \( a_0 = 1 \). Thus a total integral exists if and only if there is a sequence \( a_0 = 1, a_1, \ldots \) in \( A \) such that \( f(a_n) = a_{n-1} \).

The total integral \( \phi \) defined by \( \phi(x^{(n)}) = a^{(n)} \) will be an algebra homomorphism precisely when the multiplication formula \( a_i a_j = \frac{(i+j)!}{i!j!} a_{i+j} \) is valid for all \( i, j \). Thus when there is a sequence with this additional property, we may apply Proposition 1.4, which yields the final claims in the proposition. \( \blacksquare \)

**Remark 2.6.** If \( \text{char } k = p > 0 \), then one can define a finite dimensional divided power Hopf algebra \( H \) with basis \( x^{(0)} = 1, x^{(1)}, \ldots, x^{(p^{m}-1)} \) for any positive integer \( m \). This is a Hopf subalgebra of the infinite divided power Hopf algebra, and in fact, it is the Hopf algebra dual of the truncated polynomial ring \( k[x]/(x^{p^{m}}) \). An \( H\)-comodule algebra is an algebra \( A \) equipped with a derivation \( f \) such that \( f^{p^{m}} = 0 \). We get a result for this situation exactly analogous to that of Proposition 2.5. This example is discussed in [5, Example 4 in Sections 1&2], [3, Example 1.8(2)], where a nicer condition is stated: \( A \supseteq A^{\text{co}}H \) is faithfully flat Galois if and only if there exists \( a \in A \) with \( f^{p^{m}-1}(a) = 1 \).

### 3. The case where \( H \) is a general polynomial algebra

In this section we extend the results of the previous sections to the case where \( H = k[X] \) is a polynomial algebra in the indeterminates from the set \( X \); we make \( H \) into a Hopf algebra by declaring the elements of \( X \) to be primitive. When \( \text{char } k = 0 \), an \( H\)-comodule algebra structure is determined by a locally nilpotent family \( \{f_x\}_{x \in X} \) of commuting derivations on the algebra \( A \). In this case \( A \supseteq A^{\text{co}}H \) is faithfully flat Galois if and only if there exist elements \( \theta_x \in A \) with \( f_x(\theta_x) = \delta_{x,y} \) for all \( x, y \in X \). In the case of arbitrary characteristic, \( H\)-comodule algebras are algebras with higher derivations and we obtain results corresponding to those in Section 2. It is no longer the case that \( A \) need be a smash product \( A^{\text{co}}H \# H \) when \( A \supseteq A^{\text{co}}H \) is faithfully flat Galois, but if \( A \) is commutative then \( A \) is faithfully flat Galois if and only if \( A \cong A^{\text{co}}H[X] \).
We will write a basis for $H = k[X]$ as $\{x^n\}$, using the multi-index notation introduced in the proof of Proposition 1.5. We add one bit of notation: for $x \in X$, we define the multi-index $e_x$ by $e_x(y) = \delta_{x,y}$.

Let $A$ be an $H$-comodule with structure map $\rho(a) = \sum_n f_n(a) \otimes x^n$ (this sum is over all $X$-multi-indices $n$) for maps $f_n : A \to A$. As in the case of one variable, this implies $f_0 = \text{id}_A$ and $f_i \circ f_j = \binom{k+j}{j} f_{i+j}$; we will call such a family of maps $X$-iterative. The finiteness of the sum implies that the family $\{f_n\}$ is locally nilpotent, that is, for any $a \in A$, only finitely many $f_n(a)$ are nonzero. The composition formula shows that all the maps in the family commute. If $A$ is an algebra, this structure makes $A$ into an $H$-comodule algebra if and only if $\{f_n\}$ is a commuting $X$-higher derivation, that is, if and only if $f_n(ab) = \sum_{i+j=n} f_i(a) f_j(b)$ for all $a, b \in A$ and all $n$. Note that $A^{\text{co}H} = \bigcap_n \text{ker } f_n$.

Suppose that $\text{char } k = 0$. If we set $f_x = f_{e_x}$, then $\{f_x\}_{x \in X}$ is a commuting family of locally nilpotent derivations on $A$, and they determine all the other members of the iterative $X$-higher derivation via $f_n = (\prod_{x \in X} f^{n(x)}_{e_x})/n!$. Conversely, given a commuting family of locally nilpotent derivations on $A$, with the property that for any $a \in A$, $f_x(a)$ is nonzero for only finitely many $x \in X$, we can use this formula to define a locally nilpotent iterative $X$-higher derivation. In this case $A^{\text{co}H} = \bigcap_{x \in X} \text{ker } f_x$.

**Proposition 3.1.** Let $H = k[X]$ be the polynomial algebra on the set $X$ and let $A$ be an $H$-comodule algebra.

1. If the comodule structure on $A$ is defined by the locally nilpotent $X$-iterative $X$-higher derivation $\{f_n\}$, then $A \supseteq A^{\text{co}H}$ is faithfully flat Galois if and only if for each $x \in X$ there exists $\theta_x \in A$ such that $f_{e_x}(\theta_x) = 1$ and $f_n(\theta_x) = 0$ for $n \neq 0, e_x$.

   If $\text{char } k = 0$ and the comodule structure on $A$ is defined by the commuting locally nilpotent derivations $\{f_x\}_{x \in X}$, then it is enough to check that $f_y(\theta_x) = \delta_{x,y}$ for any $x, y \in X$.

2. If in addition $\theta_x \theta_y = \theta_y \theta_x$ for all $x, y \in X$, then $A$ is an $H$-module algebra via the action $x.a = \text{ad } \theta_x(a)$, with $A^{\text{co}H}$ a submodule, and $A$ is isomorphic as an $H$-comodule algebra to the multiple differential operator ring $A^{\text{co}H}[\theta_x; \text{ad } \theta_x]_{x \in X}$ with commuting indeterminates and derivations. (In case $\text{char } k = 0$, the map $f_x$ corresponds to $\partial/\partial \theta_x$.)

**Proof.** Since $H = U(g)$ where $g$ is the Abelian Lie algebra with basis $X$, Proposition 1.5 implies $A \supseteq A^{\text{co}H}$ is faithfully flat Galois if and only if there exist elements $\theta_x \in A$ for $x \in X$ with $\rho(\theta_x) = \theta_x \otimes 1 + 1 \otimes x$. This equality holds if and only if the condition in (1) is satisfied by the elements $\theta_x$.

Since $g$ is Abelian, the hypothesis in the second paragraph of Proposition 1.5 is satisfied whenever $\theta_x \theta_y = \theta_y \theta_x$ for all $x, y \in X$. In this case, $A \cong A^{\text{co}H} \# k[X]$. We see easily from the definition that this smash product is just the multiple differential operator ring $A^{\text{co}H}[\theta_x; \text{ad } \theta_x]_{x \in X}$. 

**Corollary 3.2.** Let $A$ be a commutative $k[X]$-comodule algebra. Then $A \supseteq A^{\text{co}H}$ is faithfully flat Galois if and only if $A \cong A^{\text{co}H}[X]$ as $k[X]$-comodule algebras.

**Proof.** This follows from Proposition 3.1, since the commutativity of $A$ implies that the $k[X]$-module action must be trivial.
Example 3.3. In the case of multiple variables, a faithfully flat Galois extension need not always be a smash product. For example, suppose \( \text{char } k = 0 \), let \( H = k[x, y] \), and let the free algebra \( A = k\langle s, t \rangle \) be made into an \( H \)-comodule algebra via the commuting derivations \( f_x = \partial/\partial s \) and \( f_y = \partial/\partial t \). The extension \( A \cong A^{co H} \) is faithfully flat Galois by Proposition 3.1 (and hence cleft by Proposition 1.3): take \( \theta^*_x = s \) and \( \theta^*_y = t \). However, \( \theta_x \) and \( \theta_y \) do not commute. In fact, we cannot have \( A \cong A^{co H} \# k[x, y] \), since by Bergman's Centralizer Theorem, [1, Theorem 5.3], the free algebra does not contain a copy of \( k[x, y] \).

There is a generalization of the divided power Hopf algebra to the multi-variable case: see [10, Sections 12.2 & 12.3]. One can formulate and prove results that parallel those in Section 2. For example, a comodule algebra in this case is determined by a locally nilpotent family of commuting derivations. We leave this case to the interested reader.

4. The case where \( H \) is a free algebra or a shuffle algebra

In this section, we consider the Hopf algebra \( H = k\langle X \rangle \), the free algebra on \( X \), and a related Hopf algebra, the shuffle algebra \( \text{Sh}_k(X) \) on \( X \). These algebras are in some sense dual to each other. In our realization of them, both have the same vector space structure. The shuffle algebra has a simpler comodule structure, which makes possible a nice description of \( H \)-comodule algebras: they are determined by a locally nilpotent family \( \{f_x\}_{x \in X} \) of derivations. On the other hand, the free algebra has a more complicated comodule structure, which leads to a more complicated description of \( H \)-comodule algebras in terms of a generalization of iterative higher derivations, but the free algebra has a nicer algebra structure, which guarantees that any faithfully flat Galois extension is actually a smash product.

Let us begin with the free algebra \( H = k\langle X \rangle \) on the set \( X \). We make this into a Hopf algebra by declaring the elements of \( X \) to be primitive, whence it is connected by Lemma 1.1 or [10, Proposition 11.0.10]. The primitivity of the elements of \( X \) uniquely determines an algebra homomorphism \( \Delta : H \to H \otimes_k H \), which makes \( H \) into a bialgebra and in fact a Hopf algebra. In order to explicitly describe \( \Delta \), we need some notation.

First, let \( W \) be the set of all words in the alphabet \( X \) (including the empty word, which we will denote by 1). The set \( W \) is a vector space basis for \( k\langle X \rangle \). Now suppose \( w = x_1 \cdots x_n \in W \). For a subset \( I \) of \( \{1, \ldots, n\} \), we denote by \( I^c \) the complement \( \{1, \ldots, n\} \setminus I \). We set \( w(I) = \prod_{i \in I} x_i \), where this product is taken in the same order as \( I \); we define \( w(I^c) \) similarly. Then \( \Delta(w) = \sum_{I \subseteq \{1, \ldots, n\}} w(I) \otimes w(I^c) \).

In order to describe \( H \)-comodule algebras, we need to introduce the shuffle multiplication. If \( V \) is a vector space with basis \( X \), the shuffle algebra \( \text{Sh}(V) \) is defined by Sweedler in [10, Chapter 12]; we refer the reader there for definitions and background material. We will use the notation \( \text{Sh}_k(X) \) instead of \( \text{Sh}(V) \). A vector space basis for \( \text{Sh}_k(X) \) is given by the set \( W \) of words in \( X \) and the coalgebra structure is defined by \( \epsilon(w) = 0 \) for \( w \neq 1 \) and \( \Delta(w) = \sum_{u, v \in W, uv = w} u \otimes v \).

The multiplication on \( \text{Sh}_k(X) \) can be defined in two equivalent ways. The first description we give is the one in [10, p. 248], although we use different notation. If we let \( W_n \) be the set of words in \( W \) of length \( n \), then the permutation group \( S_n \) acts on \( W_n \) via \( \sigma(x_1 \cdots x_n) = x_{\sigma^{-1}(1)} \cdots x_{\sigma^{-1}(n)} \). For \( 0 \leq i \leq n \), let us denote by \( S_n(i) \) the set of \( \sigma \in S_n \) such that \( \sigma|_{\{1, \ldots, i\}} \) and \( \sigma|_{\{i+1, \ldots, n\}} \) are order-preserving functions. (In the terminology of [10], the elements of \( S_n(i) \) are the inverses of the \( i \)-shuffles.) We define the multiplication \( * \) on \( \text{Sh}_k(X) \) as follows. If \( u, v \in W \) have lengths \( i, j \) respectively, then
\( u \ast v = \sum_{\sigma \in S_{n+j}(i)} \sigma.(uv) \). For example, \( x \ast y = xy + yx \) for all \( x, y \in X \). With this multiplication and the antipode defined by \( S(x_1 \cdots x_n) = (-1)^n x_n \cdots x_1 \), \( S_h(X) \) becomes a commutative Hopf algebra.

We need to describe \( u \ast v \) in a second way for our application to \( k \langle X \rangle \). Let \( u, v, w \in W \) and suppose \( w \) has length \( n \). Then we define \( N_{w,u,v} \) to be the number of subsets \( I \) of \( \{1, \ldots, n\} \) such that \( w(I) = u \) and \( w(I^c) = v \). It is not hard to see that \( N_{w,u,v} = 0 \) unless \( w = \sigma.(uv) \) for some \( \sigma \in S_n(i) \), where \( i \) is the length of \( u \). The shuffle multiplication can now be described by the formula \( u \ast v = \sum_{w \in W} N_{w,u,v} w \). We leave the verification of this equality to the reader.

We can now describe \( H \)-comodule algebras when \( H = k \langle X \rangle \). Let \( A \) be an \( H \)-comodule, with structure map given by \( \rho(a) = \sum_{w \in W} f_w(a) \otimes w \) for maps \( f_w : A \rightarrow A \). The counitary law implies \( f_1 = \text{id} \), while the coassociative law implies

\[
\sum_{u,v \in W} f_u \circ f_v(a) \otimes u \otimes v = \sum_{n \in W_n, I \subseteq \{1, \ldots, n\}} f_w(a) \otimes w(I) \otimes w(I^c).
\]

Thus \( f_u \circ f_v(a) \) must equal the sum of all \( f_w(a) \)'s with some \( w(I) = u \), \( w(I^c) = v \) (counted according to multiplicity). That is, \( f_u \circ f_v = \sum_{w \in W} N_{w,u,v} f_w \). This can be expressed symbolically by writing \( f_u \circ f_v = f_{uv} \). Generalizing our previous terminology, we say a family \( \{f_w\}_{w \in W} \) of maps from \( A \) to \( A \) is \( W \)-iterative if \( f_1 = \text{id} \) and \( f_u \circ f_v = f_{uv} \) for all \( u, v \in W \). For the sum defining \( \rho(a) \) to be finite, the family \( \{f_w\}_{w \in W} \) must be locally nilpotent in the sense that for any \( a \in A \), there are only finitely many \( w \in W \) with \( f_w(a) \neq 0 \).

Now suppose \( A \) is an \( H \)-comodule algebra with structure map \( \rho \) as above. Then

\[
\sum_{u,v \in W} f_u(a) f_v(b) \otimes uv = \rho(a) \rho(b) = \rho(ab) = \sum_{w \in W} f_w(ab) \otimes w
\]

for all \( a, b \in A \). This is equivalent to the equality \( f_w(ab) = \sum_{u,v \in W, uv = w} f_u(a) f_v(b) \) for all \( w \in W, a, b \in A \). A family \( \{f_w\}_{w \in W} \) of maps from \( A \) to \( A \) with \( f_1 = \text{id} \) satisfying this product rule is called a \( W \)-higher derivation on \( A \).

We can carry out any of the above calculations in reverse. Thus we see that \( H \)-comodule algebras correspond to pairs \( (A, f = \{f_w\}_{w \in W}) \) where \( A \) is an algebra and \( f \) is a locally nilpotent iterative \( W \)-higher derivation on \( A \). Note that \( A^{coH} \) equals \( A^f = \bigcap_{w \in W} \ker f_w \).

**Proposition 4.1.** Let \( H = k \langle X \rangle \) be the free algebra on \( X \) and let \( (A, f) \) be an \( H \)-comodule algebra, where \( f \) is a locally nilpotent \( W \)-iterative \( W \)-higher derivation on \( A \). Then the extension \( A \supseteq A^{coH} \) is faithfully flat Galois if and only if for each \( x \in X \), there exists \( a_x \in A \) with \( f_x(a_x) = 1 \) and \( f_w(a_x) = 0 \) for \( w \neq 1, x \).

Moreover, if this is the case, then there is an \( H \)-module action on \( A \) defined by \( x.a = a_x a - aa_x \) with \( A^{coH} \) a submodule, and \( A \) is isomorphic as an \( H \)-comodule algebra to \( A^{coH} \# H \).

**Remark 4.2.** The structure of comodule algebras is sufficiently complicated that it seems worthwhile to re-state this result directly in terms of \( \rho \). Thus the extension \( A \supseteq A^{coH} \) is faithfully flat Galois if and only if for each \( x \in X \), there exists \( a_x \in A \) with \( \rho(a_x) = a_x \otimes 1 + 1 \otimes x \).

**Proof.** The equivalence of the conditions in the proposition on \( a_x \) and the condition in the remark on \( a_x \) is clear from the connection between \( \rho \) and \( f \). We will work with the condition in the remark.
Since $H$ is connected, we know from Proposition 1.3 that $A \supseteq A^{coH}$ is faithfully flat Galois if and only if there is a total integral $\phi : H \to A$. If $x \in X$, then $\rho \circ \phi(x) = \phi(x) \otimes 1 + 1 \otimes x$, so we may take $a_x = \phi(x)$.

Suppose conversely that for each element $x \in X$, there is an element $a_x \in A$ such that $\rho(a_x) = a_x \otimes 1 + 1 \otimes x$. By the universal property of $k\langle X \rangle$, we can extend the map $x \mapsto a_x$ to an algebra homomorphism $\phi : H \to A$. Since $X$ generates $H$ and $\phi$ acts like a comodule map on $X$, $\phi$ must in fact be a comodule map on all of $H$, that is, $\phi$ must be a total integral. We conclude from Proposition 1.4 that $A \supseteq A^{coH}$ is faithfully flat Galois, and that $A$ is in fact a smash product $A^{coH} \# H$.

We now turn to the study of comodule algebras over the shuffle algebra $H = Sh_k(X)$. Let $A$ be an $H$-comodule with structure map given by $\rho(a) = \sum_{w \in W} f_w(a) \otimes w$ for maps $f_w : A \to A$. The coassociative law implies that $f_1 = \text{id}_A$ and the coassociative law implies that $f_u \circ f_v = f_{uv}$ for all $u, v \in W$. It follows that all the $f_w$ are determined by the functions $f_x$, and we will denote an $H$-comodule by $(A, f = \{f_x\}_{x \in X})$. If $w = x_1 \cdots x_n$, we then write $f_w$ for $f_{x_1} \circ \cdots \circ f_{x_n}$. The sum $\rho(a)$ is finite if and only if the family $f$ is locally nilpotent in the sense that for every $a \in A$, there are only finitely many $w \in W$ with $f_w(a) \neq 0$ (equivalently, $f_x(a) \neq 0$ for only finitely many $x \in X$ and there exists $n = n(a)$ such that any composition of $n$ of the $f_x$'s annihilates $a$). Note that $A^{coH}$ equals $A^f = \bigcap_{x \in X} \ker f_x$.

Suppose $(A, f)$ is an $H$-comodule and $A$ is an algebra. Then $A$ is an $H$-comodule algebra if and only if $\rho$ is multiplicative. We have $\rho(ab) = \sum_{w \in W} f_w(ab) \otimes w$, while $\rho(a) \rho(b) = \sum_{u,v \in W} f_u(a) f_v(b) \otimes (u \ast v) = \sum_{u,v,w \in W} N_{w,u,v} f_u(a) f_v(b) \otimes w$. Thus $\rho$ is multiplicative if and only if for each $w \in W$ of length $n$ and each $a, b \in A$, we have $f_w(ab) = \sum_{u,v \in W} N_{w,u,v} f_u(a) f_v(b) = \sum_{I \subseteq \{1, \ldots, n\}} f_{w(I)}(a) f_{w(I^c)}(b)$. If $w = x \in X$, this says $f_x(ab) = f_x(a)b + a f_x(b)$, so each $f_x$ is a derivation. Conversely, if each $f_x$ is a derivation, it is easy to derive the formula $f_w(ab) = \sum_{I \subseteq \{1, \ldots, n\}} f_{w(I)}(a) f_{w(I^c)}(b)$ for any $w = x_1 \cdots x_n$. Thus an arbitrary locally nilpotent family of derivations defines an $H$-comodule structure on an algebra $A$.

**Proposition 4.3.** Let $X$ be a set and let $H = Sh_k(X)$ be the shuffle algebra on $X$. Let $(A, f)$ be an $H$-comodule algebra, where $f = \{f_x\}_{x \in X}$ is a locally nilpotent family of derivations on $A$. For any $w = x_1 \cdots x_n \in W$, set $f_w = f_{x_1} \circ \cdots \circ f_{x_n}$. Then the extension $A \supseteq A^{coH}$ is faithfully flat Galois if and only if there exist elements $a_w \in A$ for each $w \in W$ such that $a_1 = 1$ and the following condition holds for all $v, w \in W$: $f_v(a_w) = a_w$ whenever $uv = w$, while $f_v(a_w) = 0$ if there is no decomposition $w = uv$.

Moreover, if such a family $\{a_w\}_{w \in W}$ of elements exists and has the additional property that $a_{uv} = a_{uwv}$ for all $u, v \in W$, where $a_{uwv}$ is defined to be $\sum_{w \in W} N_{w,u,v} a_w$, then there is an $H$-module action on $A$ with $A^{coH}$ a submodule, and $A \cong A^{coH} \# H$ as $H$-comodule algebras.

**Proof.** $H$ is connected by [10, Lemma 12.0.1]. Thus $A \supseteq A^{coH}$ is faithfully flat Galois if and only if there is a total integral $\phi : H \to A$. The coalgebra structure on $Sh_k(X)$ is such that $\phi : H \to A$ is a total integral if and only if the elements $\phi(w) = a_w$ satisfy the conditions stated in the first paragraph.
If there are elements $a_w$ satisfying all of the conditions stated, then $\phi : H \to A$ defined by $\phi(w) = a_w$ is a total integral and an algebra homomorphism, so we may apply Proposition 1.4 to obtain the final conclusion.

The hypotheses of Proposition 4.3 imply that $f_y(a_x) = \delta_{x,y}$ for all $x, y \in X$. However, the existence of such elements $a_x$ does not imply the existence of all the required elements $a_w$.

References


Department of Mathematical Sciences, University of Wisconsin–Milwaukee, Milwaukee, WI 53201-0413, USA

E-mail address: adbell@uwm.edu  Home page: http://www.uwm.edu/~adbell/