$U(\mathfrak{g})$-Galois Extensions

Darren B. Parker[*]

MR Subject Classifications: 16W30, 16S30
Keywords: Hopf algebra, Galois extension, comodule algebra, faithfully flat, Universal enveloping algebra

Abstract

This paper studies the structure of $U(\mathfrak{g})$-Galois extensions. In particular, we use a result of Bell to construct a "PBW-like" free basis for faithfully flat $U(\mathfrak{g})$-Galois extensions. We then move to non-faithfully flat extensions and propose a possible equivalent condition for a $U(\mathfrak{g})$-extension to be Galois. We get a partial result for this.

1 Introduction

This paper is concerned with Hopf Galois extensions. These extensions come from the generalizations of classical Galois field extensions given in [CHR65], where a group acts faithfully on an extension of commutative rings. These concepts have been generalized to Hopf algebra actions and coactions on extensions of associative algebras in [KT81].

The results that are most important for this paper come from [Bel00]. He considers faithfully flat H-Galois extensions for certain Hopf algebras H. Using results from [Sch90], he obtains results in the case when H is connected and, more specifically, when H is a universal enveloping algebra.

One of Bell's results states that if H is connected and $A^{coH} \subseteq A$ is faithfully flat H-Galois, then we have $A \cong A^{coH} \#_\sigma H$ for some 2-cocycle σ. In particular, A is a free A^{coH}-module. For our main result, Theorem 4.6, we give an explicit construction of a free basis in the case $H = U(\mathfrak{g})$. This construction is analogous to the construction of a PBW-basis for $U(\mathfrak{g})$. We also prove other connections between faithfully flat Galois extensions $A^{coU(\mathfrak{g})} \subseteq A$ and $K \subseteq U(\mathfrak{g})$, where K is the ground field.

In Section 5, we consider the case where the extension is not faithfully flat. We get Proposition 5.2 which suggests that a certain map $\bar{c}$ determines whether or not an extension $A^{coU(\mathfrak{g})} \subseteq A$ is $U(\mathfrak{g})$-Galois.

[*] Department of Mathematics, University of Dayton, Dayton, Ohio 45469, dbparker@udayton.edu, http://academic.udayton.edu/darrenparker

The author would like to thank the referee for the many helpful suggestions. In particular, the results for connected Hopf algebras, as well as Lemma 3.3, are given in a more general context than in the original paper. Also, an observation by the referee led to a strengthening of Theorem 4.6.

2 Preliminaries

The primary reference is [Mon93]. The ground field is always K, and tensor products are assumed to be over K unless otherwise specified.

In this paper, we primarily concentrate on the Hopf algebra $U(\mathfrak{g})$, where $\mathfrak{g}$ is a Lie algebra over K. The Hopf algebra structure is given by $\Delta(x) = 1 \otimes x + x \otimes 1$, $\varepsilon(x) = 0$, and $S(x) = -x$. We then extend Δ and ε to algebra homomorphisms and S to an algebra anti-homomorphism of $U(\mathfrak{g})$.

The objects of interest in this paper are Hopf Galois extensions. They are generalizations of classical Galois extensions, where the group action is replaced by a Hopf algebra coaction. Let H be a Hopf algebra, with A a right H-comodule algebra. That is, we have an algebra map $\rho : A \to A \otimes H$ such that $(\rho \otimes id) \circ \rho = (id \otimes \Delta) \circ \rho$ and $(id \otimes \varepsilon) \circ \rho = id \otimes 1$. Let $A^{coH} = \{a \in A : \rho(a) = a \otimes 1\}$ denote the coinvariants of A. An extension $B \subseteq A$ of K-algebras is right H-Galois if $B = A^{coH}$ and the map $\beta : A \otimes_B A \to A \otimes_K H$ given by $\beta(a \otimes b) = (a \otimes 1)\rho(b)$ is bijective.

If $H = KG$, then H-comodule algebras are G-graded algebras (see [Mon93, 1.6.7,4.1.7]), and H-Galois extensions are precisely the strongly G-graded extensions (see [Ulb81] or [Mon93, 8.1.7]). This gives a close link between KG-Galois extensions and G itself, for if $A = \oplus_{g \in G} A_g$ is the grading, then $G \cong \{A_g : g \in G\}$ as groups, where the multiplcation of the subspaces $\{A_g\}$ is given by setwise multiplication. One can also show that if G is a finite group, then $(KG)^*$-Galois field extensions are precisely classical Galois field extensions with Galois group G.

The main result of this paper depends heavily on [Bel00]. He studied Hopf Galois extensions of connected Hopf algebras (i.e. Hopf algebras whose only simple subcoalgebra is $K1_H$), and obtained the following result.

Proposition 2.1. [Bel00, 1.3] Let H be a connected Hopf algebra and let A be an H-comodule algebra. Then the following are equivalent.

(i) The extension $A^{coH} \subseteq A$ is faithfully flat H-Galois.

(ii) The extension $A^{coH} \subseteq A$ is H-cleft.

(iii) There is a total integral $\phi : H \to A$.

Note that a total integral is an H-comodule map $\phi : H \to A$ such that $\phi(1) = 1$, and $A^{coH} \subseteq A$ is an H-cleft extension if there is a total integral which is convolution invertible (see [Mon93, 1.4, 7.2]).

By [Mon93, 7.2.2], any H-cleft extension is isomorphic to a crossed product $A^{coH} \#_\sigma H$. This and the above imply that any faithfully flat H-Galois extension is in fact free over A^{coH} when H is connected. Since $U(\mathfrak{g})$ is connected by [Mon93, 5.5.3], this result applies to $U(\mathfrak{g})$-Galois extensions. Our goal will be to construct a free basis in a similar fashion as the PBW basis for $U(\mathfrak{g})$. Bell's characterization of $U(\mathfrak{g})$-Galois extensions will be useful.

Proposition 2.2. [Bel00, 1.5] $A^{coU(\mathfrak{g})} \subseteq A$ is faithfully flat $U(\mathfrak{g})$-Galois if and only if there is a map $\lambda : \mathfrak{g} \to A$ such that $\rho(\lambda(x)) = \lambda(x) \otimes 1 + 1 \otimes x$.

Thus, $\lambda(x)$ plays the same role in the comodule structure of A as x does in $U(\mathfrak{g})$.

3 $U(\mathfrak{g})$-comodules

Let us fix some notation for $U(\mathfrak{g})$. Let $\{x_i : i \in I\}$ be an ordered basis for $\mathfrak{g}$. We use the "multi-index" notation as described in [Mon93, 5.5]. Consider all functions $\mathbf{n} : I \to \mathbb{Z}_{\geq 0}$ with finite support. In other words, $\mathbf{n}(i) \neq 0$ for only finitely many $i \in I$. These functions can be thought of as ordered m-tuples $(\mathbf{n}(i_1), \cdots, \mathbf{n}(i_m))$, where $i_1 < \cdots < i_m$ are the only elements in I which do not vanish under $\mathbf{n}$. We then allow the length of these tuples to be arbitrarily large (but finite). Define $x^{\mathbf{n}} = x_{i_1}^{\mathbf{n}(i_1)} \cdots x_{i_m}^{\mathbf{n}(i_m)}$. Then the PBW basis for $U(\mathfrak{g})$ is $\{x^{\mathbf{n}} : \mathbf{n}$ has finite support$\}$. This gives us a shorthand for the PBW basis. We also define $|\mathbf{n}| = \sum_{i \in I} \mathbf{n}(i)$.

We can use this notation to write the comultiplication on $U(\mathfrak{g})$ in a compact manner. We first need some more notation. Define a partial order on these functions, so that $\mathbf{m} \leq \mathbf{n}$ if $\mathbf{m}(i) \leq \mathbf{n}(i)$ for all $i \in I$. If $\mathbf{m} \leq \mathbf{n}$, we can define a generalized binomial coefficient $\binom{\mathbf{n}}{\mathbf{m}} = \prod_{i \in I} \binom{n(i)}{m(i)}$. We get the following.

Lemma 3.1. [Mon93, 5.5] For all $\mathbf{n} : I \to \mathbb{Z}_{\geq 0}$ with finite support,

$$\Delta(x^{\mathbf{n}}) = \sum_{\mathbf{m} \leq \mathbf{n}} \binom{\mathbf{n}}{\mathbf{m}} x^{\mathbf{m}} \otimes x^{\mathbf{n}-\mathbf{m}}.$$

We can apply the same notation to the elements in A given by Proposition 2.2. If we let $a_i = \lambda(x_i)$, then we write $a^{\mathbf{n}} = a_{i_1}^{\mathbf{n}(i_1)} \cdots a_{i_m}^{\mathbf{n}(i_m)}$.

We now turn to a more general context, investigating a comodule M over a coalgebra H. Recall the coradical filtration $H = \cup_{n=0}^{\infty} H_n$, where H_0 is the coradical, and the rest of the H_n are defined inductively by $H_{n+1} = \Delta^{-1}(H \otimes H_n + H_0 \otimes H)$ (see [Mon93, 5.2]).

Definition 3.2. Let H be a coalgebra with coradical filtration $H = \cup_{n=0}^{\infty} H_n$. Let M be a right H-comodule. We define $M_n = \rho^{-1}(M \otimes H_n\}$.

The M_n have many of the same properties as the coradical filtration, and we use similar methods to study them. For subspaces $N \subseteq M$ and $C \subseteq H$, define $N \wedge C = \rho^{-1}(M \otimes C + N \otimes H)$. We use this "wedge product" in a similar way as in [Mon93, 5.2].

Lemma 3.3. Let H be a coalgebra, M a right H-comodule. For all $n \geq 0$,

(i) M_n is a subcomodule of M.

(ii) $M_{n+1} = M_n \wedge H_0$.

(iii) $M_n = \{m \in M : \rho(m) \in \sum_{i=0}^{n} M_i \otimes H_{n-i}\}$

(iv) $M = \bigcup_{n=0}^{\infty} M_n$

(v) If M is an H-comodule algebra, and H is a bialgebra such that $H_iH_j \subseteq H_{i+j}$, then $M_iM_j \subseteq M_{i+j}$

Note: M_0 is the sum of all simple subcomodules of M, and M_{n-1} is the nth level of the socle filtration of M. Also, if H is a Hopf algebra whose coalgebra filtration is a Hopf algebra filtration (see [Mon93, p. 62]), then (v) applies. In particular, this will occur if H is pointed, or, more generally, when H_0 is a subHopfalgebra of H [Mon93, 5.2.8].

Proof. Let $m \in M_n$, so that $\rho(m) = \sum m_i \otimes h_i$, with $h_i \in H_n$. Since $(\rho \otimes id) \circ \rho = (id \otimes \Delta) \circ \rho$, we have $\sum \rho(m_i) \otimes h_i = \sum m_i \otimes \Delta(h_i)$. But H_n is a subcoalgebra, so $\Delta(h_i) \in H_n \otimes H_n$, which forces $\rho(m_i) \in M \otimes H_n$. This gives us (i).

For (ii), let $\{h_i\}$ be a basis for H_0, with $\{h_i'\}$ a complementary basis in H_{n+1}. If $m \in H_{n+1}$, then we can write $\rho(m) = \sum m_i \otimes h_i + \sum m_i' \otimes h_i'$. As before, we have

$$\sum \rho(m_i) \otimes h_i + \sum \rho(m_i') \otimes h_i' = \sum m_i \otimes \Delta(h_i) + \sum m_i' \otimes \Delta(h_i')$$

Thus, each $\rho(m_i') \otimes h_i' \in M \otimes H_0 \otimes H_0 + M \otimes \Delta(H_{n+1}) \subseteq M \otimes H_0 \otimes H_0 + \sum_{i=0}^{n+1} M \otimes H_i \otimes H_{n+1-i}$ by [Mon93, 5.2.2, 2)]. But since h_i' is in a complementary basis to H_0, this forces $\rho(m_i') \in M \otimes H_n$, so $m_i' \in M_n$. Thus, $m \in M_n \wedge H_0$.

For the other direction, let $m \in M_n \wedge H_0$, so we can write $\rho(m) = \sum m_i \otimes h_i$ with $m_i \in M_n$ or $h_i \in H_0$ for all i. This implies that

$$\sum m_i \otimes \Delta(h_i) = \sum \rho(m_i) \otimes h_i \in M \otimes H \otimes H_0 + M \otimes H_n \otimes H$$

which means that $\Delta(h_i) \in H \otimes H_0 + H_n \otimes H$. Thus, $h_i \in H_{n+1}$, which gives us (ii).

Using (ii), we get (iii) from methods which are completely analogous to [Mon93, 5.2.2, 2)].

The proof of (iv) is trivial. For (v), we have, by the definition of comodule algebras, that ρ is an algebra homomorphism. Thus, if $a \in M_i, b \in M_j$, then

$$\rho(ab) = \rho(a)\rho(b) \in (M \otimes H_i)(M \otimes H_j) \subseteq M \otimes H_{i+j}$$

Thus, $ab \in M_{i+j}$. □

This makes $\{M_n\}$ a comodule filtration of M. Notice that if H is connected, then $M_0 = M^{coH}$.

4 Faithfully flat H-Galois extensions

In [Sch90], it is proven that if $A^{coH} \subseteq A$ is a right H-Galois extension, then it is right faithfully flat if and only if it is left faithfully flat. Thus, we can refer to faithfully flat Galois extensions without reference to left or right.

If $A = U(\mathfrak{g})$, we see that $A_1 = U_1$ is an important part of the comodule filtration. It is a Lie subalgebra, and A_0 is a Lie ideal of A_1. This will always be true for $U(\mathfrak{g})$-comodule algebras, so long as A_0 is commutative.

Proposition 4.1. *Let A be a H-comodule algebra, where H is a connected Hopf algebra. If A_0 is commutative, then A_1 is a Lie subalgebra of A, and $A_0 \triangleleft A_1$.*

Proof. Since H is connected, [Mon93, 5.3.2, 1] implies that $H_1 = K1_H \oplus P(H)$. Thus, if we let $a, b \in A_1$, then Lemma 3.3(*iii*) implies that $\rho(a) = a \otimes 1 + \sum_i a_i \otimes h_i$ and $\rho(b) = b \otimes 1 + \sum_i b_i \otimes h_i$, where $\{h_i\}$ is a basis for $P(H)$, and $a_i, b_i \in A_0$. Since ρ is an algebra homomorphism, a quick calculation gives us

$$\rho([a,b]) = \rho(ab - ba) = [a,b] \otimes 1 + \sum_i ([a, b_i] + [a_i, b]) \otimes h_i + \sum_{i,j} a_i b_j \otimes [h_i, h_j]$$

Since $P(H)$ is a Lie subalgebra of H, $\rho([a,b]) \in A \otimes H_1$, and so $[a,b] \in A_1$. This implies that A_1 is a Lie subalgebra of A.

Suppose that a and b are as above, except that $a \in A_0$. Then $a_i = 0$ for all i. Since $b_i \in A_0$ for all i and A_0 is commutative, the b_i's commute with a. We then have $\rho([a,b]) = [a,b] \otimes 1$, and so $[a,b] \in A_0$. Thus, $A_0 \triangleleft A_1$. □

Lemma 4.2. *Let H be a connected Hopf algebra. The map $c : A_1 \to A_0 \otimes P(H)$ given by $a \mapsto \rho(a) - a \otimes 1$ is an A_0-module homomorphism with kernel A_0. If, in addition, A_0 is central, then c is a Lie algebra homomorphism.*

Note: We may equivalently define $c(a) = \beta(1 \otimes a - a \otimes 1)$.

Proof. It is clear that $ker(c) = A_0$. To show that c is an A_0-module homomorphism, we have, for all $a \in A_0$ and $b \in A_1$,

$$\begin{aligned} c(ab) &= \rho(ab) - ab \otimes 1 = \rho(a)\rho(b) - ab \otimes 1 \\ &= (a \otimes 1)\rho(b) - (a \otimes 1)(b \otimes 1) = (a \otimes 1)(\rho(b) - b \otimes 1) = a \cdot c(b) \end{aligned}$$

Finally, if A_0 is central, let $a, b \in A_1$. We then have

$$\begin{aligned} [c(a), c(b)] &= [\rho(a) - a \otimes 1, \rho(b) - b \otimes 1] \\ &= \rho([a,b]) - [a \otimes 1, \rho(b)] - [\rho(a), b \otimes 1] + [a,b] \otimes 1 \\ &= \rho([a,b]) - [a \otimes 1, \rho(b) - b \otimes 1] - [a \otimes 1, b \otimes 1] - \\ &\quad [\rho(a) - a \otimes 1, b \otimes 1] - [a \otimes 1, b \otimes 1] + [a,b] \otimes 1 \end{aligned}$$

Now $a \otimes 1$ commutes with $\rho(b) - b \otimes 1$ since $\rho(b) - b \otimes 1 \in A_0 \otimes P(H)$ and A_0 is central. Similarly, $b \otimes 1$ commutes with $\rho(a) - a \otimes 1$. Thus,

$$\begin{aligned} [c(a), c(b)] &= \rho([a,b]) - [a \otimes 1, b \otimes 1] - [a \otimes 1, b \otimes 1] + [a,b] \otimes 1 \\ &= \rho([a,b]) - [a,b] \otimes 1 = c([a,b]) \end{aligned}$$

□

This gives us the A_0-homomorphism $\bar{c} : A_1/A_0 \to A_0 \otimes P(H)$ given by $a + A_0 \mapsto \rho(a) - a \otimes 1$. If we let $H = U(\mathfrak{g})$, we get

Corollary 4.3. $A_0 \subseteq A$ is faithfully flat $U(\mathfrak{g})$-Galois if and only if $\bar{c}$ is an isomorphism.

Proof. Suppose $A_0 \subseteq A$ is faithfully flat $U(\mathfrak{g})$-Galois. We already know that $\bar{c}$ is injective by Lemma 4.2, so it suffices to prove that it is surjective. Let $x \in \mathfrak{g}$. By Proposition 2.2, there exists some $a_x \in A_1$ such that $\rho(a_x) = a_x \otimes 1 + 1 \otimes x$. We get $\bar{c}(a_x + A_0) = 1 \otimes x$, and so $\bar{c}$ is surjective.

Conversely, for each $x \in \mathfrak{g}$, let $a_x \in A_1$ such that $\bar{c}(a_x + A_0) = 1 \otimes x$. Then $\rho(x) = a_x \otimes 1 + 1 \otimes x$, and thus $A_0 \subseteq A$ is faithfully flat $U(\mathfrak{g})$-Galois by Proposition 2.2 □

Recall that Proposition 2.1 states that a faithfully flat extension $A^{coH} \subseteq A$ is cleft, and thus $A \cong A^{coH} \#_\sigma H$ (see [DT86] or [Mon93, 7.2.3]). Given a convolution invertible total integral $\phi : H \to A$, the isomorphism Ψ is given by $a \mapsto \sum a_0 \phi^{-1}(a_1) \# a_2$. In addition, the crossed product structure is given by $h \cdot a = \sum \phi(h_1) a \phi^{-1}(h_2)$ and the cocycle is $\sigma(h,k) = \sum \phi(h_1)\phi(k_1)\phi^{-1}(h_2 k_2)$.

Lemma 4.4. Let $H = U(\mathfrak{g})$, with notation as in Lemma 3.1. Let A be a right H-comodule algebra, with $A_0 \subseteq A$ faithfully flat. Then $(1\#x_i)(1\#x^{\mathbf{n}}) = 1\#(x_i x^{\mathbf{n}}) + r$, where $r \in A_0 \otimes H_{|\mathbf{n}|}$.

Proof. We have

$$\begin{aligned}(1\#x_i)(1\#x^{\mathbf{n}}) &= \sum \sigma([x_i]_1, x_1^{\mathbf{n}}) \# (x_i)_2 x_2^{\mathbf{n}} \\ &= \sum \sigma(1, x_1^{\mathbf{n}}) \# (x_i x_2^{\mathbf{n}}) + \sum \sigma(x_i, x_1^{\mathbf{n}}) \# x_2^{\mathbf{n}}\end{aligned}$$

From Lemma 3.1, we have $\Delta(x^{\mathbf{n}}) = \sum_{\mathbf{m} \le \mathbf{n}} \binom{\mathbf{n}}{\mathbf{m}} x^{\mathbf{m}} \otimes x^{\mathbf{n}-\mathbf{m}}$. Also, $\sigma(1,h) = \varepsilon(h) 1_A$ by [Mon93, 7.1.2, 2)], so

$$(1\#x_i)(1\#x^{\mathbf{n}}) = 1\#(x_i x^{\mathbf{n}}) + \sum \sigma(x_i, x_1^{\mathbf{n}}) \# x_2^{\mathbf{n}}$$

which completes the proof. □

Lemma 4.5. Let $H = U(\mathfrak{g})$, and let $A_0 \subseteq A$ be a faithfully flat H-Galois extension. Let $a_i = \lambda(x_i)$ as in Proposition 2.2 (so $\rho(a_i) = a_i \otimes 1 + 1 \otimes x_i$). Then $\Psi(a^{\mathbf{n}}) = 1\#x^{\mathbf{n}} + r$, where $r \in A_0 \otimes H_{|\mathbf{n}|-1}$

Proof. We induct on $|\mathbf{n}|$. For $|\mathbf{n}| = 1$, we have $\Psi(a_i) = a_i\#1 - a_i\#1 + 1\#x_i = 1\#x_i$, since $\phi^{-1}(a_i) = -x_i$. For $|\mathbf{n}| > 1$, we can write $a^{\mathbf{n}} = a_i a^{\mathbf{m}}$ for some i and with $|\mathbf{m}| = |\mathbf{n}| - 1$. We then have, by induction,

$$\Psi(a^{\mathbf{n}}) = \Psi(a_i)\Psi(a^{\mathbf{m}}) = (1\#x_i)(1\#x^{\mathbf{m}} + r_1)$$

where $r_1 \in A_0 \otimes H_{|\mathbf{n}|-2}$. Multiplying through, and applying Lemma 4.4, we get

$$\Psi(a^{\mathbf{n}}) = 1\#x^{\mathbf{n}} + r_2 + (1\#x_i) r_1$$

where $r_2 \in A_0 \otimes H_{|\mathbf{n}|-1}$, and the proof is complete. □

Theorem 4.6. Let $A_0 \subseteq A$ be a faithfully flat H-Galois extension for $H = U(\mathfrak{g})$, $\{x_i : i \in I\}$ an ordered basis for $\mathfrak{g}$, and let $a_i = \lambda(x_i)$ as in Proposition 2.2. Then

(i) $\{a_i + A_0 : i \in I\}$ is a free A_0-basis for A_1/A_0. In particular, $\{1_A, a_i : i \in I\}$ is a free A_0-basis for A_1.

(ii) The set $\{a^{\mathbf{n}} : \mathbf{n}$ has finite support$\}$ is a free A_0-basis for A.

Proof. For (i), suppose that $\sum_i b_i(a_i + A_0) = 0$ for some $b_i \in A_0$. Then $\sum_i b_i a_i \in A_0$, so

$$\sum_i b_i a_i \otimes 1 = \rho(\sum_i b_i a_i) = \sum_i b_i a_i \otimes 1 + \sum_i b_i \otimes x_i$$

Thus, $\sum_i b_i \otimes x_i = 0$, and so $b_i = 0$ for all i.

Now suppose $a + A_0 \in A_1/A_0$. Then $\rho(a) = a \otimes 1 + \sum_i b_i \otimes x_i$ for some $b_i \in A_0$. We then have

$$\begin{aligned} \rho(a - \sum_i b_i a_i) &= (a \otimes 1 + \sum_i b_i \otimes x_i) - (\sum_i (b_i \otimes 1)(a_i \otimes 1 + 1 \otimes x_i)) \\ &= (a - \sum_i b_i a_i) \otimes 1 \end{aligned}$$

Thus, $a - \sum_i b_i a_i \in A_0$, and so $a + A_0 = \sum_i b_i(a_i + A_0)$. This gives us that $\{a_i + A_0\}$ is a free A_0-basis for A_1/A_0.

For (ii), assume we have a nontrivial dependence relation

$$\sum_{\mathbf{i}} c_{\mathbf{i}}\, a^{\mathbf{i}} = 0, \quad c_{\mathbf{i}} \in A_0$$

If n is the maximum degree of a monomial with a nonzero coefficient, then we have

$$0 \;=\; \rho(\sum_{\mathbf{i}} c_{\mathbf{i}}\, a^{\mathbf{i}}) = \sum_{|\mathbf{i}|=n} c_{\mathbf{i}} \otimes x^{\mathbf{i}} + s$$

where $s \in A \otimes H_{n-1}$. By the PBW theorem, $c_{\mathbf{i}} = 0$ for all $|\mathbf{i}| = n$. This contradicts our assumption of the existence of a nontrivial dependence relation, and so the $a^{\mathbf{i}}$ are independent over A_0.

It then suffices to show that the $a^{\mathbf{n}}$ span A over A_0. We use the fact that $A \cong A_0 \otimes H$ as A_0-modules under the isomorphism Ψ. We then need only show that if M is the span of all the $a^{\mathbf{n}}$ over A_0, then $1\#x^{\mathbf{n}} \in \Psi(M)$ for all $\mathbf{n}$. We induct on $|\mathbf{n}|$.

The cases $|\mathbf{n}| = 0$ and $|\mathbf{n}| = 1$ are easy to check. For $|\mathbf{n}| > 1$, we have, by Lemma 4.5, that $\Psi(a^{\mathbf{n}}) = 1\#x^{\mathbf{n}} + r$, where $r \in A_0 \otimes H_{|\mathbf{n}|-1}$. By induction, $r \in \Psi(M)$, and therefore $1\#x^{\mathbf{n}} \in \Psi(M)$ as well. □

5 The role of $\bar{c}$ in the non-faithfully flat case

Corollary 4.3 seems to indicate that the behavior of $\bar{c}$ is related to whether or not $A_0 \subseteq A$ is $U(\mathfrak{g})$-Galois. In this section, we attempt to generalize 4.3 to arbitrary $U(\mathfrak{g})$-Galois extensions. It appears that the correct map to consider in this more general context is $id \otimes \bar{c} : A \otimes_{A_0} (A_1/A_0) \to A \otimes_{A_0} (A_0 \otimes_K \mathfrak{g}) \cong A \otimes_K \mathfrak{g}$.

Lemma 5.1. For H a connected Hopf algebra, let $\{h_i\}$ be an ordered basis for $\mathfrak{g} = P(H)$. Let A be an H-comodule algebra, and let $\beta : A \otimes_{A_0} A \to A \otimes H$ be the Galois map. Let $\{a_i\}$ be a generating set for A_1 as an A_0-module. Then $\rho(a_i) = a_i \otimes 1 + \sum_j a_{ij} \otimes h_j$ for some $a_{ij} \in A_0$ by Lemma 3.3(iii). Suppose that the matrix $[a_{ij}]$ has a row finite left inverse $[b_{ij}]$ with entries in A. Then $\beta(A \otimes A_1^n) = A \otimes_K H_1^n$. In particular, β is onto if and only if $H = U(\mathfrak{g})$ or $u(\mathfrak{g})$.

Remark: There is an abuse of notation here. By $A \otimes A_1^n$, we actually mean the span over A_0 of the simple tensors $a \otimes b \in A \otimes_{A_0} A$, where $a \in A$ and $b \in A_1^n$. There is no guarantee that this will be isomorphic to the tensor product $A \otimes_{A_0} A_1^n$ if A is not flat over A_0. We will continue with this abuse of notation with the understanding that it is not the formal tensor product.

Proof. The $n = 0$ case is trivial. For $n = 1$, it suffices to show that $1 \otimes h_i \in \beta(A \otimes A_1)$ for all i. Consider the element $\alpha = \sum_j (b_{ij} \otimes a_j - b_{ij}a_j \otimes 1)$. Since $[b_{ij}]$ is row finite, this is a finite sum, and so $\alpha \in A \otimes A_1$. We have

$$\begin{aligned}
\beta(\alpha) &= \sum_j (b_{ij} \otimes 1)\rho(a_j) - \sum_j (b_{ij}a_j \otimes 1)\rho(1) \\
&= \sum_j b_{ij}a_j \otimes 1 + \sum_{j,k} b_{ij}a_{jk} \otimes h_k - \sum_j b_{ij}a_j \otimes 1 = 1 \otimes h_i
\end{aligned}$$

and so $\beta(A \otimes A_1) = A \otimes_K H_1$. Now we proceed by induction. Assume that $\beta(A \otimes A_1^n) = A \otimes_K H_1^n$. Then

$$\begin{aligned}
\beta(A \otimes A_1^{n+1}) &= (A \otimes 1)\rho(A_1^{n+1}) = (A \otimes 1)\rho(A_1^n)\rho(A_1) \\
&= \beta(A \otimes A_1^n)\rho(A_1) = (A \otimes_K H_1^n)\rho(A_1) \\
&= (A \otimes_K H_1^n)(A \otimes 1)\rho(A_1) = (A \otimes_K H_1^n)\beta(A \otimes A_1) \\
&= (A \otimes_K H_1^n)(A \otimes H_1) = A \otimes H_1^{n+1}
\end{aligned}$$

which completes the proof. □

Proposition 5.2. Let A be an H-comodule algebra for $H = U(\mathfrak{g})$. Then

(i) if $id \otimes \bar{c}$ is onto, then so is β.

(ii) If $A_0 \subseteq A$ is H-Galois and $\beta^{-1}(A \otimes H_1) = A \otimes A_1$, then $id \otimes \bar{c}$ is an isomorphism.

Proof. For (i), let $\{a_i\}$ be a generating set for A_1 as an A_0-module, and let $\{a_{ij}\}$ be as in Lemma 5.1. Since $id \otimes \bar{c}$ is onto, then for each i there exist $b_{ij} \in A$ such that $1 \otimes x_i = (id \otimes \bar{c})(\sum_j b_{ij} \otimes (a_j + A_0))$. Notice that, for each i, there are only finitely many j such that $b_{ij} \neq 0$, so the matrix $[b_{ij}]$ is row finite. But this gives us

$$1 \otimes x_i = \sum_{j,k} b_{ij} a_{jk} \otimes x_k$$

and so $\sum_j b_{ij} a_{jk} = \delta_{i,k}$. Thus, $[a_{ij}]$ has a row finite left inverse, and so β is onto by Lemma 5.1.

Now we consider (ii). Since $\beta^{-1}(A \otimes H_1) = A \otimes A_1$ and the a_i's generate A_1 over A_0 by Theorem 4.6(i), then for each i, there exist $b_{ij} \in A$ such that $\beta^{-1}(1 \otimes x_i) = \sum_j b_{ij} \otimes a_j$. Since β^{-1} is A-linear, we have $\beta^{-1}(a \otimes x_i) = \sum_j ab_{ij} \otimes a_j$. Define $\gamma : A \otimes_K \mathfrak{g} \longrightarrow A \otimes_{A_0} (A_1/A_0)$ by $\gamma(a \otimes x_i) = \sum_j ab_{ij} \otimes (a_j + A_0)$. For each $a \in A$ and $b \in A_1$, we have $\rho(b) = b \otimes 1 + \sum_i b_i \otimes x_i$ for some $b_i \in A_0$, and so

$$[\gamma \circ (id \otimes \bar{c})](a \otimes (b + A_0)) = \gamma(\sum_i ab_i \otimes x_i) = \sum_{i,j} ab_i b_{ij} \otimes (a_j + A_0)$$

But we also have that

$$\begin{aligned} a \otimes b &= \beta^{-1} \circ \beta(a \otimes b) = \beta^{-1}(ab \otimes 1 + \sum_i ab_i \otimes x_i) \\ &= ab \otimes 1 + \sum_{i,j} ab_i b_{ij} \otimes a_j \qquad (1) \end{aligned}$$

If we let $\pi : A_1 \longrightarrow A_1/A_0$ be the canonical homomorphism, then, applying $id \otimes \pi$ to both sides of (1) gives us $a \otimes (b + A_0) = \sum_{i,j} ab_i b_{ij} \otimes (a_j + A_0)$, and so $\gamma \circ (id \otimes \bar{c}) = id$.

For the other direction, we have

$$\begin{aligned} [(id \otimes \bar{c}) \circ \gamma](a \otimes x_i) &= (id \otimes \bar{c})(\sum_j ab_{ij} \otimes (a_j + A_0)) \\ &= \sum_{j,k} ab_{ij} a_{jk} \otimes x_k \end{aligned}$$

But we have $1 \otimes x_i = \beta \circ \beta^{-1}(1 \otimes x_i) = \beta(\sum_j b_{ij} \otimes a_j) = \sum_j b_{ij} a_j \otimes 1 + \sum_{j,k} b_{ij} a_{jk} \otimes x_k$. This implies that $\sum_j b_{ij} a_{jk} = \delta_{i,k}$, and thus $\sum_{j,k} ab_{ij} a_{jk} \otimes x_k = a \otimes x_i$. This gives us $[(id \otimes \bar{c}) \circ \gamma](a \otimes x_i) = a \otimes x_i$, and so $\gamma = (id \otimes \bar{c})^{-1}$. Thus, $id \otimes \bar{c}$ is an isomorphism. □

Note that we have a filtration of the A-module $A \otimes_{A_0} A$ given by $(A \otimes_{A_0} A)_n = A \otimes A_n$. Recall that a homomorphism f between two filtered A-modules M and N is said to have degree p if $f(M_i) \subseteq N_{i+p}$ for all i. It is easy to see that β is a homomorphism of degree 0 for any $U(\mathfrak{g})$-comodule algebra. However, if β is bijective, it is not clear that β^{-1} is of degree zero. But if, in addition, $id \otimes \bar{c}$ is onto, then 5.2 implies that $\beta|_{A \otimes A_n}$ is onto $A \otimes H_n$ for $H = U(\mathfrak{g})$. In this case, β^{-1} is a homomorphism of degree 0 as well. So

(ii) implies that if $A_0 \subseteq A$ is $U(\mathfrak{g})$-Galois, then β^{-1} is a homomorphism of degree 0 if $\beta^{-1}(A \otimes U_1) = A \otimes_{A_0} A_1$.

Proposition 5.2 leads one to consider what role $id \otimes \bar{c}$ plays in determining whether or not $A_0 \subseteq A$ is $U(\mathfrak{g})$-Galois. We ask

Question 5.3. Is $A_0 \subseteq A$ a $U(\mathfrak{g})$-Galois extension if and only if $id \otimes \bar{c}$ is an isomorphism?

If we knew that β^{-1} must be a homomorphism of degree 0 for any Galois extension, or, equivalently, that $\beta^{-1}(A \otimes U_1) = A \otimes A_1$, that would give us one direction ($\Rightarrow$). The other direction seems more difficult.

References

[Bel00] A.D. Bell, *Comodule algebras and Galois extensions relative to polynomial algebras, free algebras, and enveloping algebras*, Comm. Algebra **28** (2000), 337–362.

[CHR65] S.U. Chase, D.K. Harrison, and A. Rosenberg, *Galois theory and cohomology of commutative rings*, AMS Memoirs **No. 52** (1965).

[DT86] Y. Doi and M. Takeuchi, *Cleft comodule algebras for a bialgebra*, Comm. Alg. **14** (1986), 801–818.

[KT81] H.F. Kreimer and M. Takeuchi, *Hopf algebras and Galois extensions of an algebra*, Indiana Univ. Math. J. **30** (1981), 675–692.

[Mon93] S. Montgomery, *Hopf Algebras and Their Actions on Rings*, AMS, Providence, R.I., 1993.

[Sch90] H.J. Schneider, *Principal homogeneous spaces for arbitrary Hopf algebras*, Israel J. Math **72** (1990), 167–195.

[Ulb81] K.H. Ulbrich, *Vollgraduierte Algebren*, Abh. Math. Sem. Univ. Hamburg **51** (1981), 136–148.