Hopf Galois Extensions and Forms of Coalgebras and Hopf algebras

By

Darren B. Parker

A dissertation submitted in partial fulfillment of the

requirements for the degree of

Doctor of Philosophy

(Mathematics)

at the

UNIVERSITY OF WISCONSIN – MADISON

2005

Abstract

The results of this thesis are motivated by problems in the descent theory of coalgebras and Hopf algebras. If H and H' are coalgebras (or Hopf algebras) over the same field K, we attempt to find out when they are isomorphic after an extension of the base field. In other words, when is $L \otimes_K H \cong L \otimes_K H'$ for some field extension $K \subseteq L$? If H and H' are related in this way, they are said to be L-forms of each other.

In the course of studying descent theory, it becomes apparent that the nature of the field extension plays a key role. In the descent theory of Hopf algebras, this leads us naturally to the notion of Hopf Galois extensions. Hopf Galois extensions are generalizations of classical Galois field extensions, and are of interest in their own right.

The first three chapters of this thesis are devoted primarily to background material. Only 3.30 was previously unknown. Chapter 1 defines coalgebras and Hopf algebras, and gives an introduction to some of the elementary results in Hopf algebras. Chapter 2 contains the basic definitions of descent theory, and shows how these concepts can be applied to coalgebras and Hopf algebras. Chapter 3 introduces Hopf algebra actions and coactions on associative algebras, and develops these ideas to give us the definition of Hopf Galois extensions.

In Chapter 4, we begin the original results with the study of $U(\mathfrak{g})$-Galois extensions. We use a result of Bell to construct a "PBW"-like basis for faithfully

flat $U(\mathfrak{g})$-Galois extensions under certain hypotheses. Even when these hypotheses are not assumed, there are still close links between faithfully flat $U(\mathfrak{g})$-Galois extensions and $U(\mathfrak{g})$ itself. We then look at the case where the extension is not faithfully flat. It appears that whether or not an extension is $U(\mathfrak{g})$-Galois is related to a certain function $\bar{c}$ defined in Section 4.2.

In Chapter 5, we turn to the descent theory of coalgebras and Hopf algebras. In Section 5.1, we characterize the forms of grouplike coalgebras according to the structure of their simple subcoalgebras. In Section 5.2, we show how to compute the L-forms of an arbitrary K-Hopf algebra if the field extension $K \subseteq L$ is W^*-Galois for a finite dimensional semisimple Hopf algebra W. They turn out to be the invariant rings $[L \otimes H]^W$ of certain actions of W on $L \otimes H$. This result is articulated in Theorem 5.18. We also propose a conjecture which strengthens this result. This is given in Question 5.23.

Chapter 6 is devoted to computing examples using Theorem 5.18. In Section 6.1, we characterize forms of enveloping algebras. We then compute the L-forms for a specific Lie algebra $\mathfrak{g}$ and field extension $K \subseteq L$, and we observe that they satisfy the conjecture posed in Question 5.23. In Section 6.2, we turn our attention to computing forms for the dual H^* of a finite dimensional Hopf algebra H. We show that, under certain hypotheses, there is a correspondence between the L-forms of H satisfying Question 5.23 and the L-forms of H^* satisfying Question 5.23. We get a stronger result for group actions. Finally, in Section 6.3, we compute an L-form for the dihedral group algebra KD_{2n} using the adjoint action.

Acknowledgements

I would first like to thank my thesis advisor, Donald Passman, who encouraged my independence as a mathematician and gave me support. He is a terrific brainstorming partner and mentor, and his deep insights into a field which is not his own still bewilder me. I also enjoyed his dry sense of humor.

To my fiancee Stephanie Edwards, I owe more than can fit on this page. I will always be grateful for the love and support she has given me. She is simply the best.

Harry Mullikin has been family, friend, and teacher to me. He took especially good care of me during my undergraduate years.

I would be remiss if I did not mention my loving parents, who supported their son's crazy idea to spend six extra years studying math. Plus, they might send me to my room. Thanks, Mom and Dad!

I want to thank my brother Brent for his support and good humor through the years. I do not think I would have been able to survive six years of graduate school if he had not helped me learn not to take myself too seriously.

Thanks also to James Pate, my high school math teacher, who taught me about the many joys of math, and the importance of drawing a picture.

I have had many friends who have helped me along the way. They have given me emotional support, mathematical insights, and many happy memories. They include Antonio Behn, John Caughman, Jonathan Celeste, Joan Hart, Jeff Hildebrand, Christopher Kribs, Rowan Littel, Chia-Hsin Liu, David Moulton, David

Musicant, Jeff Riedl, Stephanie Wang, and Jennifer Ziebarth. Thank you all for your warm friendship.

Contents

Chapter 1

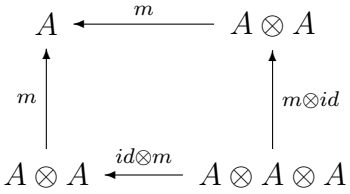
Preliminaries

In this chapter, we investigate some of the elementary properties of coalgebras and Hopf algebras. The first section is devoted to basic definitions and examples. Next, we show how to construct new Hopf algebras out of old ones. Lastly, we define cosemisimplicity and the coradical of a coalgebra.

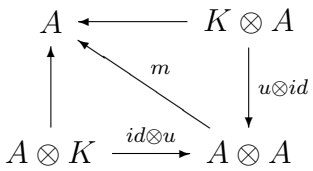
1.1 Coalgebras and Hopf algebras

The basic references for the material here are [Mon93] and [Swe69]. The base ring is always K, which we assume to be a field unless otherwise specified, and $\otimes$ is always meant to be $\otimes_K$, that is tensor product over K.

Let A be an associative K-algebra. We can think of multiplication in A as a linear map $m : A \otimes A \to A$ given by $a \otimes b \mapsto ab$. There is also an embedding $u : K \to A, k \mapsto k1_A$. These maps give rise to the following commutative diagrams:



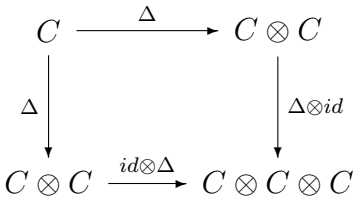
(Associativity)



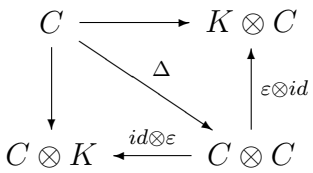
(Unit)

The first diagram comes from associativity of the multiplication in A, and the second arises from the equality $(k1_A)a = a(k1_A) = ka$ for all $k \in K$ and $a \in A$. In fact, the maps m and u along with the above commuting diagrams completely determine the algebra A once the K-vector space structure is known, and so associative algebras can be defined by the above diagrams. A coalgebra is the formal dual of an associative algebra. In other words, we take the arrows in the commuting diagrams, and run them in the opposite direction.

Definition 1.1. A coalgebra over K is a K-vector space C with linear maps $\Delta : C \to C \otimes C$ and $\varepsilon : C \to K$, which make the following diagrams commute:



(Coassociativity)



(Counit)

In fact, we can dualize almost any property in associative algebras and apply it to coalgebras. For instance, if we let τ be the "twist" homomorphism given by $\tau(a \otimes b) = b \otimes a$, then commutativity is equivalent to $m = m \circ \tau$. Dualizing, we get cocommutativity, which is $\Delta = \tau \circ \Delta$.

Computations can be cumbersome with commutative diagrams, so we use the Sweedler summation notation. For $c \in C$, $\Delta(c)$ is a sum of simple tensors, so we write $\Delta(c) = \sum_{(c)} c_{(1)} \otimes c_{(2)}$. The (1) and (2) are merely place holders for the elements of C on the right and left of the tensor symbol. We generally dispense with the parentheses and the (c), and simply write $\Delta(c) = \sum c_1 \otimes c_2$.

Sweedler notation and coassociativity give us the equality $\sum \Delta(c_1) \otimes c_2 = \sum c_1 \otimes \Delta(c_2)$, and we write these both as $\sum c_1 \otimes c_2 \otimes c_3$, and so on. Applying Sweedler notation to cocommutativity, we see that C is cocommutative if and only if $\sum c_1 \otimes c_2 = \sum c_2 \otimes c_1$ for all $c \in C$.

Example 1.2. The counit diagram gives us $\sum \varepsilon(c_1)c_2 = \sum \varepsilon(c_2)c_1 = c$.

Definition 1.3. A bialgebra is a coalgebra and an associative algebra such that Δ and ε are algebra homomorphisms. A Hopf algebra is a bialgebra such that there exists a map $S : H \to H$ which satisfies $\sum h_1 S(h_2) = \sum S(h_1)h_2 = \varepsilon(h)1_H$ for all $h \in H$. The map S is called the antipode.

The conditions for a bialgebra are equivalent to m and u being coalgebra morphisms (see 1.9). The conditions on S seem a bit strange, but it becomes more natural when we consider the following.

Definition 1.4. Let H be a coalgebra, A be an associative algebra. We define the convolution product on $Hom_K(H, A)$ as follows. Let $f, g \in Hom_K(H, A)$ and $h \in H$. Then $(f * g)(h) = \sum f(h_1)g(h_2)$.

We get the following well-known fact.

Proposition 1.5. Under the convolution product, $Hom_K(H, A)$ is an associative algebra with unit $u \circ \varepsilon : h \mapsto \varepsilon(h)1_A$.

Proof. Let $f, g, k \in Hom_K(H, A)$, $h \in H$. Then

$$\begin{aligned} ((f * g) * k)(h) &= \sum (f * g)(h_1)k(h_2) = \sum f(h_1)g(h_2)k(h_3) \\ &= \sum f(h_1)(g * k)(h_2) = (f * (g * k))(h) \end{aligned}$$

Thus, $(f * g) * k = f * (g * k)$. For the unit, we have

$$(f * (u \circ \varepsilon))(h) = \sum f(h_1)\varepsilon(h_2)1_A = f(\sum \varepsilon(h_2)h_1) = f(h)$$

and so $f * (u \circ \varepsilon) = f$. Similarly, $(u \circ \varepsilon) * f = f$. □

Now we can make sense of the conditions on S. If H is a Hopf algebra, it is both a coalgebra and an associative algebra, and so $Hom_K(H, H)$ is an associative algebra under the convolution product. We also have

$$(S * id)(h) = \sum S(h_1)h_2$$
$$(id * S)(h) = \sum h_1 S(h_2)$$

and so the conditions on S say that $S * id = id * S = u \circ \varepsilon$. Thus, S is the inverse of id under the convolution product. In particular, the antipode is unique.

Example 1.6. Let KG be a group algebra. For each $g \in G$, define $\Delta(g) = g \otimes g$, $\varepsilon(g) = 1$, and $S(g) = g^{-1}$, and extend these maps linearly. It is easy to check that this makes KG a Hopf algebra.

Example 1.7. Let $\mathfrak{g}$ be a Lie algebra (or restricted Lie algebra), and let H be the universal (resp. restricted) enveloping algebra of $\mathfrak{g}$. For $x \in \mathfrak{g}$, define $\Delta(x) = 1 \otimes x + x \otimes 1$, $\varepsilon(x) = 0$, and $S(x) = -x$. One can easily verify that $\Delta : \mathfrak{g} \to H \otimes H$ and $\varepsilon : \mathfrak{g} \to K$ are Lie algebra homomorphisms, and that $S : \mathfrak{g} \to \mathfrak{g}$ is a Lie anti-homomorphism on $\mathfrak{g}$. By the universal property of H, Δ and ε can be extended to algebra homomorphisms on H. Similarly, S can be extended to an anti-homomorphism on H. One can check that this will make H a Hopf algebra.

Given the importance of these examples, we define the following.

Definition 1.8. Let H be a coalgebra.

(i) The set of grouplike elements in H is $G(H) = \{h \in H : h \neq 0, \Delta(h) = h \otimes h\}$. H is said to be a grouplike coalgebra if it is spanned by grouplike elements. In this case, we write $H = KG(H)$.

(ii) If $g, h \in G(H)$, the set of g,h-primitives is $P_{g,h}(H) = \{x \in H : \Delta(x) = x \otimes g + h \otimes x\}$. If H is a bialgebra, then the elements in $P(H) = P_{1,1}(H)$ are the primitive elements of H.

It is easy to show that any set of distinct grouplikes is linearly independent, and hence $G(KG) = G$. Also, if $\mathrm{char}(K) = 0$, then $P(U(\mathfrak{g})) = \mathfrak{g}$ (see [Mon93, 5.5.3]) and similarly for restricted enveloping algebras in characteristic $p > 0$.

We now discuss what we mean by a morphism $f : H \to H'$ between coalgebras, bialgebras, and Hopf algebras. We want such maps to preserve the structure of H. For the most part, this comes down to dualizing the notion of algebra homomorphisms.

Definition 1.9. Let H and H' be coalgebras (resp. bialgebras or Hopf algebras), and suppose $f : H \to H'$ is a linear map. Denote comultiplication, counit, and antipode for H as Δ_H, ε_H, and S_H, and similarly for H'.

(i) f is a coalgebra morphism if $\Delta_{H'} \circ f = (f \otimes f) \circ \Delta_H$ and $\varepsilon_{H'} \circ f = \varepsilon_H$.

(ii) f is a bialgebra morphism if it is both a coalgebra morphism and an algebra homomorphism.

(iii) f is a Hopf algebra morphism if it is a bialgebra morphism and $f \circ S_H = S_{H'} \circ f$.

We can then define coideals, biideals, and Hopf ideals to be the kernels of their

respective morphisms. We get

Definition 1.10. (i) A coideal C of a coalgebra H is a subspace of H such that $\Delta(C) \subseteq C \otimes H + H \otimes C$ and $\varepsilon(C) = 0$.

(ii) A biideal of a bialgebra H is a subspace of H that is both an ideal and a coideal.

(iii) A Hopf ideal I of a Hopf algebra H is a biideal of H such that $S(I) \subseteq I$.

1.2 Basic constructions

We now proceed to show how one can construct Hopf algebras from other Hopf algebras. We start with the tensor product.

Proposition 1.11. (i) Let $(H, \Delta_H, \varepsilon_H)$ and $(H', \Delta_{H'}, \varepsilon_{H'})$ be coalgebras. Then $H \otimes H'$ is a coalgebra with comultiplication and counit given by $\Delta_{H\otimes H'}(h \otimes h') = \sum(h_1 \otimes h'_1) \otimes (h_2 \otimes h'_2)$, $\varepsilon_{H\otimes H'}(h \otimes h') = \varepsilon_H(h)\varepsilon_{H'}(h')$

(ii) If H and H' are bialgebras, then so is $H \otimes H'$. If, in addition, H and H' are Hopf algebras, then $H \otimes H'$ is a Hopf algebra with antipode $S_{H\otimes H'}(h \otimes k) = S_H(h) \otimes S_{H'}(k)$.

For our next construction, recall that, for any vector space H, we can construct the dual space $H^* = Hom_K(H, K)$.

Proposition 1.12. *[Mon93, 1.2.2, 1.2.4]* (i) If H is a coalgebra, then H^* is an associative algebra with multiplication Δ^* and unit ε. Also, if H is cocommutative, then H^* is commutative.

(ii) If H is a finite dimensional associative algebra, then H^* is a coalgebra with comultiplication $\Delta = m^*$ and counit $\varepsilon = u^*$. Also, if H is commutative, then H^* is cocommutative.

(iii) If H is a finite dimensional bialgebra (resp. Hopf algebra), then H^* is a bialgebra (resp. Hopf algebra with antipode S^*).

Proof. For (i), assume H is a coalgebra. Now K is an associative K-algebra, so by 1.5, $H^* = Hom_K(H, K)$ is an associative algebra under the convolution product with unit ε. It is a simple computation to show that $f*g = (f\otimes g)\circ\Delta = \Delta^*(f\otimes g)$.

Now suppose that H is cocommutative, so $\sum h_1\otimes h_2 = \sum h_2\otimes h_1$ for all $h \in H$. Then

$$(f * g)(h) = \sum f(h_1)g(h_2) = \sum f(h_2)g(h_1) = (g * f)(h)$$

Thus, H^* is commutative.

For (ii), suppose that H is a finite dimensional associative algebra. Then, for all $f \in H^*$, we have $\Delta(f) = f \circ m \in (H \otimes H)^* \cong H^* \otimes H^*$ and $\varepsilon(f) = f(1)$. Thus, if $\Delta(f) = \sum f_i \otimes g_i$, then $\sum f_i(h)g_i(k) = f(hk)$ for all $h, k \in H$. We need to show that $\sum f_i \otimes \Delta(g_i) = \sum \Delta(f_i) \otimes g_i$ to prove coassociativity. Let $h, k, l \in H$. Then

$$\begin{aligned}
(\sum f_i \otimes \Delta(g_i))(h \otimes k \otimes l) &= \sum f_i(h)\Delta(g_i)(k \otimes l) \\
&= \sum f_i(h)g_i(kl) \\
&= f(hkl) \\
&= \sum f_i(hk)g_i(l) \\
&= \sum \Delta(f_i)(h \otimes k)g_i(l) \\
&= (\sum \Delta(f_i) \otimes g_i)(h \otimes k \otimes l)
\end{aligned}$$

For the counit, we have $(\sum \varepsilon(f_i)g_i)(h) = \sum f_i(1)g_i(h) = f(h)$, so $\sum \varepsilon(f_i)g_i = f$. Similarly, $\sum \varepsilon(g_i)f_i = f$, so H^* is a coalgebra.

Now suppose that H is commutative. Again write $\Delta(f) = \sum f_i \otimes g_i$. For all $h, k \in H$,

$$(\sum f_i \otimes g_i)(h \otimes k) = \sum f_i(h)g_i(k) = f(hk) = f(kh) = (\sum g_i \otimes f_i)(h \otimes k)$$

and therefore H^* is cocommutative.

For (iii), we need only show that Δ and ε are algebra homomorphisms, and that S^* satisfies the required relations. Let $f, g \in H^*$, $h, k \in H$. Since Δ is an algebra homomorphism, then

$$\sum [hk]_1 \otimes [hk]_2 = \Delta_H(hk) = \Delta_H(h)\Delta_H(k) = \sum h_1k_1 \otimes h_2k_2$$

We get

$$\begin{aligned}
\Delta(fg)(h \otimes k) &= fg(hk) \\
&= \sum f([hk]_1)g([hk]_2) \\
&= \sum f(h_1k_1)g(h_2k_2) \\
&= \sum \Delta(f)(h_1 \otimes k_1)\Delta(g)(h_2 \otimes k_2) \\
&= (\Delta(f)\Delta(g))(h \otimes k)
\end{aligned}$$

Also, $\Delta(\varepsilon_H)(h \otimes k) = \varepsilon_H(hk) = \varepsilon_H(h)\varepsilon_H(k) = (\varepsilon_H \otimes \varepsilon_H)(h \otimes k)$, so $\Delta(\varepsilon) = \varepsilon \otimes \varepsilon$. Thus, Δ is an algebra homomorphism. To prove ε is an algebra homomorphism, we have

$$\varepsilon(fg) = fg(1) = f(1)g(1) = \varepsilon(f)\varepsilon(g)$$

Now suppose H is a Hopf algebra. We need to show that, for all $f \in H^*$, $\sum S^*(f_1)f_2 = \sum f_1 S^*(f_2) = \varepsilon(f)\varepsilon_H$. We have, for each $h \in H$,

$$\begin{aligned}(\sum S^*(f_1)f_2)(h) &= \sum S^*(f_1)(h_1)f_2(h_2) = \sum f_1(S(h_1))f_2(h_2) \\ &= f(\sum S(h_1)h_2) = \varepsilon_H(h)f(1) = \varepsilon(f)\varepsilon_H(h)\end{aligned}$$

The other equality is similar. □

For infinite dimensional Hopf algebras, H^* will not, in general, be a Hopf algebra. However, something can still be said. Let $H^\circ = \{f \in H^* : f(I) = 0$ for some $I \lhd H$ of finite codimension$\}$.

Theorem 1.13. *[Mon93, 9.1.1, 9.1.3]* Let H be a bialgebra.

(i) If $f \in H^*$, then $f \in H^\circ$ if and only if $m^*(f) \in H^* \otimes H^*$.

(ii) H° is a bialgebra with comultiplication m^* and counit u^*. If H is a Hopf algebra, then so is H° with antipode S^*.

Next, we characterize the grouplike elements in H°

Proposition 1.14. *[Mon93, 1.3]* $G(H^\circ) = Alg(H, K)$, where $Alg(H, K)$ is the set of K-algebra homomorphisms between H and K.

Proof. Let $f \in G(H^\circ)$. Then, for all $h, k \in H$, we have

$$f(hk) = \Delta(f)(h \otimes k) = (f \otimes f)(h \otimes k) = f(h)f(k)$$

In particular, $f(h) = f(h)f(1)$, and so, in addition, $f(1) = 1$. Thus, f is an algebra homomorphism. The converse is similar. □

Our last construction, in some sense, reverses the comultiplication of H. It is dual to the notion of the opposite algebra A^{op}.

Definition 1.15. Let H be a coalgebra. Then the coopposite coalgebra H^{cop} is H as a set, its counit ε is the same as for H, but its comultiplication is given by $\Delta'(h) = \sum h_2 \otimes h_1$.

It is easy to show that if H is a bialgebra, then so is H^{cop}. However, if H is a Hopf algebra, H^{cop} is not necessarily a Hopf algebra. To find out when H^{cop} will be a Hopf algebra, we will need a result about how multiplication and comultiplication interact with the antipode of a Hopf algebra. Recall the examples of the group algebra and the universal enveloping algebra. In each of these cases, the antipode is an anti-homomorphism. This is true in general, along with a "dual" anti-homomorphism property.

Proposition 1.16. *[Swe69]* Let H be a Hopf algebra.

(i) S is an algebra anti-homomorphism (i.e. $S(hk) = S(k)S(h)$, and $S(1) = 1$).

(ii) $\Delta \circ S(h) = \sum S(h_2) \otimes S(h_1), \varepsilon \circ S = \varepsilon$.

A map that satisfies (ii) is called a coalgebra anti-morphism.

Proof. (i) First of all, we know $\sum h_1 S(h_2) = \varepsilon(h)1_H$. For $h = 1$, we have $\Delta(1) = 1 \otimes 1$, since Δ is an algebra homomorphism. Thus, $S(1) = 1$.

Now consider the linear maps $f : H \otimes H \to H$ and $g : H \otimes H \to H$ given by $f(h \otimes k) = S(hk), g(h \otimes k) = S(k)S(h)$. We want to show that $f = g$. Let m be the multiplication map on H. Since $H \otimes H$ and H are Hopf algebras, we can multiply these functions together via the convolution product. We have, for all

$h, k \in H$,

$$\begin{aligned}
(f * m)(h \otimes k) &= \sum f(h_1 \otimes k_1) m(h_2 \otimes k_2) = \sum S(h_1 k_1) h_2 k_2 \\
&= \sum S([hk]_1)[hk]_2 = \varepsilon(hk) 1_H \\
&= \varepsilon(h)\varepsilon(k) 1_H = \varepsilon_{H \otimes H}(h \otimes k) \\
(m * g)(h \otimes k) &= \sum m(h_1 \otimes k_1) g(h_2 \otimes k_2) = \sum h_1 k_1 S(k_2) S(k_1) \\
&= \sum \varepsilon(k) h_1 S(h_2) = \varepsilon(k)\varepsilon(h) \\
&= \varepsilon_{H \otimes H}(h \otimes k)
\end{aligned}$$

Thus, m is invertible, and in fact $f = m^{-1} = g$. This proves (i).

(ii) Our arguments here are dual to those above. First of all,

$$\begin{aligned}
\varepsilon(S(h)) &= \varepsilon(S(\sum \varepsilon(h_1) h_2)) = \sum \varepsilon(h_1)\varepsilon(S(h_2)) \\
&= \sum \varepsilon(h_1 S(h_2)) = \varepsilon(\varepsilon(h)) \\
&= \varepsilon(h)\varepsilon(1) = \varepsilon(h)
\end{aligned}$$

Thus, $\varepsilon \circ S = \varepsilon$.

Now define $\phi : H \to H \otimes H, \gamma : H \to H \otimes H$ by $\phi(h) = (\Delta \circ S)(h), \gamma(h) = \sum S(h_2) \otimes S(h_1)$. Our aim is to show that $\phi = \gamma$. We have

$$\begin{aligned}
(\phi * \Delta)(h) &= \sum \phi(h_1)\Delta(h_2) = \sum \Delta(S(h_1))\Delta(h_2) \\
&= \sum \Delta(S(h_1)h_2) = \Delta(\varepsilon(h)) = \varepsilon(h)(1 \otimes 1) \\
(\Delta * \gamma)(h) &= \sum \Delta(h_1)\gamma(h_2) = \sum \Delta(h_1)(S(h_3) \otimes S(h_2)) \\
&= \sum (h_1 \otimes h_2)(S(h_4) \otimes S(h_3)) = \sum h_1 S(h_4) \otimes h_2 S(h_3) \\
&= \sum \varepsilon(h_2) h_1 S(h_3) \otimes 1 = \sum h_1 S(h_2) \otimes 1 = \varepsilon(h)(1 \otimes 1)
\end{aligned}$$

This gives us $\phi = \Delta^{-1} = \gamma$, which completes the proof. $\square$

Proposition 1.17. *[Mon93, 1.5.11]* Let H be a bialgebra. Then H^{cop} is a Hopf algebra if and only if H is a Hopf algebra and S_H is invertible. Furthermore, $S_{H^{cop}} = S_H^{-1}$ (composition inverse).

Proof. Suppose that H^{cop} is a Hopf algebra. Let $S_H = S, S_{H^{cop}} = \bar{S}$. From 1.16, both S and $\bar{S}$ are anti-homomorphisms and coalgebra anti-morphisms. Then

$$\begin{aligned} S(\bar{S}(h)) &= \sum \varepsilon(h_1)S(\bar{S}(h_2)) = \sum h_1 S(h_2)S(\bar{S}(h_3)) = \sum h_1 S(\bar{S}(h_3)h_2) \\ &= \sum \varepsilon(h_2)h_1 S(1) = h \end{aligned}$$

Similarly, $\bar{S} \circ S = id$, so S is invertible and $\bar{S} = S^{-1}$. For the converse, we first show that S^{-1} is an algebra anti-homomorphism. Let $h, h' \in H$. Write $l = S^{-1}(h), l' = S^{-1}(h')$, where $l, l' \in H$. Then

$$S^{-1}(hh') = S^{-1}(S(l)S(l')) = S^{-1}(S(l'l)) = l'l = S^{-1}(h')S^{-1}(h)$$

Also, clearly $S^{-1}(1) = 1$.

Now we need to show, for all $h \in H$ that

$$\sum S^{-1}(h_2)h_1 = \sum h_2 S^{-1}(h_1) = \varepsilon(h)1_H$$

We know that $\sum h_1 S(h_2) = \sum S(h_1)h_2 = \varepsilon(h)1_H$. Simply apply S^{-1} to these equations, and we get the desired result. □

Corollary 1.18. *[Mon93, 1.5.12]* Let H be a commutative or cocommutative Hopf algebra. Then $S^2 = id$.

Proof. If H is cocommutative, then $\sum h_2 S(h_1) = \sum h_1 S(h_2) = \varepsilon(h)1_H$. Similarly, $\sum S(h_2)h_1 = \varepsilon(h)1_H$. Thus, S is an antipode for H^{cop}, and so $S = S^{-1}$ by 1.17. This implies $S^2 = id$.

For the commutative case, $\sum h_2 S(h_1) = \sum S(h_1)h_2 = \varepsilon(h)1_H$. Similarly, $\sum S(h_2)h_1 = \varepsilon(h)1_H$. As before, $S^2 = id$. □

1.3 Cosemisimplicity and the coradical

Now we dualize the notions of simplicity and semisimplicity of associative algebras.

Definition 1.19. Let H be a coalgebra.

(i) H is said to be simple if it has no proper nontrivial subcoalgebras.

(ii) The coradical H_0 is the sum of all the simple subcoalgebras of H.

(iii) H is cosemisimple if $H = H_0$.

These are indeed dual to their corresponding concepts in associative algebras, since H is a simple coalgebra if and only if H^* is a (finite dimensional) simple algebra [Mon93, 5.1.4]. Also, $J(H^*) = H_0^\perp$ [Mon93, 5.2.9], so it is easy to see that H is cosemisimple $\Leftrightarrow H_0^\perp = 0 \Leftrightarrow H^*$ is semisimple. Note that by [Mon93, 5.1.2], all simple coalgebras are finite dimensional.

In fact, more can be said about the coradical.

Proposition 1.20. *[Swe69, 8.0.3, 8.0.6]*

(i) Let $H = \sum_i C_i$, where C_i are subcoalgebras. Then any simple subcoalgebra lies in one of the C_i.

(ii) Let $\{H_i\}$ be a set of distinct simple subcoalgebras. Then the sum of these coalgebras is direct.

(iii) $H_0 = \oplus_i H_i$, where the H_i are all the (distinct) simple subcoalgebras of H.

Definition 1.21. Let H be a coalgebra.

(i) H is said to be pointed if every simple subcoalgebra is one-dimensional.

(ii) H is said to be connected if H_0 is one-dimensional.

Since H_0 contains all the simple subcoalgebras of H, then any connected coalgebra is a pointed coalgebra. Also, it is easy to check that any one-dimensional subcoalgebra of H must be of the form Kg, where $g \in G(H)$. Thus, H is pointed if and only if $H_0 = KG(H)$. Consequently, all group algebras are pointed. In addition, by [Mon93, 5.5.3], we have that $U(\mathfrak{g})$ is connected.

The coradical has additional importance. Define inductively, for each $n \geq 1$, $H_n = \Delta^{-1}(H \otimes H_{n-1} + H_0 \otimes H)$. The H_n form a coalgebra filtration, by which is meant the following.

Theorem 1.22. *[Mon93, 5.2.2]* For all $n \geq 0$, the family $\{H_n\}$ satisfies

(i) $H_n \subseteq H_{n+1}$ and $H = \bigcup_{n \geq 0} H_n$.

(ii) $\Delta(H_n) \subseteq \sum_{i=0}^{n} H_i \otimes H_{n-i}$.

Chapter 2

Theory of Descent

Given a K-coalgebra or Hopf algebra, one may ask what happens if the base field is extended (e.g. to the algebraic closure of K). One may also ask whether or not two coalgebras or Hopf algebras are isomorphic after extension of the base field. Questions of these types are dealt with in descent theory.

In this chapter, we introduce the basic definitions of descent theory. Then we describe how these definitions can be applied to coalgebras and Hopf algebras.

2.1 General descent theory

Much of the material and notation here comes from [Knu74]. Let K be a commutative ring, L a commutative K-algebra. Given a left K-module M, we can construct the L-module $M_L = L \otimes M$. Thus, we can take K-modules and "ascend" to L-modules. The goal of descent theory is to say something about what happens when we go in the other direction. In other words, if we start with L-modules, what happens when we "descend" to K-modules?

An example of the type of problem encountered is the following. Given an element $y \in M_L$, what conditions will guarantee that $y = 1_L \otimes x$ for some $x \in M$? This is a problem in descent of elements.

Example 2.1. Let $K \subseteq L$ be a finite Galois field extension. Then K is a K-module and $K_L = L \otimes K \cong L$. So the descent of elements problem mentioned above is equivalent to asking when an element $a \in L$ is in K. Of course this happens if and only if $\sigma(a) = a$ for all $\sigma \in Gal(L/K)$, the Galois group of L over K.

Another problem we may consider is descent of modules. In other words, given an L-module N, what are the K-modules M such that $N \cong M_L$? This same question can be asked in other contexts and leads naturally to the notion of L-forms.

Definition 2.2. Let L be a commutative K-algebra, H a K-object. A K-object H' is an L-form of H if $L \otimes H \cong L \otimes H'$ as L-objects.

The word "object" above can be replaced with "associative algebra", "Lie algebra", "module", or any other category such that tensoring with L over K leaves us in the same category, except that the base ring changes to L.

2.2 Descent of coalgebras and Hopf algebras

The central part of this thesis is concerned with computing L-forms of coalgebras and Hopf algebras. But in order for these definitions to make sense in this context, we must show that given H a K-coalgebra (or K-Hopf algebra), then $L \otimes H$ is an L-coalgebra (resp. L-Hopf algebra).

Definition 2.3. Let K, L be as above, H a K-coalgebra. Then $L \otimes H$ is an

L-coalgebra with the following structure.

$$\begin{aligned} \Delta_{L\otimes H}(a\otimes h) &= \sum (a\otimes h_1)\otimes_L (1\otimes h_2) \\ \varepsilon_{L\otimes H}(a\otimes h) &= \varepsilon_H(h)a \end{aligned}$$

If H is a K-Hopf algebra, then $L\otimes H$ is an L-Hopf algebra with the antipode given by $S_{L\otimes H}(a\otimes h) = a\otimes S_H(h)$.

Note: $(L\otimes H)\otimes_L (L\otimes H)\cong L\otimes H\otimes H$ as L-vector spaces via the map given by $(a\otimes h)\otimes_L (b\otimes k)\mapsto ab\otimes h\otimes k$. We use this identification for $\Delta_{L\otimes H}$, so $\Delta_{L\otimes H}(a\otimes h) = \sum a\otimes h_1\otimes h_2$.

Example 2.4. [HP86] Let $K=\mathbb{R}$, and $L=\mathbb{C}$. Let $H=KA$, where A is an infinite cyclic group. Then $H' = \mathbb{R}[c,s : c^2+s^2=1, cs=sc]$ has a Hopf algebra structure

$$\Delta(c) = c\otimes c - s\otimes s, \quad \Delta(s) = s\otimes c + c\otimes s$$

$$\varepsilon(c) = 1, \quad \varepsilon(s) = 0$$

$$S(c) = c, \quad S(s) = -s$$

and it is called the trigonometric algebra. Let $a = 1\otimes c + i\otimes s = c+is \in L\otimes H'$. Direct computation gives us $a\in G(L\otimes H')$ with $a^{-1} = c-is$. Furthermore, we have $a+a^{-1} = 2c$, so $c\in L<a>$. Similarly, $a-a^{-1}=2is$, so $s\in L<a>$. Thus $L\otimes H' = L<a>\cong LA$, so H and H' are L-forms. Note that H and H' are not isomorphic over $\mathbb{Q}$, since $G(H)=A$ and $G(H')=\{1\}$.

We can extend the notion of forms to a slightly more general context.

Definition 2.5. Let $\mathcal{X}$ be a subcategory of the category of commutative K-algebras. Given a K-object H, we say that a K-object H' is a form of H with respect to $\mathcal{X}$ if H' is an L-form of H for some $L \in \mathcal{X}$

This generalizes the term "form" used in [HP86], where a form was defined to be an L-form for some L which is faithfully flat over K. In our terminology, this would be called a form with respect to faithfully flat commutative K-algebras.

Two questions naturally arise.

Question 2.6. Given K, L as above, and a K-Hopf algebra H, what are all the L-forms of H?

Question 2.7. Given a K-Hopf algebra H what are all the forms of H with respect to $\mathcal{X}$ for a given category $\mathcal{X}$ of commutative K-algebras?

The first question is explored by Pareigis in [Par89] where he found L-forms of group rings, which he called twisted group rings. He assumed the extension $K \subseteq L$ to be "F-Galois" for some group F and assumed L to be free as a K-module.

The second question is addressed by Haggenmüller and Pareigis in [HP86]. They restrict their attention to extensions $K \subseteq L$ of commutative rings which are faithfully flat. If G is a finitely generated group with finite automorphism group F, they found a correspondence between forms of KG with respect to faithfully flat commutative K-algebras and the set of "F-Galois extensions" of K. We will address this more general notion of Galois extension in the next chapter.

Chapter 3

Actions, Coactions, and Galois Extensions

In studying the descent theory of Hopf algebras and coalgebras, the nature of the field extension $K \subseteq L$ will be an important factor in computing L-forms. The extensions we deal with are generalizations of classical Galois extensions. Instead of having a field extension with a corresponding group, we will have an extension of associative algebras with a corresponding Hopf algebra. Hopf Galois extensions are helpful in descent theory, and are also of interest in their own right.

In this chapter, we begin by defining actions of Hopf algebras on associative algebras, which will be the analogue of automorphism actions of groups and derivation actions of Lie algebras. We then give a link between invariants of Hopf algebra actions and semisimplicity. After defining smash products and crossed products, we move to coactions. This will lead us to Hopf Galois extensions.

3.1 Hopf module algebras

In classical Galois extensions, the Galois group acts as automorphisms on the field extension. We must generalize this notion for Hopf algebras.

Definition 3.1. Let H be a Hopf algebra and let A be an associative algebra. We say that A is an H-module algebra if A is an H-module, and for each $a, b \in A$ and $h \in H$ we have

(i) $h \cdot (ab) = \sum (h_1 \cdot a)(h_2 \cdot b)$

(ii) $h \cdot 1_A = \varepsilon(h) 1_A$

If A and H merely satisfy (i) and (ii) (i.e. the map $h \otimes a \mapsto h \cdot a$ is not necessarily an H-module action), we say that H measures A.

Example 3.2. Let $H = KG$ be a group algebra, and suppose that A is an H-module algebra. For all $a, b \in A$, and $g \in G$, we have $g \cdot (ab) = (g \cdot a)(g \cdot b)$ and $g \cdot 1_A = 1_A$, so G acts as automorphisms on A.

Example 3.3. Let $H = U(\mathfrak{g})$ be a universal enveloping algebra, and suppose that A is an H-module algebra. For $x \in \mathfrak{g}$ and $a, b \in A$, we have $x \cdot (ab) = (x \cdot a)b + a(x \cdot b)$ and $x \cdot 1_A = 0$, so $\mathfrak{g}$ acts as derivations on A.

Example 3.4. Let H be a Hopf algebra. The left adjoint action of H on itself is given by $h \cdot h' = (ad_l h)(h') = \sum h_1 h' S(h_2)$. We have, for all $h, l, m \in H$,

$$\begin{aligned} h \cdot (lm) &= \sum h_1 lm S(h_2) \\ &= \sum \varepsilon(h_2) h_1 lm S(h_3), \quad \text{by counit diagram} \\ &= \sum h_1 l \varepsilon(h_2) m S(h_3) \\ &= \sum h_1 l S(h_2) h_3 m S(h_4), \quad \text{by definition of } S \\ &= \sum (h_1 \cdot l) h_2 m S(h_3) = \sum (h_1 \cdot l)(h_2 \cdot m) \end{aligned}$$

and so H is an H-module algebra.

Note that in the case $H = KG$, we get $(ad_l g)(a) = gag^{-1}$ for $g \in G$ and $a \in H$, and for H an enveloping algebra, we get $(ad_l x)(a) = xa - ax$ for $x \in \mathfrak{g}, a \in H$. Thus, the left adjoint action corrresponds to the classical adjoint actions for groups and Lie algebras.

Condition (ii) in Definition 3.1 says that, in some sense, H acts trivially on 1_A. This leads us to the notion of invariants.

Definition 3.5. (i) If M is an H-module, then the set of invariants of H in M is $M^H = \{m \in M : h \cdot m = \varepsilon(h)m, \text{ for all } h \in H\}$.

(ii) If we let H act on itself by left multiplication, then the invariants are called left integrals, and are denoted by $\int_H^l = \{t \in H : ht = \varepsilon(h)t \text{ for all } h \in H\}$.

The term invariant comes from group actions.

3.2 Integrals and semisimplicity

Integrals are an important tool in the study of Hopf algebras. Their importance is highlighted in the following generalization of Maschke's Theorem.

Theorem 3.6. *[LS69]* Let H be any finite dimensional Hopf algebra. Then H is semisimple if and only if $\varepsilon(\int_H^l) \neq 0$.

Proof. Assume H is semisimple. Then every left H-module is completely reducible. In particular, H is a completely reducible H-module under left multiplication. We have that $ker(\varepsilon)$ is an ideal of H, so there is some left ideal I such that $H = I \oplus ker(\varepsilon)$. Let $0 \neq t \in I$. Since $h - \varepsilon(h)1_H \in ker(\varepsilon)$ for each $h \in H$, we have $ht = (h - \varepsilon(h)1_H)t + \varepsilon(h)t \in I \oplus ker(\varepsilon)$. Since $I \oplus ker(\varepsilon)$ is direct, and $ht \in I$, we

must have $(h - \varepsilon(h)1_H)t = 0$. Then $ht = \varepsilon(h)t$, so $t \in \int_H^l$. But $t \notin ker(\varepsilon)$, and so $\varepsilon(\int_H^l) \neq 0$.

Now suppose $\varepsilon(\int_H^l) \neq 0$, and let M be any left H-module. It suffices to show that M is completely reducible, so we need only prove that for each submodule $U \leq M$ there is an H-projection $M \to U$. Let $t \in \int_H^l$ with $\varepsilon(t) = 1$. Let $\pi : M \to U$ be any K-linear projection, and define $\tilde{\pi} : M \to U$ by $\tilde{\pi}(m) = \sum t_1 \cdot \pi(S(t_2) \cdot m)$. If $u \in U$, then $\tilde{\pi}(u) = \sum t_1 \cdot (S(t_2) \cdot u) = \varepsilon(t)u = u$. It then suffices to show that $\tilde{\pi}$ is an H-module map. First, note that

$$\begin{aligned} \sum t_1 \otimes t_2 \otimes h &= \Delta(t) \otimes h = \sum \Delta((\varepsilon(h_1)t) \otimes h_2 \\ &= \sum \Delta(h_1 t) \otimes h_2 \\ &= \sum \Delta(h_1)\Delta(t) \otimes h_2 \\ &= \sum h_1 t_1 \otimes h_2 t_2 \otimes h_3 \end{aligned} \tag{3.1}$$

We have

$$\begin{aligned} \tilde{\pi}(h \cdot m) &= \sum t_1 \cdot \pi(S(t_2) \cdot h \cdot m) \\ &= \sum h_1 t_1 \cdot \pi(S(h_2 t_2)h_3 \cdot m), \text{ by Eqn. 3.1} \\ &= \sum h_1 t_1 \cdot \pi(S(t_2)S(h_2)h_3 \cdot m) \\ &= \sum h_1 t_1 \cdot \pi(S(t_2)\varepsilon(h_2) \cdot m) \\ &= h \cdot \sum t_1 \cdot \pi(S(t_2) \cdot m) = h \cdot \tilde{\pi}(m) \end{aligned}$$

Thus, $\tilde{\pi}$ is a projection, and so M is completely reducible. The theorem is proved.

□

Note that if G is a finite group, then $\int_{KG}^l = Kt$, where $t = \sum_{g \in G} g$, in which case $\varepsilon(t) = |G|$. Thus, when $H = KG$, then we get the classical version of Maschke's

Theorem. Also notice that $\int^l_{KG}$ is one-dimensional. This is true in general for finite dimensional Hopf algebras (see [Mon93, 2.1.3]).

An application of 3.6 to descent of Hopf algebras is the following.

Proposition 3.7. Let H be a finite dimensional K-Hopf algebra with $K \subseteq L$ an extension of fields. Then $\int^l_{L\otimes H} = L \otimes \int^l_H$. In particular, if H' is an L-form of H, then H' is semisimple if and only if H is semisimple.

Proof. By the above remarks, $\dim_L(\int^l_{L\otimes H}) = 1$ and $\dim_K(\int^l_H) = 1$. Thus, it suffices to show that $L \otimes \int^l_H \subseteq \int^l_{L\otimes H}$. Let $0 \neq t \in \int^l_H$. Then for all $a, b \in L$ and $h \in H$, we have $(a \otimes t)(b \otimes h) = ab \otimes th = \varepsilon(t)ab \otimes h = \varepsilon(a \otimes t)(b \otimes h)$. This gives us the first statement. For the second statement, notice that $\varepsilon_H(\int^l_H) \neq 0$ if and only if $\varepsilon_{L\otimes H}(L \otimes \int^l_H) \neq 0$. Thus, H is semisimple if and only if $L \otimes H$ is semisimple. By the same argument, H' is semisimple if and only if $L \otimes H'$ is semisimple. Since $L \otimes H \cong L \otimes H'$, the theorem follows. □

In [Chi92], Chin uses 3.6 to give an alternate proof of an old result of Hochschild [Hoc54]. This proof assumes the fact that if H is a finite dimensional semisimple Hopf algebra, then any subHopfalgebra over which H is a free module is also semisimple [Mon93, 2.2.2].

Theorem 3.8. *[Hoc54]* Let $\mathfrak{g}$ be a finite dimensional restricted Lie algebra of characteristic $p \neq 0$. Then $u(\mathfrak{g})$ is semisimple if and only if $\mathfrak{g}$ is abelian and $\mathfrak{g} = K\mathfrak{g}^p$.

Proof. Let E be the algebraic closure of K. It is easy to see that $u(E\otimes\mathfrak{g}) = E\otimes u(\mathfrak{g})$ and that $[E \otimes \mathfrak{g}]^p = E \otimes \mathfrak{g}$ if and only if $\mathfrak{g} = K\mathfrak{g}^p$. Also, $\int^l_{E\otimes u(\mathfrak{g})} = E \otimes \int^l_{u(\mathfrak{g})}$ by 3.7,

so $E \otimes u(\mathfrak{g})$ is semisimple if and only if $u(\mathfrak{g})$ is semisimple. Thus, we may assume that K is algebraically closed. In particular, $\mathfrak{g} = K\mathfrak{g}^p$ if and only if $\mathfrak{g} = \mathfrak{g}^p$.

First, assume that $\mathfrak{g}$ is abelian with $\mathfrak{g} = \mathfrak{g}^p$. Then $u(\mathfrak{g}) = u(\mathfrak{g})^p$, and so the p^{th} power map $^p : u(\mathfrak{g}) \to u(\mathfrak{g})$ is surjective. Since ^{p} is semilinear, and $u(\mathfrak{g})$ is finite dimensional, then ^{p} is injective as well. Thus, $u(\mathfrak{g})$ has no nonzero nilpotent elements, and so $u(\mathfrak{g})$ is semisimple.

Now suppose that $H = u(\mathfrak{g})$ is semisimple, and for the moment assume that $\mathfrak{g} =< x >= \text{span}\{x^{p^e} : e \geq 0\}$. By 3.6 there is some $t \in \int_H^l$ such that $\varepsilon(t) \neq 0$.

Claim: $x \in < x >^p$.

Proof. Suppose $\dim_K(< x >) = n$. We have $x^{p^i} \in \mathfrak{g}$, so there is some nontrivial polynomial f such that $f(x) = \sum_{i=0}^{n} a_i x^{p^i} = 0$. But $\dim_K(u(\mathfrak{g})) = p^n$ by the restricted PBW theorem, so f is actually the minimal polynomial for x. We can uniquely write $t = g(x) = \sum_{j=0}^{p^n-1} b_j x^j$. Since $xg(x) = xt = 0$, then $f(x)$ divides $xg(x)$. By comparison of degrees, $xg(x) = \alpha f(x)$, where $\alpha \in K$. Note that $\varepsilon(t) = \sum b_j \varepsilon(x^j) = b_0$, so $b_0 \neq 0$. But then also $a_0 \neq 0$ since $xg(x) = \alpha f(x)$. Thus,

$$x = -\sum_{i=1}^{n} (\frac{a_i}{a_0}) x^{p^i} \in < x >^p$$

□

In general, let $x \in \mathfrak{g}$. By the restricted PBW theorem, $u(\mathfrak{g})$ is a free module over $< x >$. Then the remarks before the statement of the theorem imply that $< x >$ is semisimple. By the claim, $x \in < x >^p \subseteq \mathfrak{g}^p$, and so $\mathfrak{g} = \mathfrak{g}^p$.

Since $a_0 \neq 0$ from the above, each $x \in \mathfrak{g}$ satisfies a separable polynomial. Hence, so does $ad(x)$. Thus, the action of $ad(x)$ on $\mathfrak{g}$ is completely reducible. Let

$y \in \mathfrak{g}$ be an eigenvector for $ad(x)$. Then $ad(x)$ acts on $u(< y >)$, a commutative ring. But $ad(x)$ annihilates $< y >^p \ni y$, so $[x, y] = 0$. Since $\mathfrak{g}$ is spanned by the eigenvectors of $ad(x)$, we conclude that $[x, \mathfrak{g}] = 0$. Thus, $\mathfrak{g}$ is abelian. □

Theorem 3.6 also makes determining the invariants under actions of semisimple Hopf algebras extremely nice. We get the following well-known result.

Lemma 3.9. If M is an H-module, and $0 \neq t \in \int_H^l$, then $t \cdot M \subseteq M^H$. If H is semisimple, then $t \cdot M = M^H$.

Proof. Let $m \in M$. For all $h \in H$, we have $h \cdot (t \cdot m) = ht \cdot m = \varepsilon(h)(t \cdot m)$, and so $t \cdot M \subseteq M^H$.

If H is semisimple, let $m \in M^H$. Since $\varepsilon(t) \neq 0$, we can assume, without loss of generality, that $\varepsilon(t) = 1$. We then have $t \cdot m = \varepsilon(t)m = m$, so $m \in t \cdot M$, and we are done. □

3.3 Smash products and crossed products

Hopf module actions on associative algebras give rise to two important constructions. The first is a generalization of skew group rings.

Definition 3.10. Let A be an H-module algebra. We can then construct the associative algebra $A\#H$, which is $A \otimes H$ as a set. The element $a \otimes h$ is written $a\#h$, and multiplication is given by

$$(a\#h)(b\#k) = \sum a(h_1 \cdot b)\#h_2k$$

We often write $a\#h = ah$.

It is easy to show that $A\#H$ is indeed an associative algebra with unit $1\#1$. Notice that in the case of $H = KG$, we have, for all $g, h \in G$, $(ag)(bh) = a(g \cdot b)gh$, which is the same as multiplication in in the skew group ring $A * G$. The next construction is a generalization of group crossed products.

Definition 3.11. Suppose H measures A (so A is not necessarily an H-module), and let $\sigma \in Hom_K(H \otimes H, A)$ be invertible under the convolution product (i.e. there exists $\tau \in Hom_K(H \otimes H, A)$ such that $\sigma * \tau = \tau * \sigma = u \circ \varepsilon$). Then we construct $A\#_\sigma H$. Again, $A\#_\sigma H = A \otimes H$ as a set. Multiplication is given by

$$(a\#h)(b\#k) = \sum a(h_1 \cdot b)\sigma(h_2, k_1)\#h_3k_2$$

For $H = KG$, we have $(ag)(bh) = a(g \cdot b)\sigma(g, h)gh$, which gives us a group crossed product. As in the case of group crossed products, we must have certain conditions on the map σ and the manner in which H measures A in order for $A\#_\sigma H$ to be an associative algebra.

Proposition 3.12. *[DT86, BCM86]* $A\#_\sigma H$ is an associative algebra with identity $1\#1$ if and only if for all $h, k, m \in H$ and $a \in A$,

(i) $h \cdot (k \cdot a) = \sum \sigma(h_1, k_1)(h_2k_2 \cdot a)\sigma^{-1}(h_3, k_3)$

(ii) $\sigma(h, 1) = \sigma(1, h) = \varepsilon(h)1_A$, and

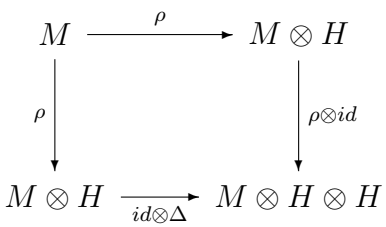
$$\sum [h_1 \cdot \sigma(k_1, m_1)]\sigma(h_2, k_2m_2) = \sum \sigma(h_1, k_1)\sigma(h_2, k_2, m)$$

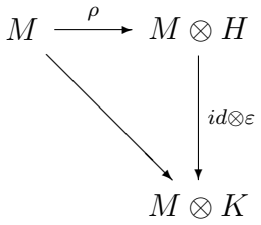
The proof of this is analogous to that of the proof of associativity for group crossed products. It is quite tedious, and so it will be omitted. Note that σ^{-1} is the inverse of σ under the convolution product (i.e. $\sigma^{-1} = \tau$ in 3.11).

3.4 Comodules and Hopf comodule algebras

One of the limitations in classical Galois theory is that it is difficult to define infinite dimensional Galois extensions. Although it is most natural to think of Galois extensions arising from module actions, we get the most generality when we think of them as arising from coactions. These coactions are duals of actions.

Definition 3.13. Let H be a coalgebra. A right H-comodule M is a vector space with a linear map $\rho : M \to M \otimes H$ which makes the following diagrams commute.





We have a summation notation for comodules similar to the Sweedler notation for coalgebras. We write $\rho(m) = \sum m_0 \otimes m_1$. Here the elements m_0 belong to M while the elements m_1 belong to H. Also $(\rho \otimes id) \circ \rho(m) = (id \otimes \Delta)\rho(m) = \sum m_0 \otimes m_1 \otimes m_2$ and so on.

Example 3.14. Let H be a coalgebra. Then H is an H-comodule with $\rho = \Delta$. We call this the regular corepresentation, since it is dual to the notion of the regular representation of an associative algebra.

We can get other examples from duals of module actions.

Proposition 3.15. *[Mon93, 1.6.4]*

(i) Let H be a coalgebra. If M is a right H-comodule, then M is a left H^*-module.

(ii) Let H be an associative algebra, M a left H-module. Then M is naturally a right H°-comodule algebra if and only if $H \cdot m$ is finite dimensional for all $m \in M$.

(iii) If H is a finite dimensional bialgebra, then any H-module M is an H^*-comodule and conversely. In particular, if $\{h_1, \cdots, h_n\}$ is a basis for H with dual basis $\{h_1^*, \cdots, h_n^*\}$ in H^*, then the comodule structure is given by $\rho(m) = \sum_i (h_i \cdot m) \otimes h_i^*$. The module structure is given by $h \cdot m = \sum m_1(h) m_0$.

Proof. For (i), let M be a right H-comodule, for H a coalgebra. For each $f \in H^*$ and $m \in M$, define $f \cdot m = \sum f(m_1) m_0$. To show that this makes M a left H^*-module, we have, for all $f, g \in H^*$ and $m \in M$,

$$\begin{aligned} f \cdot (g \cdot m) &= f \cdot \sum g(m_1) m_0 = \sum g(m_1)(f \cdot m_0) \\ &= \sum g(m_2) f(m_1) m_0 = \sum fg(m_1) m_0 \\ &= (fg) \cdot m \end{aligned}$$

For (ii), suppose that M is a left H-module, and let $h \in H$, $m \in M$. If $H \cdot m$ is finite dimensional with basis $\{m_1, \cdots, m_n\}$, then $h \cdot m = \sum f_i(h) m_i$ for some $f_i(h) \in K$. Clearly, $f_i \in H^*$. Moreover, $f_i \in H^\circ$. For consider the homomorphism $\phi : H \to End_K(H \cdot m)$ given by $\phi(h)(k \cdot m) = hk \cdot m$. Then $I = ker\phi$ is an ideal of finite codimension since $H \cdot m$ is finite dimensional. Furthermore, if $h \in I$, then $h \cdot m = 0$, and so $f_i(h) = 0$ for all i. Thus, $f_i(I) = 0$, and so $f_i \in H^\circ$. Now define $\rho(m) = \sum_i m_i \otimes f_i$. We show that this makes M a right H°-comodule. We have $\rho(m) = \sum_i m_i \otimes f_i$. Since $H \cdot m_i \subseteq H \cdot m$, then $\rho(m_i) = \sum_j m_j \otimes g_{ij}$ for some $g_{ij} \in H^\circ$.

Claim: $\Delta(f_i) = \sum_j g_{ji} \otimes f_j$ for all i.

Proof. For all $h, k \in H$ and $m \in M$, we have

$$\begin{aligned}\sum_i f_i(hk)m_i &= hk \cdot m = h \cdot (k \cdot m) \\ &= h \cdot \sum_j f_j(k)m_j = \sum_{i,j} f_j(k)g_{ji}(h)m_i\end{aligned}$$

Since the m_j are linearly independent, $\Delta(f_i)(h \otimes k) = f_i(hk) = (\sum_j g_{ji} \otimes f_j)(h \otimes k)$. This proves the claim. □

We then have

$$\begin{aligned}((\rho \otimes id) \circ \rho)(m) &= (\rho \otimes id)(\sum_i m_i \otimes f_i) = \sum_{i,j} m_j \otimes g_{ij} \otimes f_i \\ &= \sum_j m_j \otimes \Delta(f_j) = ((id \otimes \Delta) \circ \rho)(m)\end{aligned}$$

For the converse, let M be an H°-comodule algebra. If $h \in H$ and $m \in M$, then $h \cdot m = \sum m_1(h)m_0$, so $H \cdot m$ is contained in the span of $\{m_0\}$, a finite set. Thus, $H \cdot m$ is finite dimensional.

Finally, (iii) follows directly from the constructions in (i) and (ii). □

We can also dualize invariants.

Definition 3.16. If M is a right H-comodule, then the coinvariants of H in M are the elements of $M^{coH} = \{m \in M : \rho(m) = m \otimes 1\}$.

Proposition 3.17. *[Mon93, 1.7.1]*

(i) Let M be a right H-comodule with corresponding H^*-module structure. Then $M^{H^*} = M^{coH}$.

(ii) If M is a left H-module such that it is also a right H°-comodule, then $M^H = M^{coH^\circ}$.

Proof. For (i), we have that $m \in M^{coH}$ if and only if $\rho(m) = m \otimes 1$. But recall that for all $f \in H^*, f \cdot m = \sum f(m_1)m_0$, and so $m \in M^{coH}$ if and only if $f \cdot m = f(1)m = \varepsilon(f)m$. But this is equivalent to $m \in M^{H^*}$

For (ii), we have that $m \in M^H$ if and only if $h \cdot m = \varepsilon(h)m$ for all $h \in H$. But $h \cdot m = \sum m_1(h)m_0$, so this will be true if and only if $\rho(m) = m \otimes \varepsilon$. This is equivalent to $m \in M^{coH^\circ}$. □

Our last dualization is of H-module algebras.

Definition 3.18. An associative algebra A is a right H-comodule algebra if it is a right H-comodule, and we have, for all $a, b \in A$, $\rho(ab) = \rho(a)\rho(b)$, and $\rho(1) = 1 \otimes 1$.

Example 3.19. *Let H be a Hopf algebra. Since Δ is an algebra homomorphism, the regular corepresentation makes H an H-comodule algebra.*

Example 3.20. Let A be a KG-comodule algebra. For $a \in A$, suppose that $\rho(a) = \sum_{g \in G} a_g \otimes g$. Then we have

$$\sum_{g \in G} \rho(a_g) \otimes g = (\rho \otimes id) \circ \rho(a) = (id \otimes \Delta) \circ \rho(a) = \sum_{g \in G} a_g \otimes g \otimes g$$

Thus, $\rho(a_g) = a_g \otimes g$. We also have $a = \sum \varepsilon(a_1)a_0 = \sum_g a_g$. If we set $A_g = \{b \in A : \rho(b) = b \otimes g\}$, then $a \in \bigoplus_{g \in G} A_g$ and so $A = \bigoplus_{g \in G} A_g$. Since ρ is an algebra homomorphism, $A_g A_h \subseteq A_{gh}$ for all $g, h \in G$, and so KG-comodule algebras are G-graded K-algebras. Conversely, if $A = \bigoplus_{g \in G} A_g$ is a G-graded, associative algebra, then defining $\rho(a_g) = a_g \otimes g$ for each $a_g \in A_g$ and extending linearly makes A a KG-comodule algebra, so KG-comodule algebras are precisely G-graded associative K-algebras. Note that $A^{coKG} = A_1$.

As in 3.15, if H is finite dimensional, then A is a left H-module algebra if and only if it is a right H^*-comodule algebra.

3.5 Hopf Galois extensions

Now we are ready to define Hopf Galois extensions.

Definition 3.21. [KT81] Let H be a Hopf algebra, and suppose $B \subseteq A$ is an extension of right H-comodule algebras. This extension is right H-Galois if

(i) $B = A^{coH}$

(ii) The map $\beta : A \otimes_B A \to A \otimes_K H$ given by $\beta(a \otimes b) = (a \otimes 1)\rho(b) = \sum ab_0 \otimes b_1$ is bijective.

Proposition 3.22. Let H be a Hopf algebra. Then $K \subseteq H$ is an H-Galois extension.

Proof. We first show that $H^{coH} = K$. Suppose that $\Delta(h) = h \otimes 1$. Then $h = \sum \varepsilon(h_1)h_2 = \varepsilon(h)1_H \in K$.

From the comodule structure, we have that $\beta : H \otimes_K H \to H \otimes_K H$ is given by $\beta(h \otimes k) = \sum hk_1 \otimes k_2$. If, for $h, m \in H$, we define $\gamma(h \otimes m) = \sum hS(m_1) \otimes S(m_2)$,

then

$$\begin{aligned}(\gamma \circ \beta)(h \otimes m) &= \gamma(\sum hm_1 \otimes m_2) = \sum hm_1 S(m_2) \otimes m_3 \\ &= \sum h\varepsilon(m_1) \otimes m_2 = h \otimes (\sum \varepsilon(h_1)h_2) \\ &= h \otimes m \\ (\beta \circ \gamma)(h \otimes m) &= \beta(\sum hS(m_1) \otimes m_2) = \sum hS(m_1)m_2 \otimes m_3 \\ &= \sum h\varepsilon(m_1) \otimes m_2 = h \otimes (\sum \varepsilon(m_1)m_2) \\ &= h \otimes m\end{aligned}$$

Thus, β is bijective and so $K \subseteq H$ is H-Galois. □

Example 3.23. Suppose that $F \subseteq E$ is a classically Galois extension of fields, with Galois group $G = \{x_1, \cdots, x_n\}$ and $K \subseteq F$. Let $\{p_1, \cdots, p_n\} \subseteq (KG)^*$ be the dual basis to the $\{x_i\} \subseteq KG$. The action of G on E gives us a coaction $\rho(a) = \sum_i (x_i \cdot a) \otimes p_i$. From 3.17, we have $F = E^{KG} = E^{co(KG)^*}$. The Galois map is $\beta(a \otimes b) = \sum a(x_i \cdot b) \otimes p_i$. By comparisons of dimensions over K, we need only show that β is injective. Let $\sum_j a_j \otimes b_j \in ker(\beta)$, where $\{b_j\}$ is a basis of E over F. Then $\sum_j a_j(x_i \cdot b_j) = 0$ for each i. But Dedekind's lemma on the independence of automorphisms gives us that the matrix $[x_i \cdot b_j]$ is invertible, so $a_j = 0$ for all j. Thus, $ker(\beta) = 0$, and so β is injective. This makes β bijective, which makes $F \subseteq E$ $(KG)^*$-Galois.

Conversely, if $F \subseteq E$ is $(KG)^*$-Galois, then β being bijective means that

$$\begin{aligned}\dim_F(E)^2 &= \dim_F(E \otimes_K (KG)^*) = \dim_F(E \otimes_F [F \otimes_K (KG)^*]) \\ &= \dim_F(E) \cdot |G|\end{aligned}$$

Thus, $\dim_F(E) = |G|$, so $F = E^G \subseteq E$ is classically Galois.

Our next example considers KG-Galois extensions. Recall that KG-comodule algebras are simply G-graded algebras. KG-Galois extensions must satisfy an additional property.

Definition 3.24. A G-graded algebra A is said to be strongly graded if $A_gA_h = A_{gh}$ for all $g, h \in G$.

Lemma 3.25. Let A be a G-graded algebra. Then the following are equivalent.

(i) A is strongly graded.

(ii) $A_gA_{g^{-1}} = A_1$ for all $g \in G$.

(iii) For each $g \in G$, there exist $a_i^g \in A_g$ and $b_i^{g^{-1}} \in A_{g^{-1}}$ which satisfy $\sum_i a_i^g b_i^{g^{-1}} = 1$.

Proof. $(i) \Rightarrow (ii)$ is obvious. Since $1 \in A_1$, then $(ii) \Rightarrow (iii)$ is clear. It suffices to show that $(iii) \Rightarrow (i)$. Let $g, h \in G$. We know that $A_gA_h \subseteq A_{gh}$, so it suffices to show the other inclusion. Let $a \in A_{gh}$. Assuming (iii), there exist $a_i^g \in A_g, b_i^{g^{-1}} \in A_{g^{-1}}$ such that $\sum a_i^g b_i^{g^{-1}} = 1$. Then

$$a = 1 \cdot a = \sum a_i^g (b_i^{g^{-1}} a)$$

But $a_i^g \in A_g$ and $b_i^{g^{-1}} a \in A_{g^{-1}}A_{gh} \subseteq A_h$. Thus, $a \in A_gA_h$, which concludes the proof. □

Theorem 3.26. *[Ulb81]* Let A be a KG-comodule algebra. Then $A_1 \subseteq A$ is KG-Galois if and only if A is strongly graded.

Proof. Assume that $A_1 \subseteq A$ is KG-Galois. Then for each $g \in G$ there exist $a_i, b_i \in A$ such that $\beta(\sum_i a_i \otimes b_i) = 1 \otimes g$. Since A is G-graded, we can write

$a_i = \sum_{u\in G} a_i^u, b_i = \sum_{v\in G} b_i^v$ such that $a_i^u \in A_u, b_i^v \in A_v$. We then have $1 \otimes g = \beta(\sum_i a_i \otimes b_i) = \sum_{u,v\in G}(\sum_i a_i^u b_i^v) \otimes v$. This implies that $\sum_{u\in G}(\sum_i a_i^u b_i^g) = 1 \in A_1$. But we have $\sum_i a_i^u b_i^g \in A_{ug}$. Also, as u runs over G, so does ug. Since the sum of the A_g's is direct, we conclude that $\sum_i a_i^u b_i^g = 0$ unless $u = g^{-1}$. Thus, $\sum_i a_i^{g^{-1}} b_i^g = 1$, and A is strongly graded.

Now suppose that A is strongly graded. Then for each $g \in G$, there exist $a_i^{g^{-1}} \in A_{g^{-1}}$ and $b_i^g \in A_g$ such that $\sum_i a_i^{g^{-1}} b_i^g = 1$. We need only show that β is bijective. Define $\gamma : A \otimes_K KG \to A \otimes_{A_1} A$ by $\gamma(a \otimes g) = \sum_i a a_i^{g^{-1}} \otimes b_i^g$. We have

$$\begin{aligned}(\beta \circ \gamma)(a \otimes g) &= \beta(\sum_i a a_i^{g^{-1}} \otimes b_i^g) \\ &= \sum_i a a_i^{g^{-1}} b_i^g \otimes g = a \otimes g\end{aligned}$$

Finally, we need to show that for all $a, b \in A$, then $(\gamma \circ \beta)(a \otimes b) = a \otimes b$. Since $A = \sum_{g\in G} A_g$, then it suffices to show this for $b \in A_g$ for each $g \in G$. We have

$$\begin{aligned}(\gamma \circ \beta)(a \otimes b) &= \gamma(ab \otimes g) \\ &= \sum_i aba_i^{g^{-1}} \otimes b_i^g = \sum a \otimes ba_i^{g^{-1}} b_i^g, \text{ since } ba_i^{g^{-1}} \in A_1 \\ &= a \otimes b\end{aligned}$$

which completes the proof. □

One interpretation of this result is that a K-algebra must closely resemble KG in order to be a KG-Galois extension. In this case, the group G is replaced by the set of subspaces A_g which form a group under setwise multiplication. This group is in fact isomorphic to the group G.

3.6 Finite dimensional Hopf Galois extensions

If H is finite dimensional, then H^*-Galois extensions are a bit easier to understand since they can be defined in terms of actions of H on A (see 3.15). The following results come from [KT81] and [Ulb82].

Theorem 3.27. Let H be a finite dimensional Hopf algebra, A a left H-module algebra. The following are equivalent:

(i) $A^H \subseteq A$ is right H^*-Galois.

(ii) The map $\pi : A\#H \to End(A_{A^H})$ given by $\pi(a\#h)(b) = a(h\cdot b)$ is an algebra isomorphism, and A is a finitely generated projective right A^H-module.

(iii) If $0 \neq t \in \int_H^l$, then the map $[\ ,\ ] : A \otimes_{A^H} A \to A\#H$ given by $[a,b] = atb$ is surjective.

In particular, if our extension is a finite extension of fields $K \subseteq L$, then (ii) becomes $\pi : L\#H \to End_K(L)$ is bijective. In particular, $|L : K| = \dim_K(H)$.

We get stronger results when $A = D$ is a division algebra.

Theorem 3.28. *[CFM90]* Let D be a left H-module algebra, where D is a division algebra, and H is a finite dimensional Hopf algebra. The following are equivalent:

(i) $D^H \subseteq D$ is H^*-Galois.

(ii) $[D : D^H]_r = \dim_K H$ or $[D : D^H]_l = \dim_K H$

(iii) $D\#H$ is simple.

(iii) $D \cong D^H\#_\sigma H^*$, for some 2-cocycle σ.

Example 3.29. Let $K \subseteq L$ be a totally inseparable finite field extension of exponent ≤ 1 (i.e. $a^p \in K$ for all $a \in L$). Since $Der_K(L)$ is finite dimensional over L,

there exists a finite p-basis of L over K [Jac64, p. 182]. In other words, there is a finite set $\{a_1, \cdots, a_n\}$ such that $\{a_1^{m_1} \cdots a_n^{m_n} : 0 \leq m_i < p\}$ is a basis of L over K. For each i, we can define a derivation δ_i such that $\delta_i(a_j) = \delta_{i,j}$. We can think of δ_i as the i^{th} partial derivative with respect to the a_j's. It is easy to see that $\mathfrak{g} = \text{span}\{\delta_i : 1 \leq i \leq n\}$ is a restricted Lie algebra, and in fact $Der_K(L) = L\mathfrak{g} \cong L \otimes \mathfrak{g}$. In particular, $Der_K(L)$ is an abelian restricted Lie algebra. Clearly, $K = L^{u(\mathfrak{g})}$. We also have $\dim_K(u(\mathfrak{g})) = p^n = [L : K]$, and so $K \subseteq L$ is a $u(\mathfrak{g})^*$-Galois extension by 3.28(ii).

In fact, more can be said.

Theorem 3.30. Suppose that $K \subseteq L$ is a finite field extension of characteristic $p > 0$. Then $K \subseteq L$ is a $u(\mathfrak{g}')^*$-Galois extension if and only if $K \subseteq L$ is totally inseparable of exponent ≤ 1, and $\mathfrak{g}'$ is an L-form of $\mathfrak{g}$, where $\mathfrak{g}$ is as in Example 3.29.

Proof. Suppose that $K \subseteq L$ is a $u(\mathfrak{g}')^*$-Galois extension, where $\mathfrak{g}'$ is some restricted Lie algebra. Let $a \in L$ and $x \in \mathfrak{g}'$. Since x acts as a derivation on L, we have $x \cdot a^p = pa^{p-1}(x \cdot a) = 0$. Thus, $a^p \in K$ and so $K \subseteq L$ is totally inseparable of exponent ≤ 1. Define $f : L \otimes \mathfrak{g} \to End_K(L)$ by $f(a \otimes x)(b) = a(x \cdot b)$. Since f is just π without the $\#$, it follows from 3.27(ii) that f is injective. But one can check that $imf \subseteq Der_K(L)$ and that f is in fact a Lie homomorphism. Furthermore,

$$\dim_K(u(\mathfrak{g}')) = [L : K] = \dim_K(u(\mathfrak{g}))$$

and so $\dim_K(\mathfrak{g}') = \dim_K(\mathfrak{g})$. Thus, f is actually a Lie isomorphism, which implies $\mathfrak{g}$ and $\mathfrak{g}'$ are L-forms.

Conversely, suppose that $K \subseteq L$ is totally inseparable of exponent ≤ 1, and that $\phi : L \otimes \mathfrak{g}' \to L \otimes \mathfrak{g} \cong Der_K(L)$ is an L-isomorphism. We define an action of $\mathfrak{g}'$ on L

via $x \cdot a = \phi(x) \cdot a$. This extends to an action of $L \otimes \mathfrak{g}'$ on L. By 3.28, (ii), we need only show that $K = L^{\mathfrak{g}'}$. But this follows from $K = L^{\mathfrak{g}} = L^{L \otimes \mathfrak{g}} = L^{L \otimes \mathfrak{g}'} = L^{\mathfrak{g}'}$. $\square$

If we look ahead to 6.1, we see that $u(\mathfrak{g})$ and $u(\mathfrak{g}')$ are L-forms, and that all the L-forms of $u(\mathfrak{g})$ are obtained from L-forms of $\mathfrak{g}$. Thus, 3.30 says that if $K \subseteq L$ is $u(\mathfrak{g})^*$-Galois, it is also H^*-Galois for all forms H of $u(\mathfrak{g})$.

Question 3.31. If H is a finite dimensional Hopf algebra, and $K \subseteq L$ is a finite H^*-Galois field extension, is it also $(H')^*$-Galois for all L-forms H' of H?

A result from [GP87] puts this question in doubt. Specifically, it is shown that if $K \subseteq L$ is a separable H^*-Galois field extension, then H is an $\tilde{L}$-form of a group algebra, where $\tilde{L}$ is the normal closure of L. But the next example shows that a separable H^*-Galois field extension does not have to be classically Galois.

Example 3.32. Let $K = \mathbb{Q}, L = K(\omega)$, where ω is a real fourth root of 2. Then $K \subseteq L$ is H^*-Galois, where $H = K < c, s : c^2 + s^2 = 1, cs = sc = 0 >$. We have $g = c + is \in G(\tilde{L} \otimes H)$, and $o(g) = 4$. Thus, H is an $\tilde{L}$-form of KG, where G is cyclic of order 4. But notice that $g \notin L \otimes H$. In fact $G(L \otimes H) = \{1, g^2\}$. Thus, H is not an L-form of a group algebra.

Note that in the restricted enveloping algebra $u(\mathfrak{g})$ of Example 3.29 we have $\delta_i^p = 0$ for all i, and so $K\mathfrak{g}^p = 0$. Thus, by 3.8, $u(\mathfrak{g})$ is not semisimple. Since $u(\mathfrak{g}')$ is a form of $u(\mathfrak{g})$, then 3.7 implies that $u(\mathfrak{g}')$ is not semisimple either.

It should be noted that there are more equivalent conditions in 3.27 and 3.28 (see [Mon93, 8.3.3,8.3.7]).

Chapter 4

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

In this chapter, we look at faithfully flat $U(\mathfrak{g})$-Galois extensions, where $\mathfrak{g}$ is an arbitrary Lie algebra. What seems to be the case, as with KG-Galois extensions, is that such extensions bear a fairly close resemblance to $U(\mathfrak{g})$. This is highlighted in Theorem 4.14.

4.1 $U(\mathfrak{g})$-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, $n(i) \neq 0$ for only finitely many $i \in I$. These functions can be thought of as ordered m-tuple $(\mathbf{n}(i_1), \cdots, \mathbf{n}(i_m))$, 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 $\{x^{\mathbf{n}} : \mathbf{n} \text{ has finite support}\}$. This gives us a shorthand for such a 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 $\binom{\mathbf{n}}{\mathbf{m}} = \prod_{i \in I} \binom{n(i)}{m(i)}$.

Lemma 4.1. *[Mon93, 5.5]* For all $\mathbf{n} : I \to \mathbb{Z}_{\geq 0}$ with finite support,

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

Proof. Recall that $\Delta(x_i) = x_i \otimes 1 + 1 \otimes x_i$ for all $i \in I$, and that Δ is an algebra homomorphism. The result then follows by induction on the degree of the monomial $x^{\mathbf{n}}$. The details are left to the masochistic reader. □

We now consider right $U(\mathfrak{g})$-comodules. We approach such comodules in much the same way as we approached KG-comodules. We take a $U(\mathfrak{g})$-comodule M, and an arbitrary element $m \in M$. Then we run this element through the commuting diagrams for comodules. So let ρ denote the coaction on M. Then $\rho(m) = m' \otimes 1 + \sum_{\mathbf{n}>0} m_{\mathbf{n}} \otimes x^{\mathbf{n}}$, where only finitely many of the $m_{\mathbf{n}} \in M$ are nonzero. We have $m = \sum \varepsilon(m_1) m_0 = m'$, since $\varepsilon(x^{\mathbf{n}}) = 0$ for all $\mathbf{n} > 0$ (this follows from the fact that $\varepsilon(x_i) = 0$ for all $i \in I$ and ε is an algebra homomorphism). Thus, $\rho(m) = m \otimes 1 + \sum_{\mathbf{n}>0} m_{\mathbf{n}} \otimes x^{\mathbf{n}}$. Since $(\rho \otimes id) \circ \rho = (id \otimes \Delta) \circ \rho$, then

$$\rho(m) \otimes 1 + \sum_{\mathbf{n}>0} \rho(m_{\mathbf{n}}) \otimes x^{\mathbf{n}} = m \otimes 1 \otimes 1 + \sum_{\mathbf{n}>0} \sum_{\mathbf{j} \leq \mathbf{n}} \binom{\mathbf{n}}{\mathbf{j}} m_{\mathbf{n}} \otimes x^{\mathbf{n}-\mathbf{j}} \otimes x^{\mathbf{j}} \quad (4.1)$$

For each fixed $\mathbf{j}$, we get $\rho(m_{\mathbf{j}}) = \sum_{\mathbf{n} \geq \mathbf{j}} \binom{\mathbf{n}}{\mathbf{j}} m_{\mathbf{n}} \otimes x^{\mathbf{n}-\mathbf{j}}$. If we adjust the indices, this gives us

$$\rho(m_{\mathbf{n}}) = \sum_{\mathbf{k} \geq 0} \binom{\mathbf{n}+\mathbf{k}}{\mathbf{n}} m_{\mathbf{n}+\mathbf{k}} \otimes x^{\mathbf{k}} \quad (4.2)$$

This equality is also true for $\mathbf{n} = \mathbf{0}$ if we let $m_{\mathbf{0}} = m$.

Definition 4.2. Define $M_n = \{m \in M : \rho(m) \in M \otimes U_n\}$, where $\{U_n\}$ is the standard filtration of $U(\mathfrak{g})$.

Lemma 4.3. $M_n = \{m \in M : \rho(m) - m \otimes 1 \in \bigoplus_{i=1}^{n} M_i \otimes \mathfrak{g}^{n-i}\}$

Note: By $\mathfrak{g}^i$, we mean the linear span of the monomials in elements of $\mathfrak{g}$ of degree i.

Proof. Let $m \in M_n$, and write $\rho(m) = m \otimes 1 + \sum_{\mathbf{i}>0} m_{\mathbf{i}} \otimes x^{\mathbf{i}}$ as in (4.1). It suffices to show that for each $\mathbf{i} > 0$, we have $m_{\mathbf{i}} \in M_{n-|\mathbf{i}|}$, since we will then have $m_{\mathbf{i}} \otimes x^{\mathbf{i}} \in M_{n-|\mathbf{i}|} \otimes \mathfrak{g}^{|\mathbf{i}|}$.

Since $m \in M_n$, we have $m_{\mathbf{i}} = 0$ whenever $|\mathbf{i}| > n$. By (4.2), we have that $\rho(m_{\mathbf{i}}) = \sum_{\mathbf{k}\geq 0} \binom{\mathbf{i}+\mathbf{k}}{\mathbf{i}} m_{\mathbf{i}+\mathbf{k}} \otimes x^{\mathbf{k}}$. As mentioned above, we must have $m_{\mathbf{i}+\mathbf{k}} = 0$ whenever $n < |\mathbf{i}+\mathbf{k}| = |\mathbf{i}| + |\mathbf{k}|$. It then follows that $\rho(m_{\mathbf{i}}) \in M \otimes U_{n-|\mathbf{i}|}$, and so $m_{\mathbf{i}} \in M_{n-|\mathbf{i}|}$. □

Lemma 4.4. (i) $M = \bigcup_{n=0}^{\infty} M_n$

(ii) If M is a $U(\mathfrak{g})$-comodule algebra, then $M_i M_j \subseteq M_{i+j}$

(iii) $\rho(M_n) \subseteq \bigoplus_{i=0}^{n} M_{n-i} \otimes U_i$

Proof. (i) is trivial. For (ii), 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

$$\rho(ab) \quad = \quad \rho(a)\rho(b) \in (M \otimes U_i)(M \otimes U_j) \subseteq M \otimes U_{i+j}$$

Thus, $ab \in M_{i+j}$. Finally, (iii) is a direct result of 4.3. □

This makes $\{M_n\}$ a comodule filtration of M. Notice that $M_0 = M^{coU(\mathfrak{g})}$.

4.2 Faithfully flat H-Galois extensions

Recall the following definition.

Definition 4.5. Let $B \subseteq A$ be an extension of rings.

(i) The extension is left flat if, whenever $0 \to M \to M' \to M'' \to 0$ is an exact sequence of left B-modules, then $0 \to A \otimes M \to A \otimes M' \to A \otimes M'' \to 0$ is also exact.

(ii) The extension is left faithfully flat if it is flat, and if, for all nonzero left B-modules M, we have $A \otimes M \neq 0$.

The definitions are analogous for right flat and right faithfully flat.

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.

Let A be a $U(\mathfrak{g})$-comodule algebra. We now consider when $A^{coU(\mathfrak{g})} \subseteq A$ is a faithfully flat $U(\mathfrak{g})$-Galois extension. This was studied extensively in [Bel]. Before we get to Bell's result, a few preliminaries are in order.

Definition 4.6. (i) A total integral is a right H-comodule morphism $\phi : H \to A$ such that $\phi(1) = 1$.

(ii) The extension $A^{coH} \subseteq A$ is H-cleft if there exists a total integral which is convolution invertible.

H-cleft extensions are important because of the following result.

Theorem 4.7. *[Mon93, 7.2.2]* The extension $A^{coH} \subseteq A$ is H-cleft if and only if $A \cong A^{coH} \#_\sigma H$ for some 2-cocycle σ, and some crossed product action of H on

A^{coH}.

In particular, any H-cleft extension is a free A^{coH}-extension, since $A^{coH}\#_\sigma H \cong A^{coH} \otimes H$ as left A^{coH}-modules. This leads us to Bell's result.

Proposition 4.8. *[Bel, 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 $\phi : H \to A$.

Recall from the remarks following 1.21 that $U(\mathfrak{g})$ is a connected Hopf algebra, so 4.8 can be applied to faithfully flat $U(\mathfrak{g})$-Galois extensions. Thus, such extensions are free extensions over $A^{coU(\mathfrak{g})} = A_0$. The main goal of this section is to construct a "PBW-like" free A_0-basis for A when A_0 is commutative.

Lemma 4.9. Let A be a $U(\mathfrak{g})$-comodule algebra. If A_0 is commutative, then A_1 is a Lie subalgebra of A, and $A_0 \triangleleft A_1$.

Proof. Let $a, b \in A_1$. By 4.3, $\rho(a) = a\otimes 1 + \sum_i a_i \otimes x_i$ and $\rho(b) = b\otimes 1 + \sum_i b_i \otimes x_i$, where $a_i, b_i \in A_0$. Since ρ is an algebra homomorphism, a quick calculation gives us

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

Thus, $\rho([a,b]) \in A \otimes U_1$, 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, $A_0 \lhd A_1$. □

Lemma 4.10. The map $c : A_1 \to A_0 \otimes \mathfrak{g}$ 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.

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 $\rho(b) - b \otimes 1 \in A_0 \otimes \mathfrak{g}$ 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 map $\bar{c} : A_1/A_0 \to A_0 \otimes \mathfrak{g}$ given by $a + A_0 \mapsto \rho(a) - a \otimes 1$. Recall the Galois map $\beta : A \otimes_{A^{coH}} A \to A \otimes_K H$ given by $\beta(a \otimes b) = (a \otimes 1)\rho(b)$.

Lemma 4.11. Let A be a $U(\mathfrak{g})$-comodule algebra. Let $\{a_i\}$ be a generating set for A_1 as an A_0-module, with $\rho(a_i) = a_i \otimes 1 + \sum_j a_{ij} \otimes x_j$. Suppose that the matrix $[a_{ij}]$ has a row finite left inverse $[b_{ij}]$ with entries in A. Then $\beta(A \otimes A_1^n) = A \otimes_K U_n$. In particular, β is onto.

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 (see [Pas91, p. 89]). This will not be an issue in this section, since $A_0 \subseteq A$ will be assumed to be faithfully flat. 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, for all i, that $1 \otimes x_i \in \beta(A \otimes A_1)$. 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 not an infinite sum, and so $\alpha \in A \otimes A_1$. We have

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

and so $\beta(A \otimes A_1) = A \otimes_K U_1$. Now we proceed by induction. Assume that

$\beta(A \otimes A_1^n) = A \otimes_K U_n$. Then

$$\begin{aligned}
\beta(A \otimes A_1^{n+1}) &= (A \otimes 1)\rho(A_1^{n+1}) = (A \otimes 1)\rho(A_1^n)\rho(A_1) \\
&= \beta(A \otimes A_1^n)\rho(A_1) = (A \otimes_K U_n)\rho(A_1) \\
&= (A \otimes_K U_n)(A \otimes 1)\rho(A_1) = (A \otimes_K U_n)\beta(A \otimes A_1) \\
&= (A \otimes_K U_n)(A \otimes U_1) = A \otimes U_{n+1}
\end{aligned}$$

which completes the proof. □

For the main result, we need the following corollary of 4.8.

Proposition 4.12. *[Bel, 1.5]* $A_0 \subseteq A$ is faithfully flat $U(\mathfrak{g})$-Galois if and only if there is a linear map $\lambda : \mathfrak{g} \to A$ such that $\rho(\lambda(x)) = \lambda(x) \otimes 1 + 1 \otimes x$.

Proof. Suppose that the extension is faithfully flat Galois. By 4.8, there is a total integral $\phi : U(\mathfrak{g}) \to A$. Let $\lambda = \phi|_{\mathfrak{g}}$. Recall that Δ is the coaction for $U(\mathfrak{g})$. We then have, for all $x \in \mathfrak{g}$,

$$\begin{aligned}
\rho(\lambda(x)) &= (\rho \circ \phi)(x) = (\phi \otimes id) \circ \Delta(x) \\
&= \phi(x) \otimes 1 + \phi(1) \otimes x = \lambda(x) \otimes 1 + 1 \otimes x
\end{aligned}$$

Now suppose that we have a map $\lambda : \mathfrak{g} \to A$ such that $\rho(\lambda(x)) = \lambda(x) \otimes 1 + 1 \otimes x$. We extend λ to a total integral $\phi : U(\mathfrak{g}) \to A$. Define $\phi(x^{\mathbf{n}}) = \prod_{i \in I} \lambda(x_i)^{\mathbf{n}(i)}$. We then have

$$\begin{aligned}
(\rho \circ \phi)(x^{\mathbf{n}}) &= \rho(\prod_{i \in I} \lambda(x_i)^{\mathbf{n}(i)}) = \prod_{i \in I} \rho(\lambda(x_i))^{\mathbf{n}(i)} \\
&= \prod_{i \in I} (\lambda(x_i) \otimes 1 + 1 \otimes x_i)^{\mathbf{n}(i)} = \prod_{i \in I} (\sum_{k_i = 0}^{\mathbf{n}(i)} \binom{\mathbf{n}(i)}{k_i} \lambda(x_i)^{k_i} \otimes x_i^{\mathbf{n}(i) - k_i})
\end{aligned}$$

But if we define $\mathbf{k}(i) = k_i$ and multiply everything out, we get

$$\begin{aligned}(\rho \circ \phi)(x^{\mathbf{n}}) &= \sum_{\mathbf{k} \leq \mathbf{n}} \left(\prod_{i \in I} \binom{\mathbf{n}(i)}{\mathbf{k}(i)} \lambda(x_i)^{\mathbf{k}(i)} \otimes x_i^{(\mathbf{n}-\mathbf{k})(i)}\right) = \sum_{\mathbf{k} \leq \mathbf{n}} \binom{\mathbf{n}}{\mathbf{k}} \phi(x^{\mathbf{k}}) \otimes x^{\mathbf{n}-\mathbf{k}} \\ &= ((\phi \otimes id) \circ \Delta)(x^{\mathbf{n}})\end{aligned}$$

Thus, ϕ is a comodule map. From its definition, we get that $\phi(1) = 1$, and so ϕ is a total integral. Thus, $A^{coH} \subseteq A$ is faithfully flat Galois. □

Corollary 4.13. *$A_0 \subseteq A$ 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 4.10, so it suffices to prove that it is surjective. Let $x \in \mathfrak{g}$. By 4.12, 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 4.12 □

Notice for $x \in \mathfrak{g}$ that $\lambda(x)$ plays the same role in the comodule structure of A as x plays in $U(\mathfrak{g})$ (where the coaction is given by Δ). Thus, faithfully flat $U(\mathfrak{g})$-Galois extensions bear a close resemblance to $U(\mathfrak{g})$ itself.

We can take this analogy even further. In $A = U(\mathfrak{g})$, we have $A_0 = K$ and $A_1 = \mathfrak{g} \oplus K$. Thus, we have $\mathfrak{g} \cong A_1/A_0$. In fact, for all $x \in \mathfrak{g}$, we have $x + A_0 = \{a \in A : \rho(a) = a \otimes 1 + 1 \otimes x\}$. Similarly, if $A_0 \subseteq A$ is faithfully flat $U(\mathfrak{g})$-Galois, then it is easy to check that $a_x + A_0 = \{a \in A : \rho(a) = a \otimes 1 + 1 \otimes x\}$. This leads us to the main theorem.

Theorem 4.14. Let $A_0 \subseteq A$ be a faithfully flat $U(\mathfrak{g})$-Galois extension, with $\{x_i : i \in I\}$ an ordered basis for $\mathfrak{g}$. Then

(i) If we define $a_i = \lambda(x_i)$ as in 4.12, then $\{a_i + A_0\}$ is a free A_0-basis for A_1/A_0. In particular, $\{1, a_i\}$ is a free basis for A_1.

(ii) The set consisting of 1 and ordered monomials in $\{a_i\}$ is a free A_0-basis for the submodule of A it generates.

(iii) $A =< A_1 >$.

(iv) If A_1 is a Lie subalgebra of A, then the set consisting of 1 and ordered monomials in $\{a_i\}$ form a free A_0-basis for A. In particular, this holds when A_0 is commutative.

Proof. For (i), suppose that $\sum_i b_i(a_i + A_0) = 0$ for some $b_i \in A_0$. It follows that $\sum_i b_i a_i \in A_0$, 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 $\sum_{\vec{i}} c_{\vec{i}}\, a_{i_1} \cdots a_{i_n} = 0$, $c_{\mathbf{i}} \in A_0$, where $i_1 \leq \cdots \leq i_n$ and n is the maximum degree of a monomial with a

nonzero coefficient. In order to allow for monomials of different lengths, we define $a_0 = 1$, so $i_j \in I \cup \{0\}$. We have

$$\begin{aligned} 0 &= \rho(\sum_{\vec{i}} c_{\vec{i}}\, a_{i_1} \cdots a_{i_n}) \\ &= \sum_{\vec{i}} (c_{\vec{i}} \otimes 1)(a_{i_1} \otimes 1 + 1 \otimes x_{i_1}) \cdots (a_{i_n} \otimes 1 + 1 \otimes x_{i_n}) \\ &= \sum_{|\vec{i}|=n} c_{\vec{i}} \otimes x_{i_1} \cdots x_{i_n} + s \end{aligned}$$

where $s \in A \otimes U_{n-1}$. By the PBW theorem, $c_{\vec{i}} = 0$ for all $|\vec{i}| = n$. This contradicts our assumption of the existence of a nontrivial dependence relation, and gives us (ii).

For (iii), first note that $A \otimes_{A_0} A_1^n$ and $A \otimes_{A_0} A_n$ are naturally embedded in $A \otimes A$ since the extension is faithfully flat. We have $A = \bigcup_n A_n$, so it suffices to show that $A_1^n = A_n$ for all n. We first show that $A \otimes_{A_0} A_1^n = A \otimes_{A_0} A_n$. The matrix $\{a_{ij}\}$ from 4.11 is the identity matrix by 4.12, and is thus left invertible with row finite left inverse. Also, $\{a_i\}$ generates A_1 as an A_0-module by (i), and so 4.11 implies that $\beta(A \otimes_{A_0} A_1^n) = A \otimes_K U_n$, which gives us

$$\beta(A \otimes_{A_0} A_1^n) \subseteq \beta(A \otimes_{A_0} A_n) \subseteq A \otimes_K U_n = \beta(A \otimes_{A_0} A_1^n)$$

Thus, $\beta(A \otimes_{A_0} A_n) = \beta(A \otimes_{A_0} A_1^n)$, and by the bijectivity of β, we get $A \otimes_{A_0} A_n = A \otimes_{A_0} A_1^n$.

Now consider the exact sequence $0 \to A_1^n \to A_n \to A_n/A_1^n \to 0$. By flatness, we get the exact sequence $0 \to A \otimes_{A_0} A_1^n \to A \otimes_{A_0} A_n \to A \otimes_{A_0} (A_n/A_1^n) \to 0$. But the second map in this sequence is the inclusion map, which is onto since $A \otimes A_1^n = A \otimes A_n$, so $A \otimes_{A_0} (A_n/A_1^n) = 0$. By faithful flatness, we get $A_n/A_1^n = 0$, and so $A_n = A_1^n$.

For (iv), we know by (i) that the a_i form an A_0 basis for A_1. Then (iii) implies that A is spanned by monomials in the a_i. But A_1 is a Lie subalgebra of A, and so the monomials in a_i are spanned by the ordered monomials in the a_i. Finally, by (ii), the ordered monomials are independent over A_0, so they form a free basis. $\square$

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

Corollary 4.13 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 4.13 to arbitrary $U(\mathfrak{g})$-Galois extensions. It appears that the correct map to consider in this more general context is $id \otimes \bar{c} : A \otimes_{A_0} (A_1/A_0) \to A \otimes_{A_0} (A_0 \otimes_K \mathfrak{g}) \cong A \otimes_K \mathfrak{g}$.

Proposition 4.15. (i) If $id \otimes \bar{c}$ is onto, then so is β.

(ii) If $A_0 \subseteq A$ is $U(\mathfrak{g})$-Galois and $\beta^{-1}(A \otimes U_1) = A \otimes A_1$, 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 4.11. 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. We also have

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

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 4.11.

Now we consider (ii). Since $\beta^{-1}(A \otimes U_1) = A \otimes A_1$ and the a_i's generate A_1 over A_0, 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 $\gamma : A\otimes_K \mathfrak{g} \to A\otimes_{A_0}(A_1/A_0)$ 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

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

But we also have that

$$\begin{aligned} a\otimes b &= \beta^{-1}\circ\beta(a\otimes b) = \beta^{-1}(ab\otimes 1 + \sum_i ab_i\otimes x_i) \\ &= ab\otimes 1 + \sum_{i,j} ab_ib_{ij}\otimes a_j \end{aligned} \tag{4.3}$$

If we let $\pi : A_1 \to A_1/A_0$ be the canonical homomorphism, then, applying $id\otimes\pi$ to both sides of (4.3) gives us $a\otimes(b+A_0) = \sum_{i,j} ab_ib_{ij}\otimes(a_j+A_0)$, 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 A-modules M and N are 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 necessarily true that β^{-1} is of degree zero. But if, in addition, $id \otimes \bar{c}$ is onto, then 4.15 implies that $\beta|_{A \otimes A_n}$ is onto $A \otimes U_n$. 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 4.15 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 4.16. 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 complicated.

Chapter 5

Descent theory of coalgebras and Hopf algebras

In this chapter, we present two theorems on the descent theory of coalgebras and Hopf algebras. The first theorem classifies all forms of the grouplike coalgebras with respect to fields, and the second allows us to compute L-forms when $K \subseteq L$ is a finite dimensional Hopf Galois extension.

5.1 Forms of the Grouplike Coalgebra

We now consider the descent theory for coalgebras. In this section, we classify all coalgebra forms of grouplike coalgebras with respect to fields according to the structure of their simple subcoalgebras. Recall that a coalgebra is grouplike if it is spanned by grouplike elements (i.e. elements $g \neq 0$ such that $\Delta(g) = g \otimes g$). Suppose that $C = KG$ is a grouplike coalgebra, where $G = G(C)$. It is clear that if we have a field extension $K \subseteq L$, then $L \otimes C \cong LG$. Thus, it is our goal to characterize the coalgebras H such that $L \otimes H \cong LG$. We will denote the algebraic closure of K by $\bar{K}$.

To get started, we first consider the coalgebra structure of duals of finite extension fields. Let $K \subseteq L$ be a finite field extension. Then L^* is a K-coalgebra by 1.12(ii). Let $\{\alpha_1, \cdots, \alpha_n\}$ be a basis for L over K with $\alpha_j\alpha_k = \sum_l c_{jkl}\alpha_l$, where $c_{jkl} \in K$, and let $\{\alpha_1^*, \cdots, \alpha_n^*\}$ be the dual basis in L^*. For the comultiplicative structure, let $1 \leq r, s, l \leq n$. We have

$$\Delta(\alpha_l^*)(\alpha_r \otimes \alpha_s) = \alpha_l^*(\alpha_r\alpha_s) = \sum_t c_{rst}\alpha_l^*(\alpha_t) = c_{rsl} = (\sum_{j,k} c_{jkl}\alpha_j^* \otimes \alpha_k^*)(\alpha_r \otimes \alpha_s)$$

so $\Delta(\alpha_l^*) = \sum_{j,k} c_{jkl}\alpha_j^* \otimes \alpha_k^*$.

For the counit, let $q_i \in K$ such that $\sum_i q_i\alpha_i = 1$. Then for each j, we get $\varepsilon(\alpha_j^*) = \alpha_j^*(1) = \sum_i q_i\alpha_i^*(\alpha_j) = q_j$. Thus, the $\varepsilon(\alpha_i^*)$ are the unique elements of K such that $\sum_i \varepsilon(\alpha_i^*)\alpha_i = 1$. This completes our description of the coalgebra structure of L^*.

Lemma 5.1. Let $K \subseteq L$ be a finite field extension. A coalgebra D is a morphic image of L^* if and only if $D \cong E^*$ for some field E such that $K \subseteq E \subseteq L$. In particular, any morphic image of L^* is a simple coalgebra.

Proof. Suppose that $\phi : L^* \to D$ is an onto morphism of coalgebras. We can define $\phi^* : D^* \to L^{**} \cong L$ by $\phi^*(f) = f \circ \phi$. It is then easy to show that ϕ^* is an algebra monomorphism. Let E be the image of D^* in L. Then E is a finite dimensional K-subalgebra of L, so E is a field. Furthermore, since $E \cong D^*$ as fields, then $D \cong E^*$ as coalgebras.

Conversely, if $D \cong E^*$ for E a field contained in L, then consider the inclusion map $i : E \to L$. Since i is a field monomorphism, $i^* : L^* \to E^* \cong D$ is an coalgebra morphism. Since i is injective, one can show that i^* is surjective.

Finally, let D be a morphic image of L^*. By the above, $K \subseteq D^*$ is a finite field extension. Thus, D^* is a finite dimensional simple K-algebra. By [Mon93, 5.1.4], D is a simple coalgebra. □

Some other facts will be important in helping us find forms of grouplike coalgebras. It is clear that any form H of KG must be cocommutative, since $H \subseteq L \otimes H$ and $L \otimes H$ is cocommutative. Also, if $L \otimes H$ is grouplike, it must be pointed. The following can be found in [Mon93, 5.6]. It says that pointedness will always occur for a cocommutative coalgebra as long as we carefully choose our extension field.

Proposition 5.2. If H is a cocommutative K-coalgebra, and K is algebraically closed, then H is pointed.

Thus, if we take $L = \bar{K}$, then $L \otimes H$ is pointed when H is a cocommutative coalgebra.

Proof. Let D be a simple subcoalgebra of H. Then D^* is finite dimensional by the remarks following 1.19. It is also a commutative, simple K-algebra, and so $K \subseteq D^*$ is a finite field extension. Since K is algebraically closed, $D^* \cong K$, and so $\dim_K(D) = 1$. Thus, H is pointed. □

We will need a few technical results which will help us reduce the problem of finding forms of KG to the case where L is algebraic over K. The first lemma tells us that if we have a grouplike element $g = \sum \alpha_i \otimes h_i$, then in some sense the α_i and h_i are dual to each other.

Lemma 5.3. Let $g = \sum_i \alpha_i \otimes h_i \in G(L \otimes H)$.

(i) Suppose the α_i are linearly independent, and that $\alpha_i\alpha_j = \sum_k c_{ijk}\alpha_k$ for all i, j. Then $\Delta(h_k) = \sum_{i,j} c_{ijk} h_i \otimes h_j$ for all k. In particular, $D = \text{span}\{h_i\}$ is a finite dimensional subcoalgebra of H.

(ii) If we have the hypotheses in (i), and if the α_i are algebraic over K, then D is simple.

(iii) If the nonzero h_i are linearly independent (write them as $h_1, \cdots, h_n$), and if $\Delta(h_k) = \sum_{i,j=1}^n d_{ijk} h_i \otimes h_j$, where $d_{ijk} \in K$, then $\alpha_i\alpha_j = \sum_{k=1}^n d_{ijk}\alpha_k$ for all $1 \leq i, j \leq n$. In particular, $K[\alpha_1, \cdots, \alpha_n]$ is finite dimensional, and therefore is a finite field extension.

(iv) Conversely, if we have $\{\alpha'_1, \cdots, \alpha'_n\} \in L$ and $\{h'_1, \cdots, h'_n\}$ such that $\alpha'_i\alpha'_j = \sum_k c_{ijk}\alpha'_k$ and $\Delta(h'_k) = \sum_{i,j} c_{ijk} h'_i \otimes h'_j$ with $c_{ijk} \in K$, then $\sum_i \alpha'_i \otimes h'_i \in G(L \otimes H)$.

Proof. In general, we have

$$\begin{aligned} \sum_k \alpha_k \otimes \Delta(h_k) &= \Delta(g) = g \otimes g \\ &= \sum_{i,j} \alpha_i\alpha_j \otimes h_i \otimes h_j \end{aligned} \tag{5.1}$$

If $\alpha_i\alpha_j = \sum_k c_{ijk}\alpha_k$, and the α_i are linearly independent, then $\sum_{i,j} \alpha_i\alpha_j \otimes h_i \otimes h_j = \sum_{i,j,k} c_{ijk}\alpha_k \otimes h_i \otimes h_j$, and therefore $\Delta(h_k) = \sum_{i,j} c_{ijk} h_i \otimes h_j$ by (5.1). This gives us (i).

If the α_i are algebraic over K, then let $\{\alpha_1, \cdots, \alpha_n\}$ be the α_i such that $h_i \neq 0$. Since $\varepsilon(g) = 1$, then $\sum_{i=1}^n \varepsilon(h_i)\alpha_i = 1$. This and (i) imply that the h_i satisfy the same coalgebra relations as E^*, where $E = K(\alpha_1, \cdots, \alpha_n)$. Note that since the α_i are algebraic, E is finite dimensional, and so E^* is indeed a coalgebra. Thus, D is a morphic image of E^*, and so is simple by 5.1. This gives us (ii)

If $\Delta(h_k) = \sum_{i,j} d_{ijk} h_i \otimes h_j$ and the h_i are linearly independent, then we get $\sum_k \alpha_k \otimes \Delta(h_k) = \sum_{i,j,k} d_{ijk} \alpha_k \otimes h_i \otimes h_j$. Therefore, $\alpha_i \alpha_j = \sum_k d_{ijk} \alpha_k$ by (5.1) and so we have (iii).

Finally, (iv) follows from a computation almost identical to those above. I will leave this to the fastidious reader. □

Lemma 5.4. Let $K \subseteq L$ be any field extension. For each $g \in G(L \otimes H)$, there is a simple subcoalgebra $H_g \subseteq H$ such that $g \in \bar{K} \otimes H_g$

Proof. Let $g \in G(L \otimes H)$, and let $\{\alpha_i\}$ be a basis for L over K with $\alpha_i \alpha_j = \sum_k c_{ijk} \alpha_k$, where $c_{ijk} \in K$. Then $g = \sum_i \alpha_i \otimes h_i$ for some $h_i \in H$. Let $D = \text{span}\{h_i\}$. Then $g \in L \otimes D$. Also, D is a finite dimensional coalgebra by 5.3(i).

Now let $\{v_1, \cdots, v_n\}$ be a basis for D. Then $\Delta(v_k) = \sum_{i,j=1}^{n} d_{ijk} v_i \otimes v_j$ for some $d_{ijk} \in K$. Write $g = \sum_i \beta_i \otimes v_i$ with $\beta_i \in L$. By 5.3(iii), $K[\beta_1, \cdots, \beta_n]$ is a finite field extension, and so each β_i is algebraic over K. Thus, $g \in \bar{K} \otimes D$.

But now we can write $g = \sum_i \gamma_i \otimes w_i$, where the γ_i are linearly independent in $\bar{K}$, $\gamma_i \gamma_j = \sum_k e_{ijk} \gamma_k$ with $e_{ijk} \in K$, and $w_i \in D$. By 5.3(ii), we have that $H_g = \text{span}\{w_i\}$ is a simple coalgebra. Since $g \in \bar{K} \otimes H_g$, the proof is complete. □

As a direct consequence, we get

Corollary 5.5. If a coalgebra H is an L-form of KG, then it is a $\bar{K}$-form of KG.

Proof. If $L \otimes H \cong LG$, then $G \subseteq \bar{K} \otimes H$, by 5.4. Thus, $\bar{K}G \subseteq \bar{K} \otimes H$. Since G spans $L \otimes H$ over L, G spans $\bar{K} \otimes H$ over $\bar{K}$. Thus, $\bar{K} \otimes H = \bar{K}G$. □

We now mention a fact from field theory.

Proposition 5.6. *[McC66, Thm. 20]* Let $K \subseteq E$ be a finite field extension, with L a normal extension of K containing E. Let n be the degree of separability of E over K. Then there are exactly n distinct K-isomorphisms of E onto subfields of L.

This leads us to the main theorem.

Theorem 5.7. Let H be a K-coalgebra, and suppose $K \subseteq L$ is an extension of fields. Then the following are equivalent.

(i) $L \otimes H$ is a grouplike L-coalgebra.

(ii) H is cocommutative, cosemisimple with separable coradical, and L contains the normal closure of D^* for each simple subcoalgebra $D \subseteq H$.

A coalgebra is said to have separable coradical if, for each simple subcoalgebra D, we have that D^* is a separable K-algebra. If D is cocommutative, this will make D^* a separable field extension.

Also notice that the above implies that H is a form of KG with respect to fields if and only if H is cosemisimple with separable coradical.

Proof. Suppose that $L \otimes H$ is a grouplike coalgebra, and write $G = G(L \otimes H)$. By 5.5, we can assume that L is algebraic over K. By 5.4, each $g \in G$ is contained in $L \otimes H_g$ for some simple subcoalgebra $H_g \subseteq H$. We then have

$$L \otimes H = LG \subseteq \sum_{g \in G} L \otimes H_g = L \otimes (\sum_{g \in G} H_g) \subseteq L \otimes H_0$$

and so $H = H_0$. This implies that H is cosemisimple.

We now take care of the case where H is simple. By 5.1, H^* is isomorphic to some finite field extension of K in $\bar{K}$. Let $E \cong H^*$ be any such field, and

let $\{\alpha_1, \cdots, \alpha_n\}$ be a basis for E over K, $\{h_1, \cdots, h_n\}$ a basis for H such that $\alpha_i\alpha_j = \sum_k c_{ijk}\alpha_k$ and $\Delta(h_l) = \sum_{j,k} c_{jkl}h_j \otimes h_k$. Then $g = \sum_i \alpha_i \otimes h_i$ is a grouplike element of $E \otimes H$ by 5.3(iv). Since $L \otimes H$ is grouplike, $g \in L \otimes H$. Also, the h_i are linearly independent, so $\alpha_i \in L$ for all i. Thus, $E \subseteq L$, and so L contains every isomorphic copy of H^* in $\bar{K}$. This implies that L contains the normal closure of H^* in $\bar{K}$.

Now let E and $\{h_i\}$ be as above, and suppose that $g' = \sum_j \alpha'_j \otimes h_j$ is any grouplike element in H. By 5.3(iii), we have $\alpha'_i\alpha'_j = \sum_k c_{ijk}\alpha'_k$. But then the map $\alpha_j \mapsto \alpha'_j$ extends to an isomorphism $E \to K(\alpha'_1, \cdots, \alpha'_n)$. Thus, we get a distinct grouplike element of $L \otimes H$ for every distinct isomorphism from E onto subfields of L. Another way of saying this is that the number of grouplikes is the same as the number of distinct isomorphisms of E onto subfields of L. Since L contains the normal closure of H^*, 5.6 implies that the number of distinct grouplike elements is the same as the degree of separability of H^* over K. Since $L \otimes H$ has $\dim_K(H) = \dim_K(H^*)$ distinct grouplikes, the degree of separability of H^* over K is $\dim_K(H^*)$. Therefore, H^* is separable over K.

For the general case, since H is cosemisimple, we can write $H = \oplus_i H_i$, where the H_i are the distinct simple subcoalgebras of H. Also recall from 5.3(ii) that each grouplike element of $L \otimes H$ sits in some $L \otimes H_i$. Thus, $G(L \otimes H) = \cup_i G(L \otimes H_i)$. Since $L \otimes H$ is spanned by grouplike elements, it follows that each $L \otimes H_i$ is spanned by grouplike elements. By the simple case, each H_i^* is separable, and L contains the normal closure of H_i^*. Thus, if $L \otimes H$ is grouplike, then H is cosemisimple, each simple subcoalgebra D is the dual of a finite separable extension field of K, and L contains the normal closure of each such D.

Conversely, suppose that H is cosemisimple, each simple subcoalgebra is the dual of a separable finite extension field, and L contains the normal closure of D^* for each simple subcoalgebra $D \subseteq H$. Since H is cosemisimple, $H = \oplus_i H_i$, where each H_i is simple. It suffices to show that each H_i is spanned by grouplike elements, and so, without loss of generality, H is simple. By the remarks following 1.19, H is finite-dimensional.

Since H^* is separable, and L contains the normal closure of H^*, there are $\dim_K(H^*)$ distinct isomorphisms of H^* onto subfields of L. By 5.3(iv), we get a distinct grouplike element of $L \otimes H$ for each such isomorphism, and so there are $\dim_K(H^*) = \dim_K(H)$ distinct grouplike elements of $L \otimes H$. Therefore, $L \otimes H$ is a grouplike coalgebra, and the proof is complete. □

If H is a cocommutative cosemisimple Hopf algebra, then so is $L \otimes H$, where $K \subseteq L$ is any field extension (see [Nic94, 1.2]). Since $L \otimes H$ is also pointed when L is algebraically closed, any cocommutative cosemisimple Hopf algebra is a form of a group algebra. By 5.7, H must have a separable coradical. This restricts the coalgebra structure of such Hopf algebras. We can also say something about semisimplicity in the finite dimensional case.

Corollary 5.8. Let H be a finite dimensional cocommutative cosemisimple Hopf algebra. Then H is semisimple if and only if $char(K) = 0$ or $char(K)$ does not divide $dim_K(H)$.

Proof. Let $L = \bar{K}$. By the above remarks, $L \otimes H \cong LG$, where G is a group. By 3.7, H is semisimple if and only if KG is. By Maschke's theorem, this occurs if and only if either $char(K) = 0$ or $char(K)$ does not divide $|G| = dim_K(H)$. □

Theorem 5.7 tells us which field L is the smallest one necessary in order for H to be an L-form of a grouplike coalgebra. For each simple subcoalgebra D of H, we need the normal closure of D^* to be included in L. Thus, if $H = \oplus H_i$, where the H_i are simple, and we let L_i be the normal closure of H_i^*, then $L = \prod_i L_i$ is the smallest field necessary for $L \otimes H$ to be grouplike. This leads us to another result.

Corollary 5.9. Let H be an L-form of KG, where $K \subseteq L$ is either a totally inseparable or a purely transcendental extension. Then $H \cong KG$.

Proof. Suppose $K \subseteq L$ is totally inseparable. By the above remarks, any grouplike element in $L \otimes H$ is contained in $E \otimes H$ where E is the separable closure of K in L. Since $K \subseteq L$ is totally inseparable, we have $E = K$. Thus, $H \cong K \otimes H$ is spanned by grouplike elements, and so $H \cong KG$.

If $K \subseteq L$ is purely inseparable, then any grouplike element is contained in $E \otimes H$, where E is the algebraic closure of K in L by 5.4. But $E = K$ since $K \subseteq L$ is purely transcendental. The result follows as before. □

Corollary 5.10. Let H be a cocommutative coalgebra, and suppose that $K \subseteq L$ is such that $L \otimes H$ is pointed. Let $\{H_n\}_{n=0}^{\infty}$ be the coradical filtration of H.

(i) $[L \otimes H]_0 \subseteq L \otimes H_0$.

(ii) Equality holds if and only if H has separable coradical.

(iii) If H has separable coradical, then $L \otimes H_n \subseteq [L \otimes H]_n$ for all n.

Proof. For (i), since $L \otimes H$ is pointed, $[L \otimes H]_0$ is spanned by grouplikes. Since each grouplike $g \in L \otimes H_g \subseteq L \otimes H_0$, where H_g is as in 5.4, we have $[L \otimes H]_0 \subseteq L \otimes H_0$.

For (ii), we first note that H_0 is a cosemisimple, cocommutative coalgebra. If H does not have separable coradical, then, by 5.7, $L \otimes H_0$ is not grouplike. Since $[L \otimes H]_0$ is grouplike, equality cannot hold.

If H does have separable coradical, then 5.7 tells us that $L \otimes H_0$ is grouplike, and thus cosemisimple. Then $L \otimes H_0 \subseteq [L \otimes H]_0$, and we're done by (i).

For (iii), we proceed by induction on n. The $n = 0$ case is (ii). Assume that $L \otimes H_n \subseteq [L \otimes H]_n$. We then look at $L \otimes H_{n+1}$. We have

$$\begin{aligned}
\Delta(L \otimes H_{n+1}) &= L \otimes_K \Delta(H_{n+1}) \\
&\subseteq L \otimes_K (H \otimes_K H_n + H_0 \otimes_K H) \\
&\subseteq (L \otimes H) \otimes_L (L \otimes H_n) + (L \otimes H_0) \otimes_L (L \otimes H) \\
&\subseteq (L \otimes H) \otimes_L (L \otimes H)_n + (L \otimes H)_0 \otimes_L (L \otimes H)
\end{aligned}$$

and so $L \otimes H_{n+1} \subseteq [L \otimes H]_{n+1}$, which completes the proof. □

For the next corollary, we need the following.

Theorem 5.11. *[Mon93, 2.3.1]* Suppose that H is a finite dimensional commutative semisimple Hopf algebra. Then there exists a group G and a separable extension field E of K such that $E \otimes H \cong (EG)^*$ as Hopf algebras.

Proof. By Wedderburn's Theorem, $H \cong \oplus E_i$, where each E_i is an extension field of K. Since H is finite dimensional and semisimple, it is separable by [Mon93, 2.2.2], so each E_i is separable. Let E be a separable field containing all the E_i. We have

$$E \otimes H \cong E \otimes (\oplus E_i) \cong \oplus (E \otimes E_i) \cong E^n$$

where $n = dim_K H$, since E and the E_i's are separable. Now let $\{p_i\}$ be a basis in $E \otimes H$ of orthogonal idempotents, and let $G = \{g_i\}$ be a dual basis in $[E \otimes H]^*$. It is clear that the g_i are algebra maps, so by 1.14 they are grouplike elements. But then $[E \otimes H]^*$ is generated by grouplikes, so $[E \otimes H]^* \cong EG$, and thus $E \otimes H \cong (EG)^*$. □

Lemma 5.12. Let C be a subspace of a K-Hopf algebra (or coalgebra) H, and let $K \subseteq L$ be a field extension.

(i) C is a subcoalgebra of H if and only if $L \otimes C$ is a subcoalgebra of $L \otimes H$.

(ii) C is a subHopfalgebra of H if and only if $L \otimes C$ is a subHopfalgebra of $L \otimes H$.

Proof. Suppose $L \otimes C$ is a subcoalgebra, and let $c \in C$. Then $1 \otimes c \in L \otimes C$, so $1 \otimes \Delta(c) = \Delta(1 \otimes c) \in L \otimes C \otimes C$. But then

$$1 \otimes \Delta(c) \in (K \otimes H \otimes H) \cap (L \otimes C \otimes C) = K \otimes (C \otimes C)$$

so $\Delta(c) \in C \otimes C$, and C is a subcoalgebra. The other assertions follow similarly. □

Corollary 5.13. Let H be a cocommutative Hopf algebra. If H has separable coradical, then H_0 is a subHopfalgebra. Conversely, if H_0 is a finite dimensional Hopf algebra, then H has separable coradical.

Proof. First suppose that H has separable coradical, and let $L = \bar{K}$. Then $L \otimes H$ is a pointed coalgebra, and so $(L \otimes H)_0$ is a group algebra. But this implies that $(L \otimes H)_0$ is a Hopf algebra. By 5.10, $L \otimes H_0 = (L \otimes H)_0$. Since $L \otimes H_0$ is a Hopf algebra, 5.12 implies that H_0 is a Hopf algebra.

If H_0 is a finite dimensional cocommutative Hopf algebra, then H_0^* is a finite dimensional commutative semisimple Hopf algebra. By 5.11, $L \otimes H_0^* \cong (LG)^*$ as Hopf algebras. But $L \otimes H_0^* \cong (L \otimes H_0)^*$, so $L \otimes H_0 \cong LG$. This implies, by 5.7, that H_0 has separable coradical, and thus so does H. □

We get one final corollary.

Corollary 5.14. Suppose that K is a field of characteristic zero, and that H is a K-Hopf algebra of prime dimension. Then H is semisimple and cosemisimple with separable coradical.

Proof. Again, let $L = \bar{K}$. By [Zhu94], since $L \otimes H$ is a Hopf algebra over an algebraically closed field of characteristic zero, it is a group algebra. By 5.7, H is cosemisimple with separable coradical. If we apply the above to H^*, then H^* is cosemisimple, and so H is semisimple. □

5.2 Hopf Algebra Forms

In this section, we consider the descent theory of Hopf algebras. Here, we fix the field extension $K \subseteq L$ and search for the L-forms of a given Hopf algebra H.

More specifically, suppose that H and W are K-Hopf algebras, where W is finite dimensional and semisimple. Also, let $K \subseteq L$ be a right W^*-Galois extension of fields, and suppose that $L \otimes H$ is a W-module algebra, where the action restricted to L is the Galois action. This, along with some other mild restrictions on the action of W, will guarantee that $[L \otimes H]^W$ is an L-form of H. Furthermore, all L-forms of H can be obtained in this way.

Henceforth, $L \otimes H$ will be written as $L \circ H$ and $l \otimes h$ will be written as lh for convenience, where $l \in L$, and $h \in H$.

We start with a lemma on W-module algebras.

Lemma 5.15. Let W act on a field extension $K \subseteq L$ such that $K = L^W$, and suppose that A is an associative K-algebra such that $L \circ A$ is a W-module algebra. Then

(i) Any subset of $[L \circ A]^W$ that is linearly independent over K is linearly independent over L.

(ii) $[L \circ A]^W \otimes_K [L \circ A]^W$ can be embedded in $[L \circ A] \otimes_L [L \circ A]$ as K-algebras by the map $\alpha \otimes_K \beta \mapsto \alpha \otimes_L \beta$.

Proof. Let $\{\alpha_i\}$ be a K-linearly independent set in $[L \circ A]^W$. Suppose that $\sum_{i=1}^{n} l_i \alpha_i = 0$ is a nontrivial dependence relation of minimal length with $l_i \in L$. Without loss of generality, we can assume that $l_1 = 1$, and so $\alpha_1 + \sum_{i>1} l_i \alpha_i = 0$. Let $w \in W$. By acting on the dependence relation by w and using the fact that $\alpha_i \in [L \circ A]^W$, we get $\varepsilon(w)\alpha_1 + \sum_{i>1}(w \cdot l_i)\alpha_i = 0$. If we multiply the original dependence relation by $\varepsilon(w)$, we get $\varepsilon(w)\alpha_1 + \sum_{i>1} \varepsilon(w)\alpha_i = 0$. But if we subtract these equations, we get

$$\sum_{i>0}(w \cdot l_i - \varepsilon(w) l_i)\alpha_i = 0$$

Since this is a shorter dependence relation, we must have $w \cdot l_i - \varepsilon(w) l_i = 0$ for each i, so $w \cdot l_i = \varepsilon(w) l_i$. Thus, $l_i \in L^W = K$. Since the α_i are K-linearly independent, we have a contradiction. This gives us (i), and (ii) follows immediately. □

This lemma allows us to view elements of $[L \circ A]^W \otimes [L \circ A]^W$ as belonging to $[L \circ A] \otimes_L [L \circ A]$. We can thus move elements of L through the tensor product

when looking at invariants. This will be important in our calculations for the main theorem.

Before proving the main theorem, we need to say something about the action of W on L.

Lemma 5.16. Let W be a finite dimensional K-Hopf algebra, and let $K \subseteq L$ be a W^*-Galois extension. Let $0 \neq t \in \int_W^l$ with $\Delta(t) = \sum_j t_j \otimes t'_j$, where $\{t'_j\}$ is a basis for W. Let $a_i, b_i \in L$ such that $\sum_i a_i t b_i = 1$ in $L\#H$, as in 3.27(iii). Then

(i) For all $w \in W$, we have $\sum_i (w \cdot a_i) t b_i = w$ in $L\#W$.

(ii) For all j, k we have $\sum_i (t'_j \cdot a_i)(t_k \cdot b_i) = \delta_{j,k}$. In particular, if we have $t'_1 = 1$, then $\sum_i a_i (t_j \cdot b_i) = \delta_{j,1}$.

Proof. Let $w \in W$. Then we have, by the definition of multiplication in $L\#W$,

$$w = w(\sum_i a_i t b_i) = \sum_i (w_1 \cdot a_i) w_2 t b_i = \sum_i (w_1 \cdot a_i)\varepsilon(w_2) t b_i = \sum_i (w \cdot a_i) t b_i$$

This gives us (i). For (ii), we have from (i) and the expression for $\Delta(t)$ that for all j,

$$t'_j = \sum_i (t'_j \cdot a_i) t b_i = \sum_{i,k} (t'_j \cdot a_i)(t_k \cdot b_i) t'_k$$

Since $\{t'_k\}$ is a basis, we have $\sum_i (t'_j \cdot a_i)(t_k \cdot b_i) = \delta_{j,k}$. This gives us (ii). □

As mentioned before, only certain actions of W on $L \circ H$ will be considered. We are looking for Hopf algebra forms, so we must take into consideration the algebraic and coalgebraic structure of $L \circ H$, as well as the structure imposed by the antipode. By making $L \circ H$ a W-module algebra, we are choosing actions that "respect" the algebraic structure of $L \circ H$. It thus makes sense to choose actions that respect the rest of the Hopf algebra structure as well.

Definition 5.17. Let W be a Hopf algebra, and suppose H is a W-module algebra that is also a Hopf algebra. We say that the action on H is a commuting action if it commutes with the comultiplication, counit, and antipode of H (i.e. $\Delta(w \cdot h) = w \cdot \Delta(h)$, etc).

We are now ready for the main result.

Theorem 5.18. Suppose that $K \subseteq L$ is a W^*-Galois field extension for W a finite dimensional, semisimple Hopf algebra. Let H be any K-Hopf algebra, and suppose that we have a commuting action of W on the Hopf algebra $L \circ H$ such that the action restricted to L is the Galois action. Then

(i) $H' = [L \circ H]^W$ is a K-Hopf algebra, with the K-Hopf algebra structure inherited from the L-Hopf algebra $L \circ H$.

(ii) $L \otimes H' \cong L \otimes H$ as L-Hopf algebras, via the isomorphism $l \otimes \alpha \mapsto l\alpha$.

(iii) If F is any Hopf algebra L-form of H, then there is some commuting action of W on $L \circ H$ such that $F \cong [L \circ H]^W$

Proof. Let $0 \neq t \in \int_W^l$, and let $a_i, b_i \in L$ such that $\sum_i a_i t b_i = 1$ in $L\#W$. Also write $\Delta(t) = \sum_j t_j \otimes t'_j$, where $\{t'_j\}$ is a basis for W with $t'_1 = 1$. Since W is semisimple, $[L \circ H]^W = t \cdot (L \circ H)$, and $L^W = t \cdot L$ by 3.9.

For (i), it suffices to show that $\Delta(H') \subseteq H' \otimes H'$, $\varepsilon(H') \subseteq K$, and $S(H') \subseteq H'$. Also, by above remarks, $[L \circ H]^W$ is spanned over K by elements of the form $t \cdot lh$, where $l \in L$, and $h \in H$.

Since the t'_j form a basis for W, we can write $(id \otimes \Delta) \circ \Delta(t) = \sum_{j,k} t_j \otimes t'_j \otimes t''_{jk}$ for some $t''_{jk} \in W$. We then have

$$\Delta(t \cdot lh) = t \cdot \Delta(lh) = \sum t \cdot (lh_1 \otimes h_2) = \sum_{j,k} (t_j \cdot l)(t'_j \cdot h_1) \otimes (t''_{jk} \cdot h_2)$$

In addition, we know that $\sum_i (t \cdot [b_i h_1]) \otimes (t \cdot [l a_i h_2]) \in H' \otimes H'$. If we identify this element with its image in $[L \circ H] \otimes_L [L \circ H]$ (which we can do by 5.15), then

$$\begin{aligned}
\sum_i (t \cdot [b_i h_1]) \otimes (t \cdot [l a_i h_2]) &= \sum_{i,j,k,m} (t_j \cdot b_i)(t'_j \cdot h_1) \otimes (t_m \cdot l)(t'_m \cdot a_i)(t''_{mk} \cdot h_2) \\
&= \sum_{i,j,k,m} (t'_m \cdot a_i)(t_j \cdot b_i)(t_m \cdot l)(t'_j \cdot h_1) \otimes (t''_{mk} \cdot h_2) \\
&= \sum_{j,k,m} \delta_{m,j}(t_m \cdot l)(t'_j \cdot h_1) \otimes (t''_{mk} \cdot h_2), \quad \text{by 5.16} \\
&= \sum_{j,k} (t_j \cdot l)(t'_j \cdot h_1) \otimes (t''_{jk} \cdot h_2)
\end{aligned}$$

Thus, $\Delta(t \cdot lh) = \sum_i (t \cdot [b_i h_1]) \otimes (t \cdot [l a_i h_2]) \in H' \otimes H'$, and so $\Delta(H') \subseteq H' \otimes H'$.

For the counit, we have $\varepsilon(t \cdot lh) = t \cdot \varepsilon(lh)$, so $\varepsilon(t \cdot lh) \in L^W = K$. Thus, $\varepsilon(H') \subseteq K$. Similarly, for the antipode we have $S(t \cdot lh) = t \cdot S(lh) \in [L \circ H]^W$ and we have proved (i).

For (ii), one can check that the given map is an L-Hopf algebra morphism. It then suffices to show bijectivity. For surjectivity, let $h \in H$. Then, using 5.16(ii),

$$\sum_i a_i \otimes (t \cdot b_i h) \mapsto \sum_i a_i (t \cdot b_i h) = \sum_{i,j} a_i (t_j \cdot b_i)(t'_j \cdot h) = \sum_j \delta_{j,1}(t'_j \cdot h) = h$$

Since $L \circ H$ is spanned over L by H, the map is surjective. For injectivity, suppose $\sum_i l_i \otimes \alpha_i$ is in the kernel of the map, where $\{\alpha_i\}$ is a K-linearly independent subset of H'. Then $\sum_i l_i \alpha_i = 0$. By 5.15(i), $l_i = 0$ for all i, and so the kernel is zero.

For (iii), suppose that F is an L-form of H, so $L \circ H \cong L \circ F$. Let $\Phi : L \circ F \to L \circ H$ be an L-Hopf algebra isomorphism. We define an action of W on $L \circ F$ by the Galois action on L and the trivial action on F. Explicitly, for $l \in L$ and $f \in F$, we have $w \cdot lf = \sum (w_1 \cdot l)(w_2 \cdot f) = \sum (w_1 \cdot l)(\varepsilon(w_2) f) = (w \cdot l) f$. It is easy to

check that this makes $L \circ F$ a W-module algebra, that the action commutes with Δ, ε, and S, and that $F = [L \circ F]^W$. This enables us to define an action on $L \circ H$ via the isomorphism Φ. For $\alpha \in L \circ H$, we define $w \cdot \alpha = \Phi(w \cdot \Phi^{-1}(\alpha))$.

We show that the action on $L \circ H$ is a W-module algebra action. Let $\alpha, \beta \in L \circ H$. We have

$$\begin{aligned} w \cdot \alpha\beta &= \Phi(w \cdot \Phi^{-1}(\alpha\beta)) = \Phi(w \cdot \Phi^{-1}(\alpha)\Phi^{-1}(\beta)) \\ &= \Phi(\sum (w_1 \cdot \Phi^{-1}(\alpha))(w_2 \cdot \Phi^{-1}(\beta))) \\ &= \sum \Phi(w_1 \cdot \Phi^{-1}(\alpha))\Phi(w_2 \cdot \Phi^{-1}(\beta)) \\ &= \sum (w_1 \cdot \alpha)(w_2 \cdot \beta) \end{aligned}$$

We must also show that this action commutes with $\Delta_{L\circ H}, \varepsilon_{L\circ H}$, and $S_{L\circ H}$. We do the computations for comultiplication; the other cases are similar. Let $w \in W, \alpha \in L \circ H$. Then, using the facts that Φ, Φ^{-1} are Hopf algebra morphisms, and that the action of w commutes with $\Delta_{L\circ F}$, we get

$$\begin{aligned} \Delta_{L\circ H}(w \cdot \alpha) &= \Delta_{L\circ H}(\Phi(w \cdot \Phi^{-1}(\alpha))) = (\Phi \otimes \Phi)(\Delta_{L\circ F}(w \cdot \Phi^{-1}(\alpha))) \\ &= (\Phi \otimes \Phi)(w \cdot \Delta_{L\circ F}(\Phi^{-1}(\alpha))) \\ &= (\Phi \otimes \Phi)(w \cdot (\Phi^{-1} \otimes \Phi^{-1})(\Delta_{L\circ H}(\alpha))) \\ &= (\Phi \otimes \Phi)(\sum (w_1 \cdot \Phi^{-1}(\alpha_1)) \otimes (w_2 \cdot \Phi^{-1}(\alpha_2))) \\ &= \sum (w_1 \cdot \alpha_1) \otimes (w_2 \cdot \alpha_2) = w \cdot \Delta_{L\circ H}(\alpha) \end{aligned}$$

Furthermore, $\alpha \in [L \circ H]^W$ if and only if, for all $w \in W$,

$$\begin{aligned} w \cdot \alpha = \varepsilon(w)\alpha &\Leftrightarrow \Phi(w \cdot \Phi^{-1}(\alpha)) = \varepsilon(w)\alpha \\ &\Leftrightarrow w \cdot \Phi^{-1}(\alpha) = \varepsilon(w)\Phi^{-1}(\alpha) \\ &\Leftrightarrow \Phi^{-1}(\alpha) \in [L \circ F]^W = F \end{aligned}$$

Thus, $[L \circ H]^W = \Phi(F) \cong F$, and so the L-form F is obtained through this action. □

This result is similar to what Pareigis proved in [Par89, Thm. 3,7] for H and W group rings. His construction of the L-forms of H was different, and he only assumed that $K \subseteq L$ was a free W^*-Galois extension of commutative rings. It would be interesting if Theorem 5.18 could be extended to arbitrary Galois extensions of commutative algebras. Invariants of Hopf algebra actions appear to be important in this more general context [HP86, Thm. 5]. Neither result assumed the Galois extensions to be fields.

Suppose H is a W-module algebra. Since L and H commute in $L \circ H$, if $L \circ H$ is a W-module algebra, then we must have for all $w \in W$, $l \in L$, and $h \in H$, $\sum(w_1 \cdot l)(w_2 \cdot h) = w \cdot lh = w \cdot hl = \sum(w_2 \cdot l)(w_1 \cdot h)$. Conversely, if the above equation holds, then $L \circ H$ will be a W-module algebra. This will always occur if W is cocommutative, so we have

Corollary 5.19. Suppose that W is cocommutative, and let H be a Hopf algebra which is a W-module algebra with commuting action. If $K \subseteq L$ is a W^*-Galois extension, then $[L \circ H]^W$ is an L-form of H.

We now consider some examples.

Example 5.20. Let H be a Hopf algebra, and let G be a finite subgroup of the group of Hopf automorphisms on H. Let $W = KG$. The natural action of W on H is a commuting action, and since W is cocommutative, 5.19 implies that the action yields an L-form of H when $K \subseteq L$ is W^*-Galois.

Similarly, for $W = KA, H = KG$, where A and G are groups, any group action of A on G as group automorphisms gives rise to a commuting action. Conversely, any commuting action of W on H is obtained from a group action of A on G, since if $a \in A$ and $g \in G$, then $\Delta(a \cdot g) = a \cdot \Delta(g) = (a \cdot g) \otimes (a \cdot g)$, and so $a \cdot g \in G$. This is exactly what happened in [Par89] in his definition of twisted group rings.

Example 5.21. Let H be finite dimensional, semisimple, and cocommutative, and consider the left adjoint action of H on itself. Then for all $h, k \in H$,

$$\begin{aligned}
\Delta(h \cdot k) &= \sum \Delta(h_1 k S(h_2)) = \sum (h_1 k_1 S(h_4)) \otimes (h_2 k_2 S(h_3)) \\
&= \sum (h_1 k_1 S(h_2)) \otimes (h_3 k_2 S(h_4)) = \sum (h_1 \cdot k_1) \otimes (h_2 \cdot k_2) = h \cdot \Delta(k) \\
\varepsilon(h \cdot k) &= \sum \varepsilon(h_1 k S(h_2)) = \sum \varepsilon(h_1)\varepsilon(k)\varepsilon(h_2) = \varepsilon(h)\varepsilon(k) = h \cdot \varepsilon(k) \\
S(h \cdot k) &= \sum S(h_1 k S(h_2)) = \sum S^2(h_2) S(k) S(h_1) \\
&= \sum h_2 S(k) S(h_1) = h \cdot S(k)
\end{aligned}$$

Note that since H is cocommutative, then $S^2 = id$ by 1.18. Thus, the left adjoint action is a commuting action, and so it yields an L-form of H whenever $K \subseteq L$ is an H^*-Galois extension. We refer to such a form as an *adjoint form.*

Example 5.22. Let $K = \mathbb{R}, L = \mathbb{C}$. Let $H = K[x]$, the universal enveloping algebra of the one-dimensional Lie algebra. If $W = KG$, where $G = \mathbb{Z}_2 =< \sigma >$, then $K \subseteq L$ is W^*-Galois, where σ acts on L by complex conjugation. We can let W act on $L \circ H$ by $\sigma \cdot x = \omega x$, where $|\omega| = 1$. An easy check will show that this gives us all of the commuting W-module actions of W on $L \circ H$. The corresponding form is $[L \circ H]^W = K[ix]$ if $\omega = -1$, and $[L \circ H]^W = K[(1 + \omega)x]$ otherwise. In either case, $[L \circ H]^W \cong H$, and so there are no nontrivial forms. This will also

follow from 6.1.

This differs greatly from the case $H = KG$. In that case, any action which gives us a trivial form must leave a basis of grouplike elements in LG invariant. Since $G(LG) = G$, then $(LG)^W = KG$ so the action is trivial. Thus, a group action on KG gives us a nontrivial form if and only if the action is nontrivial (e.g. the left adjoint action of a nonabelian group).

In 5.22, also note that despite the fact that there are many commuting actions on $L \circ H$, there is only one L-form (up to isomorphism). Not only that, but the form is obtained by an action on $L \circ H$ which restricts to an action on H (the trivial action). This suggests the question:

Question 5.23. Can all L-forms be obtained from actions on $L \circ H$ which restrict to actions on H?

This is easily seen to be true in the case where $W = KA$ and $H = KG$ are group algebras, since any commuting action comes from a group action of A on G. We consider a more compelling example of this in Example 6.3. Question 5.23 motivates the following definition:

Definition 5.24. A stable L-form of H under W is one which can be obtained from a commuting action of W on $L \circ H$ which restricts to an action on H. We denote the set of all stable L-forms of H under W as $\mathcal{S}_{L,W}(H)$.

Thus, the question asks whether or not all L-forms are stable. It turns out that the trivial forms of H in $L \circ H$ play an important role. In order to determine this role we first need a simple observation.

Lemma 5.25. Let $K \subseteq L$ be an extension of fields, and let H, H' be K-Hopf algebras. Then any K-Hopf algebra morphism $\phi : H \to L \otimes H'$ can be extended to an L-Hopf algebra morphism $\overline{\phi} : L \otimes H \to L \otimes H'$. The map is given by $\overline{\phi}(a \otimes h) = (a \otimes 1)\phi(h)$.

This gives us the following.

Corollary 5.26. If a form $F \subseteq L \circ H$ can be obtained by an action on $L \circ H$ which restricts to an action on a trivial form $H' \subseteq L \circ H$, then F is a stable form.

Note: By a trivial form, it is meant a form of H obtained as in 5.18 which is isomorphic to H. This would be any K-Hopf algebra $H' \in L \circ H$ such that $H' \cong H$, and such that $L \otimes H' \cong L \otimes H$ via $l \otimes h' \mapsto lh'$.

Proof. Suppose $\phi : H \to H'$ is a K-Hopf algebra isomorphism, and let $\cdot$ denote the action of W on $L \circ H$. We can define a new action $*$ on $L \circ H$, where $w * h = \phi^{-1}(w \cdot \phi(h))$ for all $w \in W$ and $h \in H$, and W has the Galois action on L. As in the proof of 5.18(iii), we see that $*$ is a commuting action on $L \circ H$. Also, $*$ restricts to an action on H.

Now $\phi : H \to L \otimes H$ is a homomorphism, which we can extend to a homomorphism $\overline{\phi} : L \otimes H \to L \otimes H$ as in 5.25. Since $L \otimes H' \cong L \otimes H$ via $l \otimes h \mapsto lh$ (by 5.18), then we can define a map $\overline{\phi^{-1}} : L \otimes H \to L \otimes H$ by $lh' \mapsto l\phi^{-1}(h')$ for all $l \in L, h' \in H'$. It is easy to see that $\overline{\phi^{-1}} = \overline{\phi}^{-1}$, so $\overline{\phi^{-1}}$ is an L-Hopf isomorphism. Furthermore, for all $a \in L$, $h \in H$, and $w \in W$, we have

$$w * ah = \sum (w_1 \cdot a)(\phi^{-1}(w_2 \cdot \phi(h_i)) = \overline{\phi^{-1}}(\sum (w_1 \cdot a)(w_2 \cdot \phi(h))$$

Let $\{a_i\}$ be a basis of L over K, and let $F' = [L \circ H]^W$ under the action $*$. We then have $\sum_i a_i h_i \in F'$ for $h_i \in H$ if and only if for all $w \in W$,

$$w * \sum_i a_i h_i = \sum_i \varepsilon(w) a_i h_i$$

$$\Leftrightarrow \quad \overline{\phi^{-1}}(\sum_i (w_1 \cdot a_i)(w_2 \cdot \phi(h_i)) = \overline{\phi^{-1}}(\sum_i \varepsilon(w) a_i \phi(h_i))$$

$$\Leftrightarrow \quad \sum_i a_i \phi(h_i) \in F$$

Thus, $F' = \overline{\phi^{-1}}(F)$. The restriction of $\overline{\phi^{-1}}$ to F gives us a K-Hopf isomorphism $F \to F'$. Also, $[L \circ H]^W = F'$ under the action of $\cdot$. Thus, $F \cong F'$ is a stable form. □

Now we turn our attention to a situation where there are no nontrivial commuting actions.

Example 5.27. Let $W = u(\mathfrak{g}), H = KG$, where $\mathrm{char}(K) = p > 0$ and $\mathfrak{g}$ is a finite dimensional restricted Lie algebra. Let $K \subseteq L$ be a W^*-Galois extension and suppose we have a commuting action of W on $L \circ H$. If $x \in \mathfrak{g}$, then

$$\Delta(x \cdot g) = x \cdot \Delta(g) = (x \cdot g) \otimes g + g \otimes (x \cdot g)$$

so $x \cdot g \in P_{g,g}(L[G]) = 0$. Thus, W acts trivially, and so $[L \circ H]^W = H$. However, this tells us nothing about the L-forms of H, since if $K \subseteq L$ is $u(\mathfrak{g})^*$-Galois, then $u(\mathfrak{g})$ is not semisimple by the remarks following 3.30. Thus, 5.18 does not apply. Fortunately, we can still determine the L-forms in this case. Recall from 3.29 that $K \subseteq L$ is totally inseparable of exponent ≤ 1, and so 5.9 implies that there cannot be any nontrivial forms.

Now we look at some examples of actions that are not commuting actions.

Example 5.28. Let G be a finite group, $W = KG, H = (KG)^*$. Then W acts on H via $(g \cdot f)(h) = f(hg)$, where $g, h \in G$ and $f \in (KG)^*$. If $\{p_x : x \in G\}$ is the dual basis of G in H, then $g \cdot p_x = p_{xg^{-1}}$. We have, for each $x, g \in G$,

$$\begin{aligned} \Delta(g \cdot p_x) &= \Delta(p_{xg^{-1}}) = \sum_{uv=xg^{-1}} p_u \otimes p_v \\ g \cdot \Delta(p_x) &= g \cdot (\sum_{st=x} p_s \otimes p_t) = \sum_{st=x} (g \cdot p_s) \otimes (g \cdot p_t) = \sum_{st=x} p_{sg^{-1}} \otimes p_{tg^{-1}} \end{aligned}$$

But if these are equal, then $sg^{-1}tg^{-1} = uv = xg^{-1} = stg^{-1}$, so $sg^{-1}t = st$ and $g^{-1} = 1$, which is a contradiction if $G \neq 1$. Thus, this is not a commuting action.

Example 5.29. With G as above, let $W = (KG)^*, H = KG$. Then $p_x \cdot g = \delta_{x,g} g$ and so

$$\begin{aligned} \Delta(p_x \cdot g) &= \Delta(\delta_{x,g} g) = \delta_{x,g} g \otimes g \\ p_x \cdot \Delta(g) &= p_x \cdot (g \otimes g) = \sum_{uv=x} (p_u \cdot g) \otimes (p_v \cdot g) \\ &= \sum_{uv=x} \delta_{u,g} \delta_{v,g} g \otimes g = \delta_{x,g^2} g \otimes g \end{aligned}$$

Thus, equality holds $\Leftrightarrow g = g^2 \Leftrightarrow g = 1$, so again we have a non-commuting action in general.

Chapter 6

Applications of the Main Theorem

In this chapter, we use 5.18 to compute L-forms for various Hopf algebras. In the first section, we characterize the L-forms of enveloping algebras, and give an example of an enveloping algebra whose L-forms are all stable. Then we turn our attention to L-forms of H^*, where H is a finite dimensional Hopf algebra. Finally, we compute a form of KD_{2n} via the adjoint action.

6.1 Forms of Enveloping Algebras

Our first result concerns the Hopf algebra forms of enveloping algebras. It turns out that these forms are merely enveloping algebras of Lie algebras which are Lie algebra forms of each other.

Proposition 6.1. Suppose that a K-Hopf algebra F is an L-form of $U(\mathfrak{g})$ in characteristic zero or $u(\mathfrak{g})$ in characteristic $p > 0$. Then

(i) F is a universal enveloping algebra in characteristic zero and a restricted enveloping algebra in characteristic $p > 0$.

(ii) If $K \subseteq L$ is a W^*-Galois field extension in characteristic zero for W a

finite dimensional semisimple Hopf algebra, and if W acts on $L \otimes U(\mathfrak{g})$ as in Theorem 5.18, then $[L \otimes U(\mathfrak{g})]^W = U([L \otimes \mathfrak{g}]^W)$ (similarly for restricted Lie algebras in characteristic p). Thus, any L-form of $U(\mathfrak{g})$ is equal to $U([L \otimes \mathfrak{g}]^W)$.

Note that in characteristic zero, $U(\mathfrak{g}) \cong U(\mathfrak{g}')$ as Hopf algebras if and only if $\mathfrak{g} \cong \mathfrak{g}'$ as Lie algebras (similarly for restricted Lie algebras in characteristic p). Thus, the above says that finding the Hopf algebra L-forms of enveloping algebras is equivalent to finding the L-forms of their Lie algebras. In addition, (ii) says that we can find the L-forms of Lie algebras in the same way that we find the L-forms of Hopf algebras. They are merely the invariant subalgebras of $L \otimes \mathfrak{g}$ under appropriate actions of W. For each $w \in W$ and $x, y \in \mathfrak{g}$, such actions satisfy $w \cdot [x, y] = w \cdot xy - w \cdot yx = \sum (w_1 \cdot x)(w_2 \cdot y) - (w_1 \cdot y)(w_2 \cdot x)$ and $w \cdot x \in L \otimes \mathfrak{g}$. If W is cocommutative, we get $w \cdot [x, y] = \sum [w_1 \cdot x, w_2 \cdot y]$. For $W = KG$, this is equivalent to G acting as Lie automorphisms on $L \otimes \mathfrak{g}$. This is analogous to the methods Jacobson used in [Jac62, Chap. 10] to find the forms of nonassociative algebras.

We will first need a well-known fact which tells us when a Hopf algebra is an enveloping algebra.

Lemma 6.2. Let H be a K-bialgebra, let $\mathfrak{g}$ be a Lie subalgebra of $P(H)$, and let B be the K-subalgebra of H generated by $\mathfrak{g}$.

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

(ii) If $char(K) = p > 0$, and if $\mathfrak{g}$ is a restricted Lie subalgebra of $P(H)$, then B is naturally isomorphic to $u(\mathfrak{g})$.

Notice that this implies that a Hopf algebra is an enveloping algebra if and

only if it is generated as an algebra by primitive elements.

Proof. (of 6.1) For (i), it suffices, by 6.2, to show that F is generated as an algebra by primitive elements. Let $\Phi : L \otimes U(\mathfrak{g}) \longrightarrow L \otimes F$ be an L-Hopf algebra isomorphism. Let $\{l_i\}$ be a basis for L over K, and let $x \in \mathfrak{g}$. Then $\Phi(x) = \sum_i l_i f_i$, for some $f_i \in F$. We have

$$\begin{aligned}
\sum_i l_i \Delta(f_i) &= \Delta(\sum_i l_i f_i) = \Delta(\Phi(x)) = (\Phi \otimes \Phi)(\Delta(x)) \\
&= \Phi(x) \otimes_L 1 + 1 \otimes_L \Phi(x) = (\sum_i l_i f_i) \otimes_L 1 + 1 \otimes_L (\sum_i l_i f_i) \\
&= \sum_i l_i \otimes_K f_i \otimes_K 1 + l_i \otimes_K 1 \otimes_K f_i = \sum_i l_i (f_i \otimes_K 1 + 1 \otimes_K f_i)
\end{aligned}$$

Since $\{l_i\}$ is a basis, we have $\Delta(f_i) = f_i \otimes 1 + 1 \otimes f_i$, and so f_i is primitive for all i. The $\Phi(x)$'s generate $L \otimes F$ over L, so the f_i's generate $L \otimes F$ over L. But this implies that the f_i's generate F over K, and so F is an enveloping algebra.

For (ii), 5.18 implies that $[L \otimes U(\mathfrak{g})]^W$ is an L-form of $U(\mathfrak{g})$. By (i), it is generated by primitive elements, which means that it is generated by elements in $L \otimes \mathfrak{g}$. But these elements are also invariants under the action of W, so they are in $[L \otimes \mathfrak{g}]^W$. Thus, $[L \otimes U(\mathfrak{g})]^W = U([L \otimes \mathfrak{g}]^W)$. The second part follows immediately. □

Example 6.3. Let ω be a primitive n^2th root of unity, $K = \mathbb{Q}(\omega^n)$, $L = \mathbb{Q}(\omega)$. Also, let $G = \mathbb{Z}_n =< \sigma >$. Then $K \subseteq L$ is a $(KG)^*$-Galois extension, where G acts on L via $\sigma \cdot \omega = \omega^{n+1}$. Define $\mathfrak{g} = K\text{-span}\{x, y_0, \cdots, y_{n-1}\}$, where the Lie product is given by $[x, y_i] = \omega^{in} y_i$, $[y_i, y_j] = 0$. We now set out to determine the L-forms of $U(\mathfrak{g})$ up to isomorphism. By 6.1, it suffices to compute the invariant rings of $L \otimes \mathfrak{g}$ under commuting actions.

Let $1 \leq k \leq n$, and define an action of G on $U(\mathfrak{g})$ by $\sigma \cdot x = \omega^{-kn}x, \sigma \cdot y_i = y_{i+k}$, where we let $y_{i+n} = y_i$ for all i. One can check that this is a commuting action, and so it will yield a form $\mathfrak{g}_k = [L \otimes \mathfrak{g}]^W$.

We now compute a basis for $\mathfrak{g}_k$. Let $d = \gcd(k, n)$, set $l = \frac{n}{d}$, and consider the elements $r = \omega^k x, s_{jt} = \sum_{i=0}^{n-1} \omega^{jk(in+1)} y_{ik+t}$, where $0 \leq t \leq d-1, 0 \leq j \leq l-1$. It is easy to check that r and the s_{jt}'s are invariants. Moreover, they form a basis for $\mathfrak{g}_k$. To see this, note that since $L \otimes \mathfrak{g} \cong L \otimes \mathfrak{g}_k$, we have $\dim(\mathfrak{g}_k) = \dim(\mathfrak{g}) = n+1$. It thus suffices to prove that $\{r, s_{jt}\}$ are linearly independent over K. Since $\{x, y_i : 0 \leq i \leq n-1\}$ is independent over K and r is a scalar multiple of x, it suffices to show that the s_{jt}'s are linearly independent over K.

Suppose $\sum_{j,t} c_{jt} s_{jt} = 0$ with $c_{jt} \in K$. Then

$$0 = \sum_{j,t} c_{jt} s_{jt} = \sum_{j=0}^{l-1} \sum_{t=0}^{d-1} \sum_{i=0}^{n-1} c_{jt} \omega^{jk(in+1)} y_{ik+t} \tag{6.1}$$

We look at the coefficients of y_t for $0 \leq t \leq d-1$. It follows from (6.1) that we get a contribution to the coefficient of y_t from each coefficient of y_{ik+t}, where $ik + t = zn + t$ for some $z \in \mathbb{Z}$. Thus, $i = \frac{zn}{k} = \frac{zl}{k/d}$, so $\frac{k}{d} | zl$. Since $\gcd(\frac{k}{d}, l) = \gcd(\frac{k}{d}, \frac{n}{d}) = 1$, we have $\frac{k}{d} | z$, so $k | zd$. Write $zd = z'k$. Then $i = \frac{zn}{k} = \frac{zdl}{k} = \frac{z'kl}{k} = z'l$. In particular, $z' \leq d-1$. We substitute $i = z'l$ in the coefficient of y_{ik+t} to get the coefficient of y_t, which is

$$\sum_{j=0}^{l-1} \sum_{z'=0}^{d-1} c_{jt} \omega^{jk(z'ln+1)} = \sum_{j=0}^{l-1} \sum_{z'=0}^{d-1} c_{jt} \omega^{jk} = \sum_{j=0}^{l-1} d c_{jt} \omega^{jk}$$

since $\omega^{jkz'ln} = 1$. Now the ω^{jk} are linearly independent over K, so $c_{jt} = 0$, which proves linear independence.

Thus, $\mathfrak{g}_k = \text{span}\{r, s_{jt} : 0 \leq t \leq d-1, 0 \leq j \leq l-1\}$. It is not difficult to

compute the Lie bracket relations. We get $[r, s_{jt}] = \omega^{nt} s_{(j+1)t}, [s_{jt}, s_{j't'}] = 0$, and $s_{(j+l)t} = \omega^{kl} s_{jt}$.

The remainder of this section will be devoted to showing that the $\mathfrak{g}_k$ are mutually nonisomorphic as Lie algebras, and that they are all the L-forms of $\mathfrak{g}$. Let $I = \text{span}\{s_{jt} : 0 \leq t \leq d-1, 0 \leq j \leq l-1\}$ and, for each $0 \leq t \leq d-1$, let $I_t = \text{span}\{s_{jt} : 0 \leq j \leq l-1\}$. It is easy to show that I and I_t are Lie ideals of $\mathfrak{g}_k$. It is also clear that I is the unique abelian Lie ideal in $\mathfrak{g}_k$ of codimension 1, and that $I = \bigoplus_{t=0}^{d-1} I_t$.

Lemma 6.4. Let $w \notin I$. Then

(i) For all $0 \leq t \leq d-1, v \in I_t$, v is an eigenvector for $ad^l(w)$.

(ii) Let $v \in I$. If v is an eigenvector for $ad(w)^m$, then $m = 0$ or $m \geq l$.

Proof. We first reduce the problem a bit. Write $w = ar + \sum_j b_j s_{jt}$. Since $w \notin I$, we have $a \neq 0$, so without loss of generality, $a = 1$. But then $ad(w) = ad(r)$ on I, since I is abelian, so we can assume that $w = r$. An easy induction gives us that $ad(r)^m(s_{jt}) = \omega^{mnt} s_{(j+m)t}$ for all $m \geq 0$. Thus, if $v = \sum_j c_j s_{jt}$, then

$$ad(r)^l(v) = \sum_j \omega^{lnt} c_j s_{(j+l)t} = \sum \omega^{lnt+kl} c_j s_{jt} = \omega^{lnt+kl} v$$

Thus, v is an eigenvector for $ad(r)^l$, which gives us (i).

For (ii), we can again assume that $w = r$. We write $v = \sum_{t=0}^{d-1} v_t$, where $v_t \in I_t$. If $ad(r)^m(v) = av$, we must have $\sum_t ad(r)^m(v_t) = \sum_t av_t$. Since the sum of the I_t's is direct, we have $ad(r)^m(v_t) = av_t$, and so each v_t is an eigenvector for $ad^m(r)$. We can then assume that $v \in I_t$ for some t.

Write $v = \sum_{j=0}^{l-1} c_j s_{jt}$ with $c_j \in K$. By (i), v is an eigenvector for $ad(r)^l$. Let $m > 0$ be minimal such that v is an eigenvector for $ad(r)^m$. Since v is an

eigenvector of $ad(r)^l$, a simple number theoretic argument gives us $m|l$. Write $l = pm$ for some integer $p \geq 1$. We have that $ad(r)^m(v) = av$ for some $a \in K$. Also, a calculation gives us

$$ad(r)^m(v) = \sum_j c_j \omega^{mnt} s_{(j+m)t} = \sum_{j=0}^{m-1} \omega^{kpm+mnt} c_{j+(p-1)m} s_{jt} + \sum_{j=m}^{pm-1} \omega^{mnt} c_{j-m} s_{jt}$$

If we equate the coefficients of $ad(r)^l(v)$ and av, we get

$$ac_j = \omega^{kmp+mnt} c_{j+(p-1)m}, \ 0 \leq j \leq m-1 \tag{6.2}$$

$$ac_j = \omega^{mnt} c_{j-m}, \qquad m \leq j \leq pm-1 \tag{6.3}$$

Let i be minimal such that $c_i \neq 0$. If $c_j = 0$ for all $j < m$, then (6.3) implies that $v = 0$. Therefore, $i < m$. An easy induction gives us, using (6.3), that for all integers $0 \leq b \leq p-1$, $c_i = \omega^{-bmnt} a^b c_{i+bm}$. Setting $b = p-1$, we get $c_i = \omega^{-(p-1)mnt} a^{p-1} c_{i+(p-1)m}$. But (6.2) gives us that $c_i = \frac{1}{a} \omega^{kmp+mnt} c_{i+(p-1)m}$. Putting these together and simplifying, we get

$$a^p = \omega^{kmp} \omega^{pmnt} = \omega^{kl+lnt}$$

Now we take p^{th} roots of both sides. Notice, since $p|l$ and $l|n$, that all the p^{th} roots of unity are in K. We have $a = \omega^{\frac{kl+lnt}{p}} \cdot (p^{th} \text{ root of unity})$, and so $\omega^{\frac{kl+lnt}{p}} \in K$. We must then have $n|\frac{kl+lnt}{p}$. Since $p|l$, we have $n|\frac{lnt}{p}$. This forces $n|\frac{kl}{p}$. But $kl = n(\frac{k}{d})$, so we must have $p|\frac{k}{d}$.

But recall that $\gcd(\frac{n}{d}, l) = 1$. Since, $p|l$ and $p|\frac{k}{d}$, it follows that $p = 1$, and so $m = l$. This gives us (ii), and the proof is complete. □

Proposition 6.5. Let $K, L, \mathfrak{g}, \mathfrak{g}_k$ be as above.

(i) The $\mathfrak{g}_k$ are mutually nonisomorphic K-Lie algebras.

(ii) The $\mathfrak{g}_k$ are all the L-forms of $\mathfrak{g}$ up to isomorphism, and thus $U(\mathfrak{g}_k)$ are all the L-forms of $U(\mathfrak{g})$.

Proof. Suppose that $1 \leq k, k' \leq n$, with $\mathfrak{g}_k \cong \mathfrak{g}_{k'}$. Let $d = \gcd(n,k)$, $d' = \gcd(n,k')$, $l = \frac{n}{d}$, and $l' = \frac{n}{d'}$. Also define $I' \triangleleft \mathfrak{g}_{k'}$ similarly as for $I \triangleleft \mathfrak{g}_k$. Without loss of generality, $l \leq l'$. Let $\Phi : \mathfrak{g}_k \to \mathfrak{g}_{k'}$ be an isomorphism of Lie algebras. Since I, I' are the unique abelian ideals of codimension 1 in their respective Lie algebras, we must have $\Phi(I) = I'$. By 6.4(i), s_{jt} is an eigenvector for $ad^l(r)$. Since Φ is an isomorphism, this makes $\Phi(s_{jt})$ an eigenvector for $ad^l(\Phi(r))$. But $\Phi(r) \notin I'$, so 6.4(ii) gives us $l \geq l'$. Then $l = l'$, which implies that $d = d'$.

We now have $gcd(n,k) = gcd(n,k') = d$. Thus,

$$\begin{aligned} \mathfrak{g}_k &= span\{r, s_{jt} : 0 \leq j \leq l-1, 0 \leq t \leq d-1\} \\ \mathfrak{g}_{k'} &= span\{r', s'_{jt} : 0 \leq j \leq l-1, 0 \leq t \leq d-1\} \end{aligned}$$

Write $\Phi(s_{00}) = \sum_{j,t} b_{jt} s'_{jt}$, where $b_{jt} \in K$, and the b_{jt} are not all zero. Also write $\Phi(r) = ar' + \sum_{j,t} a_{jt} s'_{jt}$, where $a, a_{jt} \in K$. Since $ad(\Phi(r)) = ad(ar')$ on I', an easy induction gives us

$$ad(\Phi(r))^l(\Phi(s_{00})) = \sum_{j,t} a^l \omega^{lnt} b_{jt} s'_{(j+l)t} = \sum_{j,t} a^l \omega^{lnt+k'lt} b_{jt} s'_{jt}$$

But Φ is a homomorphism, so we get

$$ad(\Phi(r))^l(\Phi(s_{00})) = \Phi(ad(r)^l(s_{00})) = \Phi(s_{l0}) = \omega^{kl}\Phi(s_{00}) = \sum_{j,t} \omega^{kl} b_{jt} s'_{jt}$$

This tells us that $\omega^{kl} b_{jt} = a^l \omega^{lnt+k'lt} b_{jt}$ for all j, t. Since not all the b_{jt} are zero, we have $a^l = \omega^{l(k-k'-nt)}$ for some t. But then $a = \omega^{k-k'-nt} \cdot (l^{th}$ root of unity), and since $a \in K$, we must have $k = k'$. This gives us (i).

For (ii), we look at what an action of G on $L \otimes \mathfrak{g}$ must satisfy (keeping in mind that G acts as Lie automorphisms on $L \otimes \mathfrak{g}$). After a bit of calculation, we get

$$\sigma \cdot x = \omega^{-kn} x + \sum_{j=1}^{n-1} b_j y_j, \qquad \sigma \cdot y_i = a_i y_{i+k}$$

for some $0 \leq k \leq n-1$, where the $a_i, b_j \in L$ are chosen so that $\sigma^n \cdot x = x$ and $\sigma^n \cdot y_i = y_i$. We will show that $[L \otimes \mathfrak{g}]^{KG} \cong \mathfrak{g}_k$.

To determine the form obtained from this action, we need only consider primitive invariant elements. Suppose that $\alpha = ax + \sum_j c_j y_j \in [L \otimes \mathfrak{g}]^{KG}$. Then

$$\begin{aligned} ax + \sum_j c_j y_j &= (\sigma \cdot a)\omega^{-kn} x + \sum_j (\sigma \cdot a) b_j y_j + \sum_j (\sigma \cdot c_j) a_j y_{j+k} \\ &= (\sigma \cdot a)\omega^{-kn} x + \sum_j ([\sigma \cdot a] b_{j+k} + [\sigma \cdot c_j] a_j) y_{j+k} \end{aligned}$$

which yields $a = (\sigma \cdot a)\omega^{-kn}$ and $c_{j+k} = (\sigma \cdot a) b_{j+k} + (\sigma \cdot c_j) a_j$.

Write $a = \sum_{i=0}^{n-1} q_i \omega^i$ with $q_i \in K$. The equation $a = (\sigma \cdot a)\omega^{-kn}$ yields

$$\sum_i q_i \omega^i = \sum_i q_i \omega^{in+i-kn} = \sum_i q_i \omega^{(i-k)n} \omega^i$$

Matching coefficients, we get $q_i = q_i \omega^{(i-k)n}$, so $q_i = 0$ or $\omega^{(i-k)n} = 1$. Thus, if $q_i \neq 0$, then $n | i-k$ and so $i = k$. Therefore, $a = q\omega^k$ for some $q \in K$.

First, suppose that $a = 0$. We then have $c_{t+k} = (\sigma \cdot c_t) a_t$. Once we are able to define c_t for $0 \leq t \leq d-1$, then we can define the rest of the c_t inductively using this relation and the fact that $d = \gcd\{k, n\}$. The only restriction on c_t is that $c_t = c_{t+kl} = (\sigma^l \cdot c_t)(\sigma^{l-1} \cdot a_t)(\sigma^{l-2} \cdot a_{t+k}) \cdots a_{t+(l-1)k} = (\sigma^l \cdot c_t) A_t$, where $A_t = (\sigma^{l-1} \cdot a_t)(\sigma^{l-2} \cdot a_{t+k}) \cdots a_{t+(l-1)k}$. For each $0 \leq t \leq d-1$, we then want to find all of the elements $c_t \in L$ such that $c_t = (\sigma^l \cdot c_t) A_t$ with $c_t \neq 0$ if possible. If c_t' is another such element, and $c_t \neq 0$, then it is easy to show that $\frac{c_t'}{c_t}$ is fixed by σ^l,

and so $\frac{c'_t}{c_t} \in L^{\sigma^l} = K(\omega^k)$. Thus, if $c_t \neq 0$, then the set $\{c_{jt} = \omega^{jk} c_t : 0 \leq j \leq l-1\}$ is a basis over K for the space of all c'_t satisfying $c'_t = (\sigma^l \cdot c'_t)A_t$. We then can define $c_{j(ik+t)}$ for all $0 \leq i \leq l-1$ by defining, inductively, $c_{j(t+k)} = (\sigma \cdot c_{jt})a_t$. By the way we have defined $c_{j(ik+t)}$, we get that $s_{jt} = \sum_{i=0}^{l-1} c_{j(ik+t)} y_{ik+t} \in [L \otimes \mathfrak{g}]^{KG}$. Furthermore, since the c_{jt} span all possible coefficients of y_t for elements in $[L \otimes \mathfrak{g}]^{KG}$ which have no nonzero x term, then the s_{jt} span the space of all invariant elements of the form $\sum_j c_j y_j$.

If $a = q\omega^k \neq 0$, then, substituting $\frac{\alpha}{q}$ for α, we can assume that $a = \omega^k$. Suppose we have two sets of elements $\{b'_t\}, \{b''_t\} \subseteq L$ such that $r = \omega^k x + \sum_t b'_t y_t$ and $r' = \omega^k x + \sum_t b''_t y_t$ are KG-invariants. Subtracting these, we get $\sum_t (b'_t - b''_t) y_t \in [L \otimes \mathfrak{g}]^{KG}$, so by the $a = 0$ case, $r - r' \in \text{span}\{s_{jt}\}$. Thus, r is unique modulo $\text{span}\{s_{jt}\}$.

Putting these together, we get that $[L \otimes \mathfrak{g}]^{KG}$ is spanned by the set

$$\{r, s_{jt} : 0 \leq t \leq d-1, 0 \leq j \leq l-1\}$$

Since $\dim_K [L \otimes \mathfrak{g}]^{KG} = n+1$, these elements form a basis for $[L \otimes \mathfrak{g}]^{KG}$. In particular, $s_{jt} \neq 0$ for all j, t. We need only show that r and the s_{jt} satisfy the same Lie product relations as their counterparts in $\mathfrak{g}_k$.

Claim: Let $0 \leq t \leq d-1$. Then $c_{j(t+ik)} = \omega^{jk(in+1)} c_{0(t+ik)}$.

Proof. We induct on i. The definition of c_{jt} gives us the $i = 0$ case. For the inductive step, we have

$$\begin{aligned} c_{j(t+[i+1]k)} &= (\sigma \cdot c_{j(t+ik)})a_{t+ik} = (\sigma \cdot [\omega^{jk(in+1)} c_{0(t+ik)}])a_{t+ik} \\ &= \omega^{jk([i+1]n+1)} (\sigma \cdot c_{0(t+ik)})a_{t+ik} = \omega^{jk([i+1]n+1)} c_{0(t+[i+1]k)} \end{aligned}$$

which completes the proof. □

As an easy corollary, we get

$$\begin{aligned} c_{(j+1)(ik+t)} &= \omega^{(j+1)k(in+1)} c_{0(ik+t)} = \omega^{k(in+1)} \omega^{jk(in+1)} c_{0(ik+t)} \\ &= \omega^{k(in+1)} c_{j(ik+t)} \end{aligned}$$

This gives us

$$\begin{aligned} [r, s_{jt}] &= [\omega^k x + \sum_j b'_j y_j, \sum_i c_{j(ik+t)} y_{ik+t}] = \sum_i \omega^k c_{j(ik+t)} [x, y_{ik+t}] \\ &= \sum_i \omega^k c_{j(ik+t)} \omega^{n(ik+t)} y_{ik+t} = \omega^{nt} \sum_i \omega^{k(in+1)} c_{j(ik+t)} y_{ik+t} \\ &= \omega^{nt} \sum_i c_{(j+1)(ik+t)} y_{ik+t} = \omega^{nt} s_{(j+1)t} \end{aligned}$$

Finally, a trivial computation shows that $s_{(j+l)t} = \omega^{kl} s_{jt}$, and so $[L \otimes \mathfrak{g}]^{KG} \cong \mathfrak{g}_k$. Thus, the $\mathfrak{g}_k$ are all the L-forms of $\mathfrak{g}$ up to isomorphism, which gives us (ii). □

Notice that all of the L-forms of $U(\mathfrak{g})$ are stable.

6.2 Forms of Duals of Hopf Algebras

We turn our attention to determining forms for duals of finite dimensional Hopf algebras. This can be looked at from two perspectives. First, there is a natural correspondence between L-forms of H and L-forms of H^*.

Proposition 6.6. Let H be a finite dimensional Hopf algebra over a field K with $K \subseteq L$ a field extension. Then

(i) $L \otimes H^* \cong (L \otimes H)^*$ as L-Hopf algebras.

(ii) The L-forms for H^* are precisely the duals of the L-forms for H.

Proof. Define $\phi : L \otimes H^* \to (L \otimes H)^*$ by $\phi(a \otimes f)(b \otimes h) = f(h)ab$ for all $a, b \in L$, $h \in H$, and $f \in H^*$. We first show that ϕ is an algebra map. It is clear that $\phi(1 \otimes \varepsilon_H) = \varepsilon_{L \otimes H}$. Let $a, b, c \in L$, $h \in H$, and $f, g \in H^*$. We then have

$$\begin{aligned}
(\phi(a \otimes f)\phi(b \otimes g))(c \otimes h) &= \sum \phi(a \otimes f)(c \otimes h_1)\phi(b \otimes g)(1 \otimes h_2) \\
&= \sum abcf(h_1)g(h_2) \\
&= abc(fg)(h) = \phi(ab \otimes fg)(c \otimes h) \\
&= \phi([a \otimes f][b \otimes g])(c \otimes h)
\end{aligned}$$

and so ϕ is an algebra homomorphism.

Now we show that ϕ is a Hopf algebra morphism. We have

$$\begin{aligned}
(\phi \otimes \phi)\Delta(a \otimes f)([b \otimes h] \otimes [c \otimes h']) &= \sum \phi(a \otimes f_1)(b \otimes h) \otimes \phi(1 \otimes f_2)(c \otimes h') \\
&= \sum abcf_1(h)f_2(h') \\
&= f(hh')abc \\
&= \phi(a \otimes f)(bc \otimes hh') \\
&= (\Delta \circ \phi(a \otimes f))([b \otimes h] \otimes [c \otimes h'])
\end{aligned}$$

and so $\Delta \circ \phi = (\phi \otimes \phi) \circ \Delta$. The other axioms follow similarly, and so ϕ is a Hopf algebra morphism.

It remains to show that ϕ is bijective. By comparing dimensions over L, we need only show that ϕ is injective. Let $\{h_i\}$ be a basis for H with dual basis $\{h_i^*\}$, and suppose that $\sum_i a_i \otimes h_i^* \in ker\phi$. Then for all j, we have

$$0 = \sum_i \phi(a_i \otimes h_i^*)(1 \otimes h_j) = a_j$$

and so $ker\phi = 0$. This gives us (i).

For (ii), let H' be an L-form of H^*. Then

$$L \otimes (H')^* \cong (L \otimes H')^* \cong (L \otimes H^*)^* \cong L \otimes H$$

Thus, $(H')^*$ is an L-form of H. Similarly, if H' is an L-form of H, then $(H')^*$ is an L-form of H^*, and so (ii) follows. □

We can also look at this question from the perspective of 5.18. In this context, we restrict our attention to stable L-forms. Let H, W, and $K \subseteq L$ be as before, except we require H to be finite dimensional. The stable L-forms for H under W are obtained by finding appropriate commuting actions of W on H. We attempt to use these actions to help us compute forms of H^*. Our goal will be to find a correspondence between stable L-forms of H under W and stable L-forms of H^* under W^{cop}. The first step in this direction is finding a correspondence between W-actions on H and W^{cop}-actions on H^*.

Proposition 6.7. If H is a left W-module algebra with a commuting action, then H° is a left W^{cop}-module with commuting action. Conversely, if H is finite dimensional, then if H^* is a left W^{cop}-module algebra with commuting action, then H is a left W-module algebra with commuting action.

Note that in the case where H is infinite dimensional, we can determine some of the commuting actions of W^{cop} on H° from the commuting actions of W on H, but not necessarily all of them.

Proof. To avoid confusion, we distinguish between the Hopf algebra maps of H and H° by writing them as Δ, Δ^*, etc. We first assume that H is a left W-module

algebra with commuting action. Then for all $f \in H^\circ$, define $(w \cdot f)(h) = f(S(w) \cdot h)$. We need to show that this is a left W^{cop}-module algebra action on H^*, and that the action commutes with the Hopf algebra maps of H°.

We first prove that if $f \in H^\circ$, then $w \cdot f \in H^\circ$. It suffices by 1.13 to show that $\Delta^*(w \cdot f) \in H^* \otimes H^*$. Since $f \in H^\circ$, we can write $\Delta^*(f) = \sum f_1 \otimes f_2$, where all the $f_1, f_2 \in H^\circ$, and for every $h, h' \in H$, we have $f(hh') = \sum f_1(h) f_2(h')$. We get

$$\begin{aligned}
\Delta^*(w \cdot f)(h \otimes h') &= (w \cdot f)(hh') = f(S(w) \cdot hh') \\
&= \sum f([S(w_2) \cdot h][S(w_1) \cdot h']) \\
&= \sum f_1(S(w_2) \cdot h) f_2(S(w_1) \cdot h') \\
&= \sum (w_2 \cdot f_1)(h)(w_1 \cdot f_2)(h') \\
&= (\sum (w_2 \cdot f_1) \otimes (w_1 \cdot f_2))(h \otimes h')
\end{aligned}$$

so $\Delta^*(w \cdot f) = \sum (w_2 \cdot f_1) \otimes (w_1 \cdot f_2) \in H^* \otimes H^*$, giving us $w \cdot f \in H^\circ$. The above also shows that the action of w commutes with comultiplication in W^{cop}.

Now we show that this definition leads to an action on H°. For all $w, w' \in W$, $f \in H^\circ$, and $h \in H$, we have

$$\begin{aligned}
(ww' \cdot f)(h) &= f(S(ww') \cdot h) = f(S(w')S(w) \cdot h) \\
&= (w' \cdot f)(S(w) \cdot h) = (w \cdot [w' \cdot f])(h)
\end{aligned}$$

Thus, it is an action. For the remainder of the W-module algebra structure, we

note that

$$\begin{aligned}(w\cdot\varepsilon)(h) &= \varepsilon(S(w)\cdot h)=\varepsilon(S(w))\varepsilon(h)=\varepsilon(w)\varepsilon(h)=(\varepsilon(w)\varepsilon)(h)\\ (w\cdot fg)(h) &= fg(S(w)\cdot h)=\sum f([S(w)\cdot h]_1)g([S(w)\cdot h]_2)\\ &= \sum f(S(w_2)\cdot h_1)g(S(w_1)\cdot h_2)=\sum(w_2\cdot f)(h_1)(w_1\cdot g)(h_2)\\ &= \sum(w_2\cdot f)(w_1\cdot g)(h)\end{aligned}$$

which gives us that W^{cop} acts trivially on ε, and $w\cdot fg=\sum(w_2\cdot f)(w_1\cdot g)$. Therefore, H° is a left W^{cop}-module algebra.

Now we must prove that we have a commuting action. As shown above, the action commutes with comultiplication in H°. For the counit and antipode,

$$\begin{aligned}\varepsilon^*(w\cdot f) &= (w\cdot f)(1_H)=f(S(w)\cdot 1_H)=\varepsilon(w)\varepsilon^*(f)\\ S^*(w\cdot f)(h) &= (w\cdot f)(S(h))=f(S(w)\cdot S(h))=f(S(S(w)\cdot h))\\ &= (f\circ S)(S(w)\cdot h)=S^*(f)(S(w)\cdot h)=(w\cdot S^*(f))(h)\end{aligned}$$

which gives us that the action commutes.

Conversely, suppose that H is finite dimensional and that H^* is a left W^{cop}-module algebra with commuting action. Then S is bijective by [Mon93, 2.1.3(2)]. Let $\{h_1,\cdots,h_n\}$ be a basis for H, $\{h_1^*,\cdots,h_n^*\}$ the dual basis in H^*. Then for each $w\in W$ and $1\le i\le n$, we have $w\cdot h_i^*=\sum_j a_{ij}(w)h_j^*$, where $a_{ij}\in W^*$. Define the action $w\cdot h_i=\sum_j a_{ji}(S^{-1}(w))h_j$.

Claim: For all $f\in H^*, w\in W, h\in H$, we have $(w\cdot f)(h)=f(S(w)\cdot h)$

Proof. It suffices to prove the claim for $f=h_i^*$ and $h=h_k$. We have

$$(w\cdot h_i^*)(h_k)=\sum_j a_{ij}(w)h_j^*(h_k)=a_{ik}(w)=h_i^*(\sum_j a_{jk}(w)h_j)=h_i^*(S(w)\cdot h_k)$$

which proves the claim. □

Let $f \in H^*$, $h \in H$, and $w, w' \in W$. We will use the fact that S and S^{-1} are algebra anti-homomorphisms and coalgebra anti-morphisms by 1.16. We have

$$\begin{aligned} f(ww' \cdot h) &= (S^{-1}(ww') \cdot f)(h) = (S^{-1}(w')S^{-1}(w) \cdot f)(h) \\ &= (S^{-1}(w) \cdot f)(w' \cdot h) = f(w \cdot [w' \cdot w']) \end{aligned}$$

Since this is true for all $f \in H^*$, it follows that $ww' \cdot h = w \cdot (w' \cdot h)$, which implies that we have a left action.

For the W-module algebra requirements, we have, for all $f \in H^*$,

$$\begin{aligned} f(\varepsilon(w) \cdot 1_H) &= \varepsilon(w)f(1_H) = \varepsilon(S^{-1}(w))\varepsilon^*(f) \\ &= \varepsilon^*(S^{-1}(w) \cdot f) = (S^{-1}(w) \cdot f)(1_H) = f(w \cdot 1_H) \end{aligned}$$

which implies that W acts trivially on 1_H.

The multiplicative aspect of H being a W-module algebra requires a small fact. Let w, f be as before, with $h, h' \in H$, and let $\Delta^*(f) = \sum f_1 \otimes f_2$. Then using the fact that we are acting on H^* by W^{cop}, as well as the fact that this action commutes,

$$\begin{aligned} \Delta^*(S^{-1}(w) \cdot f)(h \otimes h') &= (S^{-1}(w) \cdot \Delta^*(f))(h \otimes h') \\ &= \sum (S^{-1}(w_1) \cdot f_1 \otimes S^{-1}(w_2) \cdot f_2)(h \otimes h') \\ &= \sum (S^{-1}(w_1) \cdot f_1)(h)(S^{-1}(w_2) \cdot f_2)(h') \\ &= \sum f_1(w_1 \cdot h) f_2(w_2 \cdot h') \\ &= \sum \Delta^*(f)(w_1 \cdot h \otimes w_2 \cdot h') \end{aligned}$$

We then have, for all $f \in H^*$,

$$\begin{aligned} f(w \cdot [hh']) &= (S^{-1}(w) \cdot f)(hh') = \Delta^*(S^{-1}(w) \cdot f)(h \otimes h') \\ &= \sum \Delta^*(f)(w_1 \cdot h \otimes w_2 \cdot h') \\ &= \sum f([w_1 \cdot h][w_2 \cdot h']) \\ &= f(\sum [w_1 \cdot h][w_2 \cdot h']) \end{aligned}$$

and so $w \cdot (hh') = \sum (w_1 \cdot h)(w_2 \cdot h')$.

Finally, we show that the action commutes. Let $f, g \in H^*$. Then

$$\begin{aligned} (f \otimes g)(\Delta(w \cdot h)) &= \sum f([w \cdot h]_1) g([w \cdot h]_2) = fg(w \cdot h) \\ &= (S^{-1}(w) \cdot fg)(h) = \sum (S^{-1}(w_1) \cdot f)(S^{-1}(w_2) \cdot g)(h) \\ &= \sum (S^{-1}(w_1) \cdot f)(h_1)(S^{-1}(w_2) \cdot g)(h_2) \\ &= \sum f(w_1 \cdot h_1) g(w_2 \cdot h_2) \\ &= (f \otimes g)(w \cdot \Delta(h)) \end{aligned}$$

Thus, equality holds for all elements of $H^* \otimes H^* = (H \otimes H)^*$, so $\Delta(w \cdot h) = w \cdot \Delta(h)$.

For the counit,

$$\varepsilon(w \cdot h) = (S^{-1}(w) \cdot \varepsilon)(h) = (\varepsilon(S^{-1}(w))\varepsilon)(h) = \varepsilon(w)\varepsilon(h)$$

Finally, for the antipode, we have for all $f \in H^*$,

$$\begin{aligned} f(w \cdot S(h)) &= (S^{-1}(w) \cdot f)(S(h)) = S^*(S^{-1}(w) \cdot f)(h) \\ &= (S^{-1}(w) \cdot S^*(f))(h) = S^*(f)(w \cdot h) = f(S(w \cdot h)) \end{aligned}$$

so $w \cdot S(h) = S(w \cdot h)$. This completes the proof. □

Now we see how this fits in with the general theory of L-forms. Let H be a finite dimensional K-Hopf algebra, $K \subseteq L$ a W^*-Galois extension of fields, such that H is a W-module algebra with commuting action. Then, by 6.7, we have a correspondence between commuting actions on H and commuting actions on H^*. We would like this to give a correspondence between forms of H and forms of H^*, but there are two items that must be addressed. First of all, we must figure out what the $(W^{cop})^*$-Galois extensions are. This is answered in the following proposition.

Proposition 6.8. An extension $B \subseteq A$ of commutative K-algebras is right W^*-Galois if and only if it is right $(W^{cop})^*$-Galois.

Proof. Suppose $B \subseteq A$ is a commutative W^*-Galois extension. We show that the action of W on L is a W^{cop}-module algebra action as well. For $w \in W$ and $a, b \in A$, we have

$$w \cdot (ab) = w \cdot (ba) = \sum [w_1 \cdot b][w_2 \cdot a] = \sum [w_2 \cdot a][w_1 \cdot b]$$

so A is a W^{cop}-module algebra. W^{cop} clearly acts trivially on 1, and since the action of W^{cop} is the same as W, it is easy to see that $K \subseteq L$ is $(W^{cop})^*$-Galois by 3.27(ii). The converse follows similarly. □

Thus, any correspondence we get would be between L-forms of H and L-forms of H^*. The second issue involves the fact that 5.18 demands both that W have a commuting action on H and that this action makes $L \otimes H$ a W-module algebra. As was mentioned just before 5.19, this will occur if and only if $\sum (w_1 \cdot l)(w_2 \cdot h) = \sum (w_2 \cdot l)(w_1 \cdot h)$. Of course, this is always true when W is cocommutative.

Question 6.9. If $A \subseteq B$ is a W^*-Galois extension of commutative algebras, must W be cocommutative?

Greither and Pareigis showed this to be the case when $K \subseteq L$ is a separable field extension [GP87, 1.3]. Recall from the remarks following Question 3.31 that if $K \subseteq L$ is W^*-Galois, then W has to be an $\tilde{L}$-form of a group algebra, where $\tilde{L}$ is the normal closure of L. The group involved is a subgroup G of $G(\tilde{L}/K)$. Since KG is cocommutative, so is W. Cohen makes an even stronger conjecture in [Coh94], where she asks whether a noncommutative Hopf algebra can act faithfully on a commutative algebra. She and Westreich get a negative answer to this question in the case where $A \subseteq B$ is an extension of fields and $S^2 \neq id$ [CW93, 0.11].

Recall from 3.28(iv) that in the case where we have an extension of fields, we can interpret Hopf Galois extensions in terms of crossed products. Here we get $L \cong L^H \#_\sigma H^* = K_\sigma(H^*)$, since the action of the crossed product is trivial. So Question 6.9 becomes, replacing H^* with H,

Question 6.10. If $K_\sigma(H)$ is commutative, must H be commutative also?

We get a positive answer in the case of group crossed products, for if $K_\sigma(G)$ is commutative, then $\sigma(g,h)\overline{gh} = \sigma(h,g)\overline{hg}$ for all $g, h \in G$. Thus, $\overline{gh}$ and $\overline{hg}$ are scalar multiples of each other, and so $gh = hg$, making the group commutative. The general case is more difficult, since $K_\sigma(H)$ is commutative $\Leftrightarrow$ for all $h, k \in H$ $\sum \sigma(h_1, k_1)\#h_1k_1 = \sum \sigma(k_1, h_1)\#k_1h_1 \Leftrightarrow \sum \sigma(h_1, k_1)h_1k_1 = \sum \sigma(k_1, h_1)k_1h_1$, and so bases are not particularly helpful.

Let us return to the correspondence of stable L-forms. We can think of L-forms of H in two ways. In light of 5.18, we can think of them as K-subspaces of $L \otimes H$.

Another way is to think of them as Hopf-isomorphism classes of these subspaces. Thus, we can approach the task of finding a correspondence between the stable L-forms of H and H^* from each of these perspectives. Let us begin by assuming that $\mathcal{S}_{L,W}(H)$ is the set of all subspaces of $L \otimes H$ which are stable L-forms of H under W as in 5.18, and similarly for $\mathcal{S}_{L,W^{cop}}(H^*)$. To find a correspondence between stable L-forms of H under W and stable L-forms of H^* under W^{cop}, we define the map $\Phi : \mathcal{S}_{L,W}(H) \to \{\text{subspaces of } L \otimes H^*\}$ as follows. Let $H' \in \mathcal{S}_{L,W}(H)$. Then $H' = [L \otimes H]^W$ for some commuting action of W on $L \otimes H$ which restricts to an action on H. Since $LH' = L \otimes H$, the (trivial) action of W on H' uniquely determines the action of W on H, and so this action is unique. From 6.7 and 6.8, we have a corresponding commuting action of W^{cop} on H^* and $K \subseteq L$ is $(W^{cop})^*$-Galois. We define $\Phi([L \otimes H]^W) = [L \otimes H^*]^{W^{cop}}$.

It is not clear that this map will be a correspondence of stable L-forms (as subspaces). As was mentioned in Question 6.9, it is not certain that commuting actions of W on H which make $L \otimes H$ a W-module algebra correspond to actions of W^{cop} on H^* which make $L \otimes H^*$ a W-module algebra. Thus, $\Phi(H')$ may not be an L-form of H. Similarly, only the commuting actions on H which make $L \otimes H$ a W-module algebra are considered, so it is possible that some forms of H^* will not lie in the image of Φ. Something can still be said in certain cases. We restrict ourselves to a context which includes the case where W and H are both group algebras.

Given a commuting action of W on H, suppose that there exists a basis for H such that, for all $w \in W$, w and $S(w)$ act as transpose matrices on H. This occurs in the case where W and H are group algebras, since if $g \in G(W)$, then g acts

as a permutation of $G(H)$, which is a basis for H. So if we let A_g be the matrix representing the action of g on H, we get $A_g^t = A_g^{-1} = A_{g^{-1}} = A_{S(g)}$, and so g and $S(g)$ act as transpose matrices with respect to the basis $G(H)$.

So suppose that w and $S(w)$ act as transpose matrices with respect to the basis $\{h_1, \cdots, h_n\}$ of H, and let $\{h_1^*, \cdots, h_n^*\}$ be the dual basis in H^*. We then have, for all $w \in W$, $w \cdot h_i = \sum_k a_{ik}(w)h_k$, where $a_{ik} \in W^*$. By assumption, $S(w) \cdot h_i = \sum_k a_{ki}(w)h_k$. If we consider what the corresponding action of W^{cop} on H^* looks like, we have

$$(w \cdot h_i^*)(h_j) = h_i^*(S(w) \cdot h_j) = \sum_k a_{kj}(w)h_i^*(h_k) = a_{ij}(w) = \sum_k a_{ik}(w)h_k^*(h_j)$$

so $w \cdot h_i^* = \sum_k a_{ik}(w)h_k^*$.

Because of the nice relationship between the actions of W on H and W^{cop} on H^*, we get some interesting consequences:

Proposition 6.11. If w and $S(w)$ act as transpose matrices with respect to some basis $\{h_i\}$ of H for all $w \in W$, then an action of W on H makes $L \otimes H$ a W-module algebra if and only if the corresponding action of W^{cop} on H^* makes $L \otimes H^*$ a W^{cop}-module algebra.

Proof. $L \otimes H$ is a W-module algebra $\Leftrightarrow \sum(w_1 \cdot l)(w_2 \cdot h_i) = \sum(w_2 \cdot l)(w_1 \cdot h_i)$ for all $l \in L$, $w \in W$, and $1 \leq i \leq n \Leftrightarrow \sum_k (w_1 \cdot l)a_{ik}(w_2)h_k = \sum_k a_{ik}(w_1)(w_2 \cdot l)h_k \Leftrightarrow \sum a_{ik}(w_2)(w_1 \cdot l) = \sum a_{ik}(w_1)(w_2 \cdot l)$ for each i, k. The same calculations with h_i^* in place of h_i give us the same equivalent conditions for $L \otimes H^*$ being a W^{cop}-module algebra. □

Putting this together with 6.7 gives us a one-to-one correspondence between actions yielding L-forms of H and actions yielding L-forms of H^*. What makes this

especially nice is that we do not need the assumption that W is cocommutative. Similar computations as in 6.11 give us the following:

Proposition 6.12. If w and $S(w)$ act as transpose matrices with respect to the basis $\{h_i\}$, then $\sum_i l_i h_i \in [L \otimes H]^W$ if and only if $\sum_i l_i h_i^* \in [L \otimes H^*]^{W^{cop}}$.

This leads us to the following bijection of subspaces.

Theorem 6.13. Suppose that for all commuting actions of W on H the elements w and $S(w)$ act as transpose matrices with respect to some basis of H for all $w \in W$. Then the map $\Phi : \mathcal{S}_{L,W}(H) \to \mathcal{S}_{L,W}(H^*)$ is a bijection, where we consider $\mathcal{S}_{L,W}(H)$ to be the invariant subspaces of $L \otimes H$ arising from commuting actions on H which make $L \otimes H$ a W-module algebra (similarly for $\mathcal{S}_{L,W^{cop}}(H^*)$).

Proof. By 6.11, $im\Phi = \mathcal{S}_{L,W^{cop}}(H^*)$. We thus need only prove injectivity. Recall that $\Phi([L \otimes H]^W) = [L \otimes H^*]^{W^{cop}}$. For clarity, if the action of W on H is given by $\cdot$, then we write $[L \otimes H]^W = [L \otimes H]^{\cdot W}$ and similarly for H^*. Suppose there are two actions $\cdot$ and $\circ$ on H such that the corresponding actions on H^* give $[L \otimes H^*]^{\cdot W^{cop}} = [L \otimes H^*]^{\circ W^{cop}}$. Let $\sum_i l_i h_i \in [L \otimes H]^{\cdot W}$. By 6.12, we have $\sum_i l_i h_i^* \in [L \otimes H^*]^{\cdot W^{cop}} = [L \otimes H^*]^{\circ W^{cop}}$. Again by 6.12, $\sum_i l_i h_i \in [L \otimes H]^{\circ W}$, so $[L \otimes H]^{\cdot W} \subseteq [L \otimes H]^{\circ W}$. By symmetry, equality holds, and so Φ is injective, and the proof is complete. □

Now we address the question of whether Φ is bijective when considered as a map between isomorphism classes of L-forms. In this case, it is not even clear that Φ is well-defined, since Φ depends on the choice of action. In the case where $W = KG$, something can be said if we assume the transpose condition above. In

this case, there is also a nice matching of actions of W on $L \otimes H$ and $L \otimes H^*$ with the correspondence of L-forms given by 6.6. But we first need a lemma.

Lemma 6.14. Let H be a finite dimensional Hopf algebra which is a W-module algebra such that $L \otimes H$ is also a W-module algebra. Suppose further that w and $S(w)$ act as transpose matrices for all $w \in W$ with respect to the basis $\{h_i\}$ of H. Let $\{h_i^*\}$ be the dual basis in H^*, and suppose that $\sum_i b_i h_i \in [L \otimes H]^W$, $\sum_i c_i h_i^* \in [L \otimes H^*]^{W^{cop}}$. Finally, for each $w \in W$, let $w \cdot h_i = \sum_j a_{ij}(w) h_j$ where $a_{ij} \in W^*$. Then

(i) $\varepsilon(w) b_i = \sum_j a_{ji}(w_2)(w_1 \cdot b_j) = \sum_j a_{ji}(w_1)(w_2 \cdot b_j)$

(ii) $\varepsilon(w) c_i = \sum_j a_{ji}(w_2)(w_1 \cdot c_j) = \sum_j a_{ji}(w_1)(w_2 \cdot c_j)$

(iii) $\delta_{i,k}\varepsilon(w) = \sum_j a_{ji}(w_2) a_{jk}(w_1) = \sum_j a_{ij}(w_2) a_{kj}(w_1)$

Proof. For (i), let $\sum_i b_i h_i \in [L \otimes H]^W$. We have

$$\sum_i \varepsilon(w) b_i h_i = w \cdot \sum_i b_i h_i = \sum_j (w_1 \cdot b_j)(w_2 \cdot h_j) = \sum_{i,j} (w_1 \cdot b_j) a_{ji}(w_2) h_i$$

Thus, $\varepsilon(w) b_i = \sum_j a_{ji}(w_2)(w_1 \cdot b_j)$. If we do the same computations with the equality $\varepsilon(w) b_i h_i = \sum_j (w_2 \cdot b_j)(w_1 \cdot h_j)$, we get the second identity. (ii) follows similarly.

For (iii), we have

$$\varepsilon(w) h_i = \sum w_1 S(w_2) \cdot h_i = \sum_j w_1 \cdot (a_{ji}(w_2) h_j) = \sum_{j,k} a_{ji}(w_2) a_{jk}(w_1) h_k$$

This gives us $\delta_{i,k}\varepsilon(w) = \sum_j a_{ji}(w_2) a_{jk}(w_1)$, which is the first identity in (iii). If we do the same calculations using $\varepsilon(w) = \sum S(w_1) w_2$, we get the second identity. $\square$

Theorem 6.15. Let $W = KG$ with H and L as above, and suppose that $w, S(w)$ act as transpose matrices for all $w \in W$. Let $H' = [L \otimes H]^W$ with corresponding L-form $\bar{H}' = [L \otimes H^*]^W$ of H^*. Then $\bar{H}' \cong (H')^*$.

Proof. Let $\alpha = \sum_i b_i h_i \in [L \otimes H]^W$, $f = \sum_i c_i h_i^* \in [L \otimes H^*]^W$. Define the map $\phi : \bar{H}' \to (H')^*$ by $\phi(f)(\alpha) = \sum_i b_i c_i$. It is clear that ϕ is just the restriction of the isomorphism in 6.6 to $\bar{H}'$. We must first show that $\sum_i b_i c_i \in K$. We have, for each $g \in G$,

$$\begin{aligned}
\sum_i b_i c_i &= \sum_{i,j,k} a_{ji}(g) a_{ki}(g)(g \cdot b_j)(g \cdot c_k), \text{ by 6.14}(i),(ii) \\
&= \sum_{j,k} \delta_{j,k}(g \cdot b_j)(g \cdot c_k), \text{ by 6.14}(iii) \\
&= g \cdot (\sum_j b_j c_j)
\end{aligned}$$

Thus, $\sum_i b_i c_i \in L^W = K$. The fact that ϕ is a K-Hopf algebra isomorphism follows from the fact that the isomorphism in 6.6 is an L-Hopf algebra isomorphism. □

Example 6.16. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$, so $K \subseteq L$ is W^*-Galois, where $W = K\mathbb{Z}_2, \mathbb{Z}_2 =< \tau >$. Let $H = K\mathbb{Z}_n$, with $\mathbb{Z}_n =< \sigma >$. Then the commuting actions of W on H are given by $\tau \cdot \sigma = \sigma^k$, where $k^2 \equiv 1 \pmod{n}$. Let $d = \gcd(k-1, n)$. Now $[L \otimes H]^W$ is spanned by the elements $(1+\tau)\cdot\sigma^j$ and $(1+\tau)\cdot i\sigma^j$, since $1 + \tau \in \int_W^l$. A quick calculation shows that the fixed grouplike elements are $\sigma^{\frac{tn}{d}}$, where $0 \leq t \leq d-1$. The form becomes

$$\begin{aligned}
H_k = span\{\sigma^{\frac{tn}{d}}, \sigma^j + \sigma^{kj}, i\sigma^j - i\sigma^{kj} \quad &: \quad 0 \leq t \leq d-1, 0 \leq j \leq n-1, \\
j \quad &\neq \quad \frac{tn}{d}, j < kj\}
\end{aligned}$$

where $j < kj$ means that if we look at them mod n, we choose j to be the smaller one. This weeds out redundant elements so that the above is a basis. To determine

the Hopf algebra structure, let $c_j = \sigma^j + \sigma^{kj}, s_j = i\sigma^j - i\sigma^{kj}$. Then

$$c_j c_m = c_{j+m} + c_{j+km}, \quad c_j s_m = s_{j+m} - s_{j+km}, \quad s_j s_m = -c_{j+m} + c_{j+km}$$

$$\Delta(c_j) = \frac{1}{2}(c_j \otimes c_j - s_j \otimes s_j), \qquad \Delta(s_j) = \frac{1}{2}(c_j \otimes s_j + s_j \otimes c_j)$$

$$\varepsilon(c_j) = 2, \quad \varepsilon(s_j) = 0, \quad S(c_j) = c_{n-j}, \quad S(s_j) = s_{n-j}$$

We first show that the H_k are mutually nonisomorphic. If $H_k \cong H_l$, we must then have $G(H_k) \cong G(H_l)$. In particular, they must have the same order. But if we look at the basis above, this will only occur when $\gcd(k-1, n) = \gcd(l-1, n)$, since the grouplikes in H_k are contained in $< \sigma >$.

Let $\phi : H_k \to H_l$ be an isomorphism. Define $c'_j \in H_l$ analogously as in H_k. We claim that $\phi(c_j) = c'_{\gamma(j)}, s'_j = s'_{\gamma(j)}$, where γ permutes the j's mod n. Consider $id \otimes \phi : L \otimes H_k \to L \otimes H_l$. An easy computation shows that $G(L \otimes H_k) = \{\frac{1}{2}(c_j + is_j) : 1 \leq j \leq n\}$ and similarly for $G(L \otimes H_l)$. Thus,

$$\phi(c_j) + i\phi(s_j) = (id \otimes \phi)(c_j + is_j) = c'_{\gamma(j)} + is'_{\gamma(j)}$$

for some $1 \leq \gamma(j) \leq n$, and the claim follows.

Now write $n = 2^r n_1 \cdots n_m, n_i = p_i^{s_i}$, where the p_i's are distinct odd primes. Since $k^2 \equiv l^2 \equiv 1 (\text{mod } n)$ then a well-known fact from number theory gives us that $k \equiv \pm 1 (\text{mod } n_i)$, $l \equiv \pm 1 (\text{mod } n_i)$, k and l are odd when $r = 1$, and $k \equiv \pm 1 (\text{mod } 2^{r-1}), l \equiv \pm 1 (\text{mod } 2^{r-1})$ when $r > 1$.

First, suppose that n is odd. If $k \equiv 1 (\text{mod } n_i)$, then n_i divides both $k-1$ and n so $n_i | d$. Thus, $l \equiv 1 (\text{mod } n_i)$. This says that either $k \equiv l \equiv 1 (\text{mod } n_i)$ or $k \equiv l \equiv -1 (\text{mod } n_i)$ for all i. In any case, $k \equiv l (\text{mod } n_i)$ for all i, and so

$k \equiv l (\text{mod } n)$. Since $1 \leq k, l < n$, then $k = l$. A similar argument works for $r = 1$, since we have $k \equiv l \equiv 1 (\text{mod } 2)$.

The final case is when $r > 1$. We assume, for contradiction, that $k \not\equiv l (\text{mod } 2^r)$, since otherwise $k \equiv l (\text{mod } n)$ by the above case. Suppose that $k \equiv 1 (\text{mod } 2^{r-1})$. As before, $l \equiv 1 (\text{mod } 2^{r-1})$. But there are only two possible congruences for k and l mod 2^r: 1 and $2^{r-1} + 1$. Since $k \not\equiv l (\text{mod } 2^r)$, one of them, say k, must be congruent 1 mod 2^r. But then $2^r | k - 1$, so since $\gcd(k-1, n) = \gcd(l-1, n)$, and $2^r | n$, then $2^r | l - 1$. But this implies that $k \equiv l (\text{mod } 2^r)$, which is a contradiction. We must then have $k \equiv l \equiv -1 (\text{mod } 2^{r-1})$.

Without loss of generality, $k \equiv 2^{r-1} - 1 (\text{mod } 2^r)$ and $l \equiv -1 (\text{mod } 2^r)$. Then $l + 1 = m2^r, k + 1 = m'2^{r-1}$, where $m, m' \in \mathbb{Z}$ and m' is odd. Let $c'_j = \phi(c_1)$. We have, by the multiplication tables and the fact that $c_{k+1} = 2\sigma^{k+1}$,

$$\phi(c_2) + 2\phi(\sigma^{k+1}) = \phi(c_1^2) = c_j'^2 = c'_{2j} + 2\sigma^{(l+1)j}$$

Therefore, $\phi(\sigma^{k+1}) = \sigma^{(l+1)j}$ or $\phi(c_2) = 2\sigma^{(l+1)j}$. In the first case, we have $|\sigma^{k+1}| = |\sigma^{(l+1)j}|$. But $|\sigma^{(l+1)j}|$ divides $|\sigma^{l+1}| = |\sigma^{m2^r}|$, which divides $|\sigma^{2^r}|$, an odd number. In contrast, $|\sigma^{k+1}| = |\sigma^{m'2^{r-1}}|$, which is even since m' is odd. This is a contradiction.

Finally, $\phi(c_2) = \sigma^{(l+1)j}$ will only occur when $\frac{1}{2}c_2$ is grouplike. But this forces $\frac{n}{d} | 2$, which implies that $d = \frac{n}{2}$ or n. If $d = n$ then we must have $k = l = 1$. If $d = \frac{n}{2}$, then since $k, l < n$, we must have $k = l = \frac{n+2}{2}$. In either case, $k = l$, so the H_k are mutually nonisomorphic.

Now we look at the dual situation. If we let $\{p_j\}$ be the dual basis to $\{\sigma^j\}$, then we have that W acts on H^* via $\tau \cdot p_j = p_{kj}$ where $k^2 \equiv 1 \text{ (mod } n)$. Let $d =$

$\gcd(k-1,n)$. We get the L-form

$$\bar{H}_k = span\{p_{\frac{tn}{d}}, p_j + p_{kj}, ip_j - ip_{kj} \quad : \quad 0 \leq t \leq d-1, 0 \leq j \leq n-1, \\ j \quad \notin \quad (\frac{tn}{d})\mathbb{Z}, j < kj\}$$

Define $\bar{c}_j = p_j + p_{kj}, \bar{s}_j = ip_j - ip_{kj}$. The multiplication is given by

$$\begin{aligned} \bar{c}_j\bar{c}_m &= (\delta_{j,m} + \delta_{kj,m})\bar{c}_m \\ \bar{c}_j\bar{s}_m &= (\delta_{j,m} + \delta_{kj,m})\bar{s}_m \\ \bar{s}_j\bar{s}_m &= (\delta_{kj,m} - \delta_{j,m})\bar{c}_m \end{aligned}$$

Checking the rest of the Hopf algebra structure of $\bar{H}_k$, we have

$$\Delta(\bar{c}_i) = \frac{1}{2}\sum_j \bar{c}_j \otimes \bar{c}_{i-j} - \bar{s}_j \otimes \bar{s}_{i-j}, \quad \Delta(\bar{s}_j) = \frac{1}{2}\sum_j \bar{c}_j \otimes \bar{s}_{i-j} + \bar{s}_j \otimes \bar{c}_{i-j}$$

$$\varepsilon(\bar{c}_i) = 2\delta_{i,0}, \quad \varepsilon(\bar{s}_i) = 0, \quad S(\bar{c}_i) = \bar{c}_{n-i}, \quad S(\bar{s}_i) = \bar{s}_{n-i}$$

By 6.15, we have that $\bar{H}_k \cong H_k^*$. This is easy to compute directly. If we map $\bar{c}_i \mapsto 2c_i^*$ and $\bar{s}_i \mapsto -2s_i^*$, then one can check that this gives us an isomorphism $\bar{H}_K \to H_k^*$.

Most of the proof of 6.15 can be duplicated for general W. We need only show that $\sum_i b_i c_i \in K$. So we ask

Question 6.17. If $\sum_i b_i h_i \in [L \otimes H]^W, \sum_i c_i h_i^* \in [L \otimes H^*]^{W^{cop}}$, does this imply that $\sum_i b_i c_i \in K$?

This is not obvious in the general case, since 6.14 does not seem to be helpful when W is not a group algebra.

6.3 Adjoint Forms

As mentioned in 5.21, if H is a finite dimensional, semisimple, cocommutative Hopf algebra, and if $K \subseteq L$ is an H^*-Galois extension, then we can obtain a form for H via the adjoint action of H on itself. In addition, we can find a form for H^* using the correspondence of actions given in 6.7. We demonstrate this on KD_{2n}.

Example 6.18. Let ω be a primitive n^{th} root of unity, and let α be a real n^{th} root of 2. Let $K = \mathbb{Q}(\omega + \omega^{-1})$ and $L = K(\alpha, \omega)$. Let $H = KD_{2n}$, where D_{2n} is the dihedral group of order $2n$. Then D_{2n} has a presentation

$$< \sigma, \tau : \sigma^n = 1,\ \tau^2 = 1,\ \tau\sigma\tau^{-1} = \sigma^{-1} >$$

Furthermore, $K \subseteq L$ is H^*-Galois, with the action of D_{2n} on L given by

$$\sigma \cdot \alpha = \omega\alpha, \quad \sigma \cdot \omega = \omega, \quad \tau \cdot \alpha = \alpha, \quad \tau \cdot \omega = \omega^{-1}$$

We obtain a form of H by letting H act on itself via the adjoint action, which gives us $\sigma \cdot \tau = \sigma^2\tau$ and $\tau \cdot \sigma = \sigma^{-1}$. We then compute $H' = [L \otimes H]^H$ to find an L-form of H. Note that this action yields a nontrivial form, since the only group action that yields a trivial form is the trivial action.

Consider the elements $e_k = \frac{1}{n}\sum_{i=0}^{n-1} \omega^{ki}\sigma^i$, $e'_k = \frac{1}{2}\alpha^{2k}e_k\tau$. It is clear that σ fixes e_k, since σ fixes ω and σ. We have

$$\tau \cdot e_k = \frac{1}{n}\sum_{i=0}^{n-1}(\tau \cdot \omega)^{ki}(\tau \cdot \sigma)^i = \frac{1}{n}\sum_{i=0}^{n-1}\omega^{-ki}\sigma^{-i} = \frac{1}{n}\sum_{i=0}^{n-1}\omega^{ki}\sigma^i = e_k$$

and so $e_k \in H'$. For the e'_k, it is clear that they are fixed by τ, since τ fixes α, τ,

and e_k, and so we need only check the action of σ.

$$\begin{aligned}\sigma \cdot e'_k &= \frac{1}{2}(\sigma \cdot \alpha)^{2k}(\sigma \cdot e_k(\sigma \cdot \tau) = \frac{1}{2}\omega^{2k}\alpha^{2k}e_k\sigma^2\tau \\ &= \frac{1}{2}\alpha^{2k}(\frac{1}{n}\sum_i \omega^{k(i+2)}\sigma^{i+2})\tau = \frac{1}{2}\alpha^{2k}e_k\tau = e'_k\end{aligned}$$

so $e_k \in H'$.

We know that $\dim_K H' = 2n$, so for the above elements to span H', we need only show that they are linearly independent. In order to do this, we first show that the e_k's are orthogonal idempotents. We have

$$e_k e_l = (\frac{1}{n}\sum_i \omega^{ki}\sigma^i)(\frac{1}{n}\sum_j \omega^{lj}\sigma^j) = \frac{1}{n^2}\sum_{i,j}\omega^{ki+lj}\sigma^{i+j}$$

Let $0 \leq m \leq n-1$. The coefficient of σ^m is $\frac{1}{n^2}\sum_i \omega^{ki+l(m-i)} = \frac{1}{n^2}\omega^{lm}\sum_i \omega^{i(k-l)}$. But ω^{k-l} is an n^{th} root of unity. Thus, $\sum_i \omega^{i(k-l)} = 0$ unless $k = l$, in which case the coefficient becomes $\frac{1}{n}\omega^{lm}$. Thus,

$$e_k e_l = \delta_{k,l}\frac{1}{n}\sum_{m=0}^{n-1}\omega^{lm}\sigma^m = \delta_{k,l}e_l$$

and so the e_k's are orthogonal idempotents.

This makes proving that $\{e_k, e'_k : 0 \leq k \leq n-1\}$ is a basis pretty easy. If $\sum_k a_k e_k + \sum_k b_k e'_k = 0$ with $a_k, b_k \in K$, then for all $0 \leq j \leq n-1$,

$$0 = e_j(\sum_k a_k e_k + \sum_k b_k e'_k) = \sum_k a_k e_j e_k + \sum_k \frac{1}{2}\alpha^{2k}b_k e_j e_k \tau = a_j e_j + b_j e'_j$$

and so clearly $a_j = b_j = 0$. To finish off the multiplication table, we first compute

$$\tau e_k = \frac{1}{n}\sum_i \omega^{ki}\tau\sigma^i = \frac{1}{n}\sum_i \omega^{ki}\sigma^{-i}\tau = (\frac{1}{n}\sum_i \omega^{(n-k)i}\sigma^i)\tau = e_{n-k}\tau$$

We then have, using the fact that $\alpha^n = 2$,

$$\begin{aligned} e'_k e'_l &= (\frac{1}{2}\alpha^{2k} e_k \tau)(\frac{1}{2}\alpha^{2l} e_l \tau) = \frac{1}{4}\alpha^{2(k+l)} e_k e_{n-l} = \frac{1}{4}\delta_{k+l,n}\alpha^{2n} e_k = \delta_{k+l,n} e_k \\ e_k e'_l &= e_k \alpha^{2l} e_l \tau = \delta_{k,l}\alpha^{2l} e_l \tau = \delta_{k,l} e'_l \\ e'_k e_l &= \frac{1}{2}\alpha^{2k} e_k \tau e_l = \frac{1}{2}\alpha^{2k} e_k e_{n-l}\tau = \frac{1}{2}\delta_{k+l,n}\alpha^{2k} e_k \tau = \delta_{k+l,n} e'_k \end{aligned}$$

This enables us to determine the ring structure of H'. For each $k < \frac{n}{2}$ such that $2k \neq n$ or 0, let $M_k = Ke_k \oplus Ke_{n-k} \oplus Ke'_k \oplus Ke'_{n-k}$. Then $M_k \cong M_2(K)$ as rings via $e_k \mapsto e_{11}, e_{n-k} \mapsto e_{22}, e'_k \mapsto e_{12}, e'_{n-k} \mapsto e_{21}$. If $n = 2k$ or $k = 0$, then consider the ring $R = Ke_k \oplus Ke'_k$. We then have $e_k e'_k = e'_k e_k = e'_k, e_k^2 = e_k'^2 = e_k$, so e_k acts like identity and $R \cong K[\mathbb{Z}_2]$ as rings. For n odd, this gives us

$$H' \cong \bigoplus_{k=1}^{\frac{n-1}{2}} M_2(K) \oplus K[\mathbb{Z}_2]$$

and for n even, we have

$$H' \cong \bigoplus_{k=1}^{\frac{n-2}{2}} M_2(K) \oplus K[\mathbb{Z}_2] \oplus K[\mathbb{Z}_2]$$

For the rest of the Hopf algebra structure, we have for each $0 \leq k \leq n-1$,

$$\begin{aligned} \Delta(e_k) &= \frac{1}{n}\sum_{l=0}^{n-1} \omega^{kl}\sigma^l \otimes \sigma^l = \frac{1}{n^2}\sum_{i=0}^{n-1}\sum_{l=0}^{n-1}\sum_{j=0}^{n-1} \delta_{i,l}\omega^{kl}\sigma^i \otimes \sigma^l \\ &= \frac{1}{n^2}\sum_{i=0}^{n-1}\sum_{l=0}^{n-1}(\sum_{j=0}^{n-1}\omega^{j(i-l)})\omega^{kl}\sigma^i \otimes \sigma^l \\ &= \sum_{j=0}^{n-1}\frac{1}{n}(\sum_{i=0}^{n-1}\omega^{ji}\sigma^i) \otimes \frac{1}{n}(\sum_{l=0}^{n-1}\omega^{(k-j)l}\sigma^l) = \sum_{j=0}^{n-1} e_j \otimes e_{k-j} \\ \varepsilon(e_k) &= \frac{1}{n}\sum_{i=0}^{n-1}\omega^{ki}\varepsilon(\sigma^i) = \frac{1}{n}\sum_{i=0}^{n-1}\omega^{ki} = \delta_{k,0} \\ S(e_k) &= \frac{1}{n}\sum_{i=0}^{n-1}\omega^{ki}\sigma^{-i} = \sum_{i=0}^{n-1}\omega^{(n-k)i}\sigma^i = e_{n-k} \end{aligned}$$

Similarly, we get $\Delta(e'_k) = 2\sum_{j=0}^{n-1} e'_j \otimes e'_{k-j}$, $\varepsilon(e'_k) = \frac{1}{2}\delta_{k,0}$, and $S(e'_k) = e'_k$. This completes our description of the form.

We can also find corresponding forms for H^*. Let the form corresponding to the induced action on H^* be $\bar{H}$. From 6.12, We have the basis

$$\{\bar{e}_k = \sum_i \omega^{ki} p_{\sigma^i},\ \bar{e}'_k = \sum_i \alpha^{2k}\omega^{ki} p_{\sigma^i\tau} : 0 \le k \le n-1\}$$

with multiplication given by $\bar{e}_k\bar{e}_l = \bar{e}_{k+l}, \bar{e}_k\bar{e}'_l = \bar{e}'_l\bar{e}_k = 0, \bar{e}'_k\bar{e}'_l = \bar{e}'_{k+l}$. The Hopf algebra structure is given by

$$\begin{aligned}
\Delta(\bar{e}_k) &= \bar{e}_k \otimes \bar{e}_k + \frac{1}{4}\bar{e}'_k \otimes \bar{e}'_{n-k}, \quad \Delta(\bar{e}'_k) = \bar{e}_k \otimes \bar{e}'_k + \bar{e}'_k \otimes \bar{e}_{n-k} \\
\varepsilon(\bar{e}_k) &= 1, \quad \varepsilon(\bar{e}'_k) = 0 \\
S(\bar{e}_k) &= \bar{e}_{n-k}, \quad S(\bar{e}'_k) = \bar{e}'_k
\end{aligned}$$

Let $Z_1 = \text{span}\{\bar{e}_k\}$ and $Z_2 = \text{span}\{\bar{e}'_k\}$. As algebras, $Z_1 \cong Z_2 \cong K[\mathbb{Z}_n]$. They are both ideals of $\bar{H}$, but only Z_2 is a Hopf ideal.

Bibliography

[BCM86] R.J. Blattner, M. Cohen, and S. Montgomery, *Crossed Products and inner actions of Hopf algebras*, Trans. AMS **298** (1986), 671–711.

[Bel] A.D. Bell, *Comodule algebras and Galois extensions relative to polynomial algebras, free algebras, and enveloping algebras*, Preprint.

[BM94] J. Bergen and S. Montgomery (eds.), *Advances in Hopf Algebras*, Marcel Dekker, New York, 1994.

[CFM90] M. Cohen, D. Fischman, and S. Montgomery, *Hopf Galois extensions*, J. Algebra **133** (1990), 351–372.

[Chi92] W. Chin, *Crossed products of semisimple cocommutative Hopf algebras*, Proc. AMS **116** (1992), 321–327.

[Coh94] M. Cohen, *Quantum commutativity and central invariants*, in Bergen and Montgomery [BM94], pp. 25–38.

[CW93] M. Cohen and S. Westreich, *Central invariants of H-module algebras*, Comm. Alg. **21** (1993), no. 8, 2859–2883.

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

[GP87] C. Greither and B. Pareigis, *Hopf Galois theory for separable field extensions*, J. Algebra **106** (1987), 239–258.

[Hoc54] G. Hochschild, *Representations of restricted Lie algebras of characteristic p*, Proc. AMS **5** (1954), 603–605.

[HP86] R. Haggenmüller and B. Pareigis, *Hopf algebra forms of the multiplicative group and other groups*, Manuscripta Math. **55** (1986), 121–136.

[Jac62] N. Jacobson, *Lie algebras*, Interscience, New York, 1962.

[Jac64] ———, *Lectures in Abstract Algebra*, vol. 3, D. Van Nostrand, Princeton, 1964.

[Knu74] M.A. Knus, *Theorie de la Descente et Algebres d'Azumaya*, Springer-Verlag, New York, 1974.

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

[LS69] R.G. Larson and M. Sweedler, *An associative orthogonal bilinear form for Hopf algebras*, Amer. J. Math. **91** (1969), 75–93.

[McC66] P.J. McCarthy, *Algebraic Extensions of Fields*, Blaisdell, Waltham, Mass., 1966.

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

[Nic94] W.D. Nichols, *Cosemisimple Hopf algebras*, in Bergen and Montgomery [BM94], pp. 135–151.

[Par89] B. Pareigis, *Twisted group rings*, Comm. Alg. **17** (1989), 2923–2939.

[Pas91] D.S. Passman, *A Course in Ring Theory*, Brooks/Cole, Belmont, CA, 1991.

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

[Swe69] M.E. Sweedler, *Hopf Algebras*, Benjamin, New York, 1969.

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

[Ulb82] ———, *Galois erweiterungen von nicht-kommutativen ringen*, Comm. Algebra **10** (1982), 655–672.

[Zhu94] Y. Zhu, *Hopf algebras of prime dimension*, Internat. Math. Res. Notices **1994** (1994), no. 1, 53–59.