Journal of Algebra **239,** 1–34 (2001)
doi:10.1006/jabr.2000.8678, available online at http://www.idealibrary.com on IDEAL®

Forms of Coalgebras and Hopf Algebras

Darren B. Parker[1]

Department of Mathematics and Computer Science, Bemidji State University,

Communicated by Efim Zelmanov

Received August 16, 1997

We study forms of coalgebras and Hopf algebras (i.e., coalgebras and Hopf algebras which are isomorphic after a suitable extension of the base field). We classify all forms of grouplike coalgebras according to the structure of their simple subcoalgebras. For Hopf algebras, given a W^*-Galois field extension $K \subseteq L$ for W a finite-dimensional semisimple Hopf algebra and a K-Hopf algebra H, we show that all L-forms of H are invariant rings $[L \otimes H]^W$ under appropriate actions of W on $L \otimes H$. We apply this result to enveloping algebras, duals of finite-dimensional Hopf algebras, and adjoint actions of finite-dimensional semisimple cocommutative Hopf algebras. © 2001 Academic Press

Key Words: Hopf algebra; coalgebra; descent theory; Galois extension; invariants.

1. INTRODUCTION

Let K be a commutative ring, and let L be a commutative K-algebra. If H is a left K-module, we can form the L-module $L \otimes H$. A natural question to ask in this context is which K-modules H' satisfy $L \otimes H' \cong L \otimes H$ as L-modules.

We can ask the same question for algebras, coalgebras, and Hopf algebras. Specifically,

QUESTION 1.1. *Given K, L as above and a K-object H, what are all the K-objects H' such that $L \otimes H \cong L \otimes H'$ as L-objects?*

Such K-objects H' are called L-forms of H.

Another interesting question arises when we relax the assumption that L be fixed.

[1] I thank my advisor, Donald Passman, for our many conversations which helped me develop the ideas expressed in this paper.

0021-8693/01 $35.00

QUESTION 1.2. *Given a K-object H, what are the K-objects which are L-forms of H for some suitable commutative K-algebra L?*

For instance, [HP86] defines a form of H to be an L-form of H for some faithfully flat commutative K-algebra L. We can define forms in other contexts, as long as we specify what is meant by a "suitable commutative K-algebra."

Question 1.2 was addressed in [HP86]. Their interest was finding Hopf algebra forms of group rings KG. They found a correspondence between Galois extensions of the base ring with Galois group $F = \mathrm{Aut}(G)$ and Hopf algebra forms of KG in the case of G finitely generated and F finite. The Hopf algebra form was derived from the invariants of certain actions of KF on LG, where $K \subseteq L$ is an "F-Galois" extension. The definition of Galois is slightly different in this paper. An F-Galois extension in [HP86] is actually a KF^*-Galois extension in current terminology.

Question 1.1 was addressed in [Par89] for group algebras. Given $K \subseteq L$ a KF^*-Galois extension and given a group action of F on G, he constructed the twisted group ring $K_\Gamma G$. He showed that $K_\Gamma G$ is an L-form of KG and that in the case of L connected, all L-forms of KG are twisted group rings for some action of F on G.

In this paper, we address these questions when K and L are fields. In Section 3, we look at the case where H is a grouplike coalgebra KG. We classify all coalgebra forms of KG according to the structure of their simple subcoalgebras. Specifically, a coalgebra H is a form of a grouplike coalgebra with respect to fields if and only if it is cocommutative and semisimple and the duals of its simple subcoalgebras are separable field extensions of K.

In Section 4, we address Question 1.1 for Hopf algebras. We fix the field extension $K \subseteq L$ and assume this extension to be W^*-Galois for some finite-dimensional semisimple K-Hopf algebra W. We use actions of W on $L \otimes H$ and the invariants under these actions to find L-forms of H. We get Theorem 4.1, which says that all the L-forms of H are determined by W-actions on $L \otimes H$ which commute with comultiplication, counit, and the antipode. Furthermore, the L-form we get from such an action is the set of invariants in $L \otimes H$ under the action of W.

In Section 5, we use Theorem 4.1 to find L-forms of $U(\mathfrak{g})$ in characteristic zero and $u(\mathfrak{g})$ in characteristic $p > 0$. It turns out that such forms are merely enveloping algebras of Lie algebras which are L-forms of $\mathfrak{g}$. Furthermore, the L-forms of $\mathfrak{g}$ are found by appropriate actions on $L \otimes \mathfrak{g}$. We use this to compute the L-forms of an interesting class of examples.

In Section 6, we apply Theorem 4.1 to duals of finite-dimensional Hopf algebras. We get an interesting correspondence between W-actions on H

and W^{cop}-actions on H^*. We use this correspondence to get Theorems 6.1 and 6.2, which give us a correspondence between L-forms of H and L-forms of H^* from different perspectives.

Finally, in Section 7, we compute an example of an L-form obtained from the adjoint action of H on itself and then compute the corresponding form of H^*.

I thank the referee for many helpful insights and comments. In particular, the referee is responsible for the proof of Proposition 2.2, which appeared in the original version of this paper as a conjecture.

2. PRELIMINARIES

Our basic notation comes from [Mon93, Swe69]. The ground field is always K, and tensor products are assumed to be over K unless otherwise specified.

A coalgebra is a K-vector space H with linear maps $\Delta: H \to H \otimes H$, $\varepsilon: H \to K$, called the comultiplication and counit, respectively, which satisfy $(\mathrm{id} \otimes \Delta) \circ \Delta = (\Delta \otimes \mathrm{id}) \circ \Delta$, $(\mathrm{id} \otimes \varepsilon) \circ \Delta = \mathrm{id} \otimes 1$, and $(\varepsilon \otimes \mathrm{id}) \circ \Delta = 1 \otimes \mathrm{id}$. We use the Sweedler summation notation $\Delta(h) = \sum_{(h)} h_1 \otimes h_2$. A bialgebra is a coalgebra and an associative algebra with unit such that Δ, ε are algebra homomorphisms. A Hopf algebra is a bialgebra with a map $S: H \to H$ satisfying $\varepsilon(h) 1_H = \sum_{(h)} S(h_1) h_2 = \sum_{(h)} h_1 S(h_2)$. This is equivalent to S being the inverse of id under the convolution product on $\mathrm{Hom}_K(H, H)$ (see [Mon93, 1.4.1, 1.5.1]).

The canonical examples of Hopf algebras are the group algebra KG and the universal and restricted enveloping algebras $U(\mathfrak{g})$ and $u(\mathfrak{g})$. For KG we define $\Delta(\mathfrak{g}) = g \otimes g$, $\varepsilon(g) = 1$, $S(g) = g^{-1}$ for each $g \in G$, and for the enveloping algebras, we define $\Delta(x) = 1 \otimes x + x \otimes 1$, $\varepsilon(x) = 0$, $S(x) = -x$ for all $x \in \mathfrak{g}$.

DEFINITION 2.1. Let L be a commutative K-algebra, and let H be 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 "coalgebra," "Hopf 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.

EXAMPLE 2.1 [HP86]. Let $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$. Let $H = K\mathbb{Z}$, $H' = K\langle c, s: c^2 + s^2 = 1, cs = sc \rangle$ with Hopf algebra structure $\Delta(c) = c \otimes c - s \otimes s$, $\Delta(s) = s \otimes c + c \otimes s$, $\varepsilon(c) = 1$, $\varepsilon(s) = 0$, $S(c) = c$, $S(s) = -s$. H' 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 $a^{-1} = c - is$. We have $a + a^{-1} = 2c$, so $c \in L\langle a, a^{-1}\rangle$. Similarly, $s \in L\langle a, a^{-1}\rangle$. Thus $L \otimes H' = L\langle a, a^{-1}\rangle \cong L\mathbb{Z}$, so H and H' are L-forms.

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

DEFINITION 2.2. Let $\mathscr{X}$ 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 $\mathscr{X}$ if H' is an L-form of H for some $L \in \mathscr{X}$

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

If H is a coalgebra (resp. Hopf algebra), then $L \otimes H$ has a natural coalgebra (resp. Hopf algebra) structure (see [Mon93, p. 21]), so we may talk about forms of coalgebras and Hopf algebras. We have a canonical correspondence between L-forms of H and L-forms of H^*.

PROPOSITION 2.1. *Let H be a finite-dimensional Hopf algebra over a field K with $K \subseteq L$ a field extension. Then*

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

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

Proof. We define a map $\phi\colon L \otimes H^* \to (L \otimes H)^*$ by $\phi(a \otimes f)(b \otimes h) = f(h)ab$ for all $a, b \in L$, $h \in H$, $f \in H^*$. It is straightforward to show that this is an L-Hopf algebra isomorphism. This gives us (i), and (ii) follows directly. ∎

We will need the notion of Hopf Galois extensions. Let H be a Hopf algebra, with A a right H-comodule algebra. That is, we have an algebra map $\rho\colon A \to A \otimes H$ such that $(\rho \otimes \mathrm{id}) \circ \rho = (\mathrm{id} \otimes \Delta) \circ \rho$ and $(\mathrm{id} \otimes \varepsilon) \circ \rho = 1 \otimes \mathrm{id}$. Let $A^{\mathrm{co}\,H} = \{a \in A : \rho(a) = a \otimes 1\}$ denote the coinvariants of A. An extension $B \subseteq A$ of right H-comodule algebras is right H-Galois if $B = A^{\mathrm{co}\,H}$ and the map $\beta\colon A \otimes_B A \to A \otimes_K H$ given by $\beta(a \otimes b) = (a \otimes 1)\rho(b) = \sum ab_0 \otimes b_1$ is bijective.

PROPOSITION 2.2. *Let $B \subseteq A$ be a right H-Galois extension of commutative algebras. Then H is commutative.*

Proof. Since A is commutative, it is easy to show that β is an algebra homomorphism. Since β is bijective, it is an isomorphism, so $A \otimes H$ is commutative. Thus, H is commutative. ∎

If H is finite dimensional, then we can define Hopf Galois extensions in terms of actions. Let A be an H-module algebra. That is, for all $a, b \in A$, $h \in H$, we have $h \cdot (ab) = \sum (h_1 \cdot a)(h_2 \cdot b)$ and $h \cdot 1_A = \varepsilon(h)1_A$. Then H^*

is also a Hopf algebra and A is an H^*-comodule algebra with $A^{\mathrm{co}\, H^*} = A^H = \{a \in A : h \cdot a = \varepsilon(h)a\}$ (see [Mon93, 1.6.4, 1.7.2]). We get the following.

THEOREM 2.1 [KT81, Ulb82]. *Let H be a finite-dimensional Hopf algebra, and let A be a left H-module algebra. The following are equivalent*:

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

(ii) *The map π: $A\#H \to \mathrm{End}(A_{A^H})$ 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 $0 \neq t \in \int_H^l = \{k \in H : hk = \varepsilon(h)k$ for all $h \in H\}$, then the map $[,]$: $A \otimes_{A^H} A \to A\#H$ given by $[a, b] = atb$ is surjective ($\int_H^l$ is called the space of left integrals).*

The associative algebra $A\#H$ mentioned above is $A \otimes H$ as a vector space. The simple tensors are written $a\#h$, and multiplication is given by $(a\#h)(b\#k) = \sum a(h_1 \cdot b)\#h_2 k$ (see [Mon93, 4.1.3]).

Note that (ii) implies that H acts faithfully on A. Also, in light of Proposition 2.2, we have that if $B \subseteq A$ is an H^*-Galois extension of commutative rings, then H must be cocommutative. This makes Proposition 2.2 a weaker version of a conjecture in [Coh94], where Cohen 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 $S^2 \neq \mathrm{id}$[CW93, 0.11].

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

THEOREM 2.2 [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.*

(iv) *$D \cong D^H \#_\sigma H^*$.*

Note that (ii) implies that, for a finite group G, a field extension is KG^*-Galois if and only if it is classically Galois with Galois group G. Now look at $H = u(\mathfrak{g})$.

EXAMPLE 2.2. Let $K \subseteq L$ be a purely inseparable finite field extension of characteristic p and exponent ≤ 1 (i.e., $a^p \in K$ for all $a \in L$), with K the base field. Since $\mathrm{Der}_K(L)$ is finite dimensional over L, then there exists a finite p-basis of L over K [Jac64, p. 182] (i.e., a finite set $\{a_1, \dots, a_n\}$ such that $\{a_1^{m_1} \cdots a_n^{m_n} : 0 \leq m_i < p\}$ is a basis of $K \subseteq L$). For each i, we define a derivation δ_i such that $\delta_i(a_j) = \delta_{i,j}$. Then $\mathfrak{g} = K$-span

$\{\delta_i : 1 \leq i \leq n\}$ is a restricted Lie algebra, and in fact $\mathrm{Der}_K(L) = L\mathfrak{g} \cong L \otimes \mathfrak{g}$. In particular, $\mathrm{Der}_K(L)$ is an abelian restricted Lie algebra and L is a $u(\mathfrak{g})$-module algebra. Then $K = L^{u(\mathfrak{g})}$ and $\dim_K(u(\mathfrak{g})) = p^n = [L:K]$. Thus, $K \subseteq L$ is a $u(\mathfrak{g})^*$-Galois extension by Theorem 2.2(ii).

In fact, more can be said.

THEOREM 2.3. *Supose that $K \subseteq L$ is a finite field extension of characteristic $p > 0$. Then $K \subseteq L$ is a $u(\mathfrak{g}')^*$-Galois extension for $\mathfrak{g}'$ a restricted Lie algebra if and only if $K \subseteq L$ is purely inseparable of exponent ≤ 1, and $\mathfrak{g}'$ is an L-form of $\mathfrak{g}$, where $\mathfrak{g}$ is as in Example* 2.2.

Proof. Suppose that $K \subseteq L$ is a $u(\mathfrak{g}')^*$-Galois extension, where $\mathfrak{g}'$ is some restricted Lie algebra. For each $a \in L$, $x \in \mathfrak{g}'$, we have $x \cdot a^p = pa^{p-1}(x \cdot a) = 0$, so $a^p \in K$. Thus, $K \subseteq L$ is purely inseparable of exponent ≤ 1. By Theorem 2.1(ii), we have a Lie embedding $\pi\colon L \otimes \mathfrak{g}' \hookrightarrow \mathrm{Der}_K(L) \cong L \otimes \mathfrak{g}$. Since $\dim_K(u(\mathfrak{g}')) = [L:K] = \dim_K(u(\mathfrak{g}))$, then $\dim_K(\mathfrak{g}') = \dim_K(\mathfrak{g})$, and so $\pi|_{L\otimes\mathfrak{g}'}$ is actually a Lie isomorphism. Thus, $\mathfrak{g}$ and $\mathfrak{g}'$ are L-forms.

Conversely, suppose that $K \subseteq L$ is purely inseparable of exponent ≤ 1, and that $\phi\colon L \otimes \mathfrak{g}' \to L \otimes \mathfrak{g} \cong \mathrm{Der}_K(L)$ 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. We have $K = L^{\mathfrak{g}} = L^{L\otimes\mathfrak{g}} = L^{L\otimes\mathfrak{g}'} = L^{\mathfrak{g}'}$. By Theorem 2.2, we are done. ∎

If we look ahead to Proposition 5.1, $u(\mathfrak{g})$ and $u(\mathfrak{g}')$ are L-forms if and only if $\mathfrak{g}$ and $\mathfrak{g}'$ are L-forms. Thus, Theorem 2.3 says that if $K \subseteq L$ is $u(\mathfrak{g})^*$-Galois, it is also H^*-Galois for all forms H of $u(\mathfrak{g})$.

Theorem 2.3 invites the following question.

QUESTION 2.3. *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. They showed 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 2.3 [GP87]. Let $K = \mathbb{Q}$, $L = K(\omega)$, where ω is a real fourth root of 2. Then $K \subseteq L$ is H^*-Galois, where $H = K\langle c, s : c^2 + s^2 = 1, cs = sc = 0\rangle$. We have $g = c + is \in G(\tilde{L} \otimes H)$, and $o(g) = 4$. Thus, H is an $\tilde{L}$-form of $K\mathbb{Z}_4$. 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.

We will often be interested in the case where H is semisimple. When H is finite dimensional, this is true if and only if $\varepsilon(\int_H^l) \neq 0$ [LS69; Mon93, 2.2.1]). This enables us to show that semisimplicity is a property shared by L-forms.

PROPOSITION 2.3. *Let H be a finite-dimensional K-Hopf algebra with $K \subseteq L$ an extension of fields. Then $\int_{L\otimes H}^{l} = L \otimes \int_{H}^{l}$. In particular, if H' is an L-form of H, then H' is semisimple if and only if H is semisimple.*

Proof. By [Mon93, 2.1.3], $\int_{L\otimes H}^{l}$ is one dimensional over L and $\int_{H}^{l}$ is one dimensional over K. It thus suffices to show that $L \otimes \int_{H}^{l} \subseteq \int_{L\otimes H}^{l}$. This is an easy computation. ∎

If M is an H-module, this characterization of semisimplicity gives us a nice way to compute M^H when H is semisimple.

PROPOSITION 2.4. *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 $m \in M^H$. Then $\varepsilon(t)m = t \cdot m$. Since $\varepsilon(t) \neq 0$, then $m = t \cdot (\frac{1}{\varepsilon(t)} m) \in t \cdot M$, and we are done. ∎

3. 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. A grouplike coalgebra is a coalgebra with basis $\{g_i\}$ such that $\Delta(g_i) = g_i \otimes g_i$, $\varepsilon(g_i) = 1$. It thus has the same coalgebra structure as a group algebra. Recall that for any coalgebra H, $G(H) = \{h \in H : \Delta(h) = h \otimes h,\ h \neq 0\}$.

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 (see [Mon93, 1.2.3, 9.1.2]). Let $\{\alpha_1, \dots, \alpha_n\}$ be a basis for L over K with $\alpha_j \alpha_k = \sum_l c_{jkl} \alpha_l$, $c_{jkl} \in K$, and let $\{a_1, \dots, a_n\}$ be the dual basis in L^*. An easy computation gives us $\Delta(a_k) = \sum_{i,j} c_{ijk} a_i \otimes a_j$, $\sum_i \varepsilon(a_i)\alpha_i = 1$.

LEMMA 3.1. *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 a surjective morphism of coalgebras. We then have the algebra monomorphism $\phi^*: D^* \to L^{**} \cong L$. Let E be the image of D^* in L. Then E is a finite-dimensional K-subalgebra of L, so E is a field. Since $E \cong D^*$ as fields, $D \cong E^*$ as coalgebras.

Conversely, suppose $D \cong E^*$ for E a field contained in L, and consider the inclusion map $i: E \to L$. The map $i^*: L^* \to E^* \cong D$ is a surjective coalgebra morphism. ∎

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 $g = \sum \alpha_i \otimes h_i \in G(L \otimes H)$, then in some sense the α_i and h_i are dual to each other.

LEMMA 3.2. *Let* $g = \sum_i \alpha_i \otimes h_i \in G(L \otimes H)$.

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

(ii) *If we have the hypothesis as in* (i), *and if also the* α_i *are algebraic over* K, *then* D *is a simple subcoalgebra.*

(iii) *If* $h_1, \dots, h_n$ *are the nonzero* h_i *and are linearly independent, 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,* $K[\alpha_1, \dots, \alpha_n]$ *is finite dimensional, and therefore is a finite field extension.*

(iv) *Conversely, if we have* $\{\alpha'_1, \dots, \alpha'_n\} \in L$ *and* $\{h'_1, \dots, h'_n\}$ *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

$$\sum_k \alpha_k \otimes \Delta(h_k) = \Delta(g) = g \otimes g = \sum_{i,j} \alpha_i \alpha_j h_i \otimes h_j \tag{1}$$

If $\alpha_i \alpha_j = \sum_k c_{ijk} \alpha_k$, and the α_i are linearly independent, then we have $\sum_{i,j} \alpha_i \alpha_j h_i \otimes h_j = \sum_{i,j,k} c_{ijk} \alpha_k \otimes h_i \otimes h_j$, and therefore $\Delta(h_k) = \sum_{i,j} c_{ijk} h_i \otimes h_j$ by (1). This gives us (i).

If the α_i are algebraic over K, then let $\{\alpha_1, \dots, \alpha_n\}$ 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 $E = K(\alpha_1, \dots, \alpha_n)$. Thus, D is a morphic image of E^* and so is simple by Lemma 3.1. 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 (1) and so we have (iii).

Finally, (iv) follows from a computation almost identical to those above. ∎

LEMMA 3.3. *Let* $K \subseteq L$ *be any field extension, and let* $\overline{K}$ *be the algebraic closure of* K. *For each* $g \in G(L \otimes H)$, *there is a simple subcoalgebra* $H_g \subseteq H$ *such that* $g \in \overline{K} \otimes H_g$.

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 $D = \operatorname{span}\{h_i\}$. Then $g \in L \otimes D$. Also, D is a finite-dimensional coalgebra by Lemma 3.2(i).

Now let $\{v_1, \dots, v_n\}$ be a basis for D. Write $g = \sum_i \beta_i \otimes v_i$ with $\beta_i \in L$. By Lemma 3.2(iii), $K[\beta_1, \dots, \beta_n]$ is a finite field extension, and so each β_i is algebraic over K. Thus, $g \in \overline{K} \otimes D$.

But now we can write $g = \sum_i \gamma_i \otimes w_i$, where the γ_i are linearly independent in $\overline{K}$. By Lemma 3.2(ii), $H_g = \operatorname{span}\{w_i\}$ is a simple coalgebra. Since $g \in \overline{K} \otimes H_g$, then the proof is complete. ∎

COROLLARY 3.1. *If a coalgebra H is an L-form of KG, then it is a $\overline{K}$-form of KG.*

This leads us to the main theorem.

THEOREM 3.1. *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 coalgebra.*

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

Note. A coalgebra is said to have separable coradical if, for each simple subcoalgebra D, we have that D^* is a separable K-algebra (the coradical is the sum of all simple subcoalgebras). 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 $G = G(L \otimes H)$. Clearly, H must be cocommutative. By Corollary 3.1, we can assume that L is algebraic over K. By Lemma 3.3, each $g \in G$ is contained in $L \otimes H_g$ for some simple subcoalgebra $H_g \subseteq H$. We then have

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

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

We now take care of the case where H is a simple coalgebra. By Lemma 3.1, H^* is isomorphic to some finite field extension of K in $\overline{K}$. Let $E \cong H^*$ be any such field, and let $\{\alpha_1, \dots, \alpha_n\}$ be a basis for E over K, and let $\{h_1, \dots, h_n\}$ be 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 $\sum_i \alpha_i \otimes h_i$ is a grouplike element by Lemma 3.2(iv). Since $L \otimes H$ is a grouplike coalgebra, then $g \in L \otimes H$. 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 $\overline{K}$. This implies that L contains the normal closure of H^* in $\overline{K}$.

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 $L \otimes H$. By Lemma 3.2(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 $E \to K(\alpha'_1, \dots, \alpha'_n)$. Thus, we get a distinct grouplike element of $L \otimes H$ for every distinct isomorphism from E onto subfields of L. By [McC66, Theorem 20], the number of such isomorphisms is equal to the degree of separability of E over K. Since H has $\dim_K(H) = \dim_K(E)$ such grouplike elements, then $E \cong H^*$ is separable over K.

For the general case, since H is cosemisimple, we can write $H = \oplus_i H_i$, where H_i are the distinct simple subcoalgebras of H. By Lemma 3.2(ii), each grouplike element of $L \otimes H$ sits in some $L \otimes H_i$. Thus, $G(L \otimes H) = \bigcup_i G(L \otimes H_i)$. But then it follows that each $L \otimes H_i$ is spanned by grouplike elements. By the simple case, each H_i^* is separable over K, and L contains the normal closure of H_i^*.

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, then $H = \oplus_i H_i$, where each H_i is simple. It suffices to show that each $L \otimes H_i$ is spanned by grouplike elements, and so, without loss of generality, H is simple.

Since H^* is separable and L contains the normal closure of H^*, then there are $\dim_K(H^*)$ distinct isomorphisms of H^* onto subfields of L. By Lemma 3.2(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]). Any Hopf algebra is pointed when the base field is algebraically closed (see [Mon93, 5.6]). If we let $L = \overline{K}$, this will make $L \otimes H$ pointed. Thus, $L \otimes H$ is a group algebra, and so any cocommutative cosemisimple Hopf algebra is a form of a group algebra. By Theorem 3.1, 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 3.2. *Let H be a finite-dimensional cocommutative cosemisimple Hopf algebra. Then H is semisimple if and only if* $\operatorname{char}(K) = 0$ *or* $\operatorname{char}(K)$ *does not divide* $\dim_K(H)$.

Proof. Let $L = \overline{K}$. By the above remarks, $L \otimes H \cong LG$, where G is a group. By Proposition 2.3, H is semisimple if and only if KG is. By

Maschke's theorem, this occurs if and only if either $\mathrm{char}(K) = 0$ or $\mathrm{char}(K)$ does not divide $|G| = \dim_K(H)$. ∎

Theorem 3.1 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, 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 3.3. *Let H be an L-form of KG, where $K \subseteq L$ is either a purely inseparable or purely transcendental extension. Then $H \cong KG$.*

Proof. By Theorem 3.1, H is cosemisimple with separable coradical. Let C be a simple subcoalgebra of H. Then C^* is a separable field extension of K. By the remarks above, we must have $C^* \hookrightarrow L$. But if L is purely inseparable, then this forces $C^* \cong K$. Thus, every simple subcoalgebra of H is one dimensional, and so H is pointed. But H is also cosemisimple, so H is a grouplike coalgebra. Thus, $H \cong KG$. For L purely transcendental, the result follows from Corollary 3.1. ∎

COROLLARY 3.4. *Let H be a cocommutative coalgebra, and suppose that $K \subseteq L$ is such that $L \otimes H$ is pointed (e.g., $L = \overline{K}$). Let $\{H_n\}_{n=0}^{\infty}$ be the coradical filtration of H (see [Mon93, 5.2]).*

(i) *$[L \otimes H]_n \subseteq L \otimes H_n$ for all $n \geq 0$.*

(ii) *Equality holds for all $n \geq 0$ if and only if H has separable coradical.*

Proof. For (i), since $L \otimes H$ is pointed, then $[L \otimes H]_0$ is spanned by grouplike elements. Since each grouplike element $g \in L \otimes H_g \subseteq L \otimes H_0$, where H_g is as in Lemma 3.3, then $[L \otimes H]_0 \subseteq L \otimes H_0$. This takes care of $n = 0$. For $n > 0$, we have, by induction,

$$\begin{aligned}(L \otimes H)_n &= \Delta^{-1}([L \otimes H] \otimes_L [L \otimes H]_{n-1} + [L \otimes H]_0 \otimes_L [L \otimes H]) \\ &\subseteq \Delta^{-1}(L \otimes H \otimes H_{n-1} + L \otimes H_0 \otimes H) \\ &= L \otimes \Delta^{-1}(H \otimes H_{n-1} + H_0 \otimes H) = L \otimes H_n.\end{aligned}$$

For (ii), we first note that H_0 is a cosemisimple, cocommutative coalgebra. If H does not have separable coradical, then, by Theorem 3.1, $L \otimes H_0$ is not grouplike. Since $[L \otimes H]_0$ is a grouplike coalgebra, equality cannot hold.

If H does have separable coradical, then Theorem 3.1 tells us that $L \otimes H_0$ is a grouplike coalgebra and thus cosemisimple. Then $L \otimes H_0 \subseteq [L \otimes H]_0$. Thus, $L \otimes H_0 = [L \otimes H]_0$ if and only if H has separable coradical. To prove (ii), therefore, we need only show that if H has separable coradical, then $L \otimes H_n \subseteq [L \otimes H]_n$ for all n. This follows by induction as in (i). ∎

For the next corollary, we need the following.

THEOREM 3.2 [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.*

COROLLARY 3.5. *Let H be a cocommutative Hopf algebra. If H has separable coradical, then H_0 is a sub Hopf algebra. 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 $L = \overline{K}$. 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 Corollary 3.4, $L \otimes H_0 = (L \otimes H)_0$. Since $L \otimes H_0$ is a Hopf algebra, then H_0 is a Hopf algebra as well.

If H_0 is a finite-dimensional cocommutative Hopf algebra, then H_0^* is a finite-dimensional commutative semisimple Hopf algebra. By Theorem 3.2, $L \otimes H_0^* \cong (LG)^*$ as Hopf algebras. But $L \otimes H_0^* \cong (L \otimes H_0)^*$, so $L \otimes H_0 \cong LG$. This implies, by Theorem 3.1, that H_0 has separable coradical and thus so does H. ∎

We get one final corollary.

COROLLARY 3.6. *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 $L = \overline{K}$. By [Zhu94] $L \otimes H$ is a group algebra. By Theorem 3.1, H is cosemisimple with separable coradical. If we apply the above to H^*, then H^* is cosemisimple, and so H is semisimple. ∎

4. 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. For the main result, we will have $K \subseteq L$ a W^*-Galois extension of fields for some Hopf algebra W. Recall from Proposition 2.2 that this implies that W is cocommutative.

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 $h \in H$.

LEMMA 4.1. *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, 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, then we have a contradiction. This gives us (i), and (ii) follows immediately. ∎

This lemma allows us to look at elements of $[L \circ A]^W \otimes [L \circ A]^W$ as elements of $[L \circ A] \otimes_L [L \circ A]$. 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 4.2. *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. *Then there exist elements* $a_i, b_i \in L$ *such that*

(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. By Theorem 2.1(iii) there exist $a_i, b_i \in A$ such that $\sum_i a_i t b_i = 1$. Let $w \in W$. Then we have, by the definition of multiplication in $L\#W$,

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

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

This gives us (i). For (ii), we have from (i) 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, then we have $\Sigma_i(t'_j \cdot a_i)(t_k \cdot b_i) = \delta_{j,k}$. ∎

In the main theorem, we will use certain actions of W on $L \circ H$ to obtain L-forms of H. These actions must "respect" the Hopf algebra structure of $L \otimes H$.

DEFINITION 4.1. An action of W on $L \circ H$ is a commuting action if it commutes with the comultiplication, counit, and the antipode of $L \otimes H$. In other words, $\Delta(w \cdot lh) = w \cdot \Delta(lh)$, $\varepsilon(w \cdot lh) = w \cdot \varepsilon(lh)$, and $S(w \cdot lh) = w \cdot S(lh)$.

When the action on $L \circ H$ restricts to an action on H, we get

PROPOSITION 4.1. *Let W and H be Hopf algebras, and let H be a W-module algebra. Suppose $K \subseteq L$ is a field extension with L a W-module algebra. Then $L \circ H$ is a W-module algebra, and this action is a commuting action if and only if it commutes with the comultiplication, counit, and the antipode in H.*

We are now ready for the main result.

THEOREM 4.1. *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 $L \circ H$ such that the action restricted to L is the Galois action. Then*

(i) *$H' = [L \circ H]^W$ is a K-Hopf algebra.*

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

(iii) *If F is another Hopf algebra L-form of H, then there is some commuting action of W on $L \circ H$ which restricts to the Galois action on L 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 $\Sigma_i a_i t b_i = 1$ in $L\#H$. Also write $\Delta(t) = \Sigma_j t_j \otimes t'_j$, where $\{t'_j\}$ is a basis for W with $t'_1 = 1$. For (i), it suffices to show that $\Delta(H') \subseteq H' \otimes H'$, $\varepsilon(H') \subseteq K$, and $S(H') \subseteq H'$. By Proposition 2.4, $[L \circ H]^W$ is spanned over K by elements of the form $t \cdot lh$.

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

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

In addition, $\Sigma_i(t \cdot [b_i h_1]) \otimes (t \cdot [la_i h_2]) \in H' \otimes H'$. If we identify this element with its image in $[L \circ H] \otimes_L [L \circ H]$ (which we can do by Lemma

4.1), then, using Lemma 4.2(ii),

$$\begin{aligned}
&\sum_i (t \cdot [b_i h_1]) \otimes (t \cdot [la_i h_2]) \\
&\qquad = \sum_{i,j,k,m} (t_k \cdot b_i)(t'_k \cdot h_1) \otimes (t_j \cdot l)(t'_m \cdot a_i)(t''_{jm} \cdot h_2) \\
&\qquad = \sum_{i,j,k,m} (t'_m \cdot a_i)(t_k \cdot b_i)(t_j \cdot l)(t'_k \cdot h_1) \otimes (t''_{jm} \cdot h_2) \\
&\qquad = \sum_{j,k,m} \delta_{m,k}(t_j \cdot l)(t'_k \cdot h_1) \otimes (t''_{jm} \cdot h_2) \\
&\qquad = \sum_{j,k} (t_j \cdot l)(t'_k \cdot h_1) \otimes (t''_{jk} \cdot h_2).
\end{aligned}$$

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

In addition, we have $\varepsilon(t \cdot lh) = t \cdot \varepsilon(lh) \in L^W = K$, and $S(t \cdot lh) = t \cdot S(lh) \in [L \circ H]^W$, so $\varepsilon(H') \subseteq K$ and $S(H') \subseteq H'$. This gives us (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 Lemma 4.2(ii),

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

Since $L \otimes H$ is spanned over L by H, then the map is surjective. Injectivity follows from Lemma 4.1(i).

For (iii), suppose that F is an L-form of H, so $L \otimes H \cong L \otimes F$. Let $\Phi: L \otimes F \to L \otimes H$ be an L-Hopf algebra isomorphism. We define an action of W on $L \otimes F$ by $w \cdot lf = (w \cdot l)f$ for all $l \in L$ and $f \in F$. It is easy to check that this makes $L \circ F$ a W-module algebra, and that $F = [L \circ F]^W$. For $\alpha \in L \otimes H$, we define $w \cdot \alpha = \Phi(w \cdot \Phi^{-1}(\alpha))$.

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

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

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

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

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

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

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, Theorem 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 4.1 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, Theorem 5]. Neither result assumed the Galois extensions to be fields.

We now consider some examples.

EXAMPLE 4.1. 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 canonical action of W on H induces a commuting action on $L \otimes H$, where $K \subseteq L$ is W^* Galois. Thus, this action yields an L-form of H.

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 $a \in A$, $g \in G$, 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 4.2. Let H be finite dimensional, semisimple, and cocommutative, and consider the left adjoint action of H on itself. Then for all h, $k \in H$,

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

The counit and antipode commute as well, using the fact that $S^2 = \mathrm{id}$ for cocommutative coalgebras and $\varepsilon \circ S = \varepsilon$ [Mon93, 1.5.10, 1.5.12]. 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 4.3. Let $K = \mathbb{Q}$, $L = K(i)$. Let $H = K[x]$, the universal enveloping algebra of the one-dimensional Lie algebra. If $W = KG$, where $G = \mathbb{Z}_2 = \langle \sigma \rangle$, 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 Proposition 5.1.

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).

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 4.4. *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 5.1. Question 4.4 motivates the following definition:

DEFINITION 4.2. 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 $\mathscr{S}_{L,W}(H)$.

Thus, Question 4.4 asks whether or not all L-forms are stable. It seems that the trivial forms of H in $L \circ H$ play an important role. In order to determine this role we need a trivial lemma.

LEMMA 4.3. *Let $K \subseteq L$ be an extension of fields. Suppose ϕ: $H \to H'$ is a morphism of K-Hopf algebras, where $H' \subseteq L \otimes H$. Then ϕ 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 4.1. *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 Theorem 4.1 which is isomorphic to H. This would be any K-Hopf algebra $H' \subseteq L \circ H$ such that $H' \cong H$ and such that $L \otimes H' \cong L \otimes H$ via $l \otimes h' \mapsto lh'$.

Proof. Suppose ϕ: $H \to H'$ 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 $w \in W$, $h \in H$, and W has the Galois action on L. As in the proof of Theorem 4.1(iii), we have that $*$ is a commuting action on $L \circ H$. Also, $*$ restricts to an action on H.

We can extend ϕ to an L-Hopf algebra morphism $\overline{\phi}$: $L \otimes H \to L \otimes H$ by Lemma 4.3. Since $L \otimes H' \cong L \otimes H$ via $l \otimes h \mapsto lh$ (by Theorem 4.1), then we can define a map $\overline{\phi^{-1}}$: $L \otimes H \to L \otimes H$, $lh' \mapsto l\phi^{-1}(h')$ 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. We also have, for all $a \in L$, $h \in H$, $w \in W$, $w * ah = \Sigma(w_1 \cdot a)(\phi^{-1}(w_2 \cdot \phi(h_i))) = \overline{\phi^{-1}}(\Sigma(w_1 \cdot a)(w_2 \cdot \phi(h)))$.

Let $\{a_i\}$ be a basis of L over K, $F' = [L \circ H]^W$ 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 $w \in W$,

$$
\begin{aligned}
w * \sum_i a_i h_i = \sum_i \varepsilon(w) a_i h_i& \\
&\Leftrightarrow \overline{\phi^{-1}}\Big(\sum_i (w_1 \cdot a_i)(w_2 \cdot \phi(h_i))\Big) = \overline{\phi^{-1}}\Big(\sum_i \varepsilon(w) a_i \phi(h_i)\Big) \\
&\Leftrightarrow \sum_i a_i \phi(h_i) \in F.
\end{aligned}
$$

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

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

EXAMPLE 4.4. 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 $x \cdot g \in P_{g,g}(LG) = 0$. Thus, W acts trivially, and so $[L \circ W]^W = H$. 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 Theorem 2.3. Thus, Theorem 4.1 does not apply. Fortunately, we can still determine the L-forms in this case. Recall from Example 2.2 that $K \subseteq L$ is purely inseparable of exponent ≤ 1, and so Corollary 3.3 implies that there cannot be any nontrivial forms.

5. FORMS OF ENVELOPING ALGEBRAS

We now use Theorem 4.1 to compute 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 5.1. *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 of characteristic zero for W a finite-dimensional semisimple Hopf algebra, and if W acts on* $L \otimes U(\mathfrak{g})$ *as in Theorem* 4.1, *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 of the form* $U([L \otimes \mathfrak{g}]^W)$.

Note. 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). 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 invariant subalgebras of $L \otimes \mathfrak{g}$ under appropriate actions of W. Since W is cocommutative by Proposition 2.2, for each $w \in W, x, y \in \mathfrak{g}$, such actions satisfy $w \cdot [x, y] = \Sigma[w_1 \cdot x, w_2 \cdot y]$. This is analogous to the methods Jacobson used in [Jac62, Chap. 10] to find the forms of nonassociative algebras.

We first need a lemma which tells us when a Hopf algebra is an enveloping algebra.

LEMMA 5.1. *Let H be a K-bialgebra, let $\mathfrak{g}$ be a Lie subalgebra of $P(H) = \{x \in H : \Delta(x) = 1 \otimes x + x \otimes 1\}$, and let B be the K-subalgebra of H generated by $\mathfrak{g}$.*

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

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

The proof can be found in [PQ, 4.6]. Notice that this implies that a Hopf algebra is an enveloping algebra if and only if it is generated as an algebra by $P(H)$.

Proof (of 5.1). For (i), it suffices, by Lemma 5.1, to show that F is generated as an algebra by $P(F)$. Let $\Phi\colon L \otimes U(\mathfrak{g}) \to L \otimes F$ be an L-Hopf algebra isomorphism. Let $\{l_i\}$ be a basis for L over K, and let $x \in \mathfrak{g}$. Then $\Phi(x) = \Sigma_i l_i f_i$, for some $f_i \in F$. We have

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

Since $\{l_i\}$ is a basis, then $\Delta(f_i) = f_i \otimes 1 + 1 \otimes f_i$, and so $f_i \in P(F)$ 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), Theorem 4.1 implies that $[L \otimes U(\mathfrak{g})]^W$ is an L-form of $U(\mathfrak{g})$. By (i), it is generated by $P([L \otimes U(\mathfrak{g})]^W)$, 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 5.1. Let ω be a primitive n^2th root of unity for $n \geq 1$, $K = \mathbb{Q}(\omega^n)$, $L = K(\omega)$. Also, let $G = \mathbb{Z}_n = \langle \sigma \rangle$. Then $K \subseteq L$ is a $(KG)^*$-Galois extension, where G acts on L via $\sigma \cdot \omega = \omega^{n+1}$. Define $\mathfrak{g} = K\text{-span}\{x, y_0, \ldots, y_{n-1}\}$, where the Lie product is given by $[x, y_i] = \omega^{in} y_i$, $[y_i, y_j] = 0$.

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 $d = \gcd(k, n)$ and $l = \frac{n}{d}$, 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 $L \otimes \mathfrak{g} \cong L \otimes \mathfrak{g}_k$, then $\dim(\mathfrak{g}_k) = \dim(\mathfrak{g}) = n + 1$. It thus suffices to prove that $\{r, s_{jt}\}$ are linearly independent over K. Since $\{x, y_i\}$ is independent over K and r is a scalar multiple of x, then it suffices to show that the s_{jt}'s are linearly independent over K.

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

$$0 = \sum_{j,t} c_{jt} s_{jt} = \sum_{j=0}^{l-1} \sum_{t=0}^{d-1} \sum_{i=0}^{n-1} c_{jt}\, \omega^{jk(in+1)} y_{ik+t}. \tag{2}$$

We look at the coefficients of y_t for $0 \leq t \leq d - 1$. Looking at (2), 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 $\frac{k}{d} \mid zl$. Since $\gcd(\frac{k}{d}, l) = \gcd(\frac{k}{d}, \frac{n}{d}) = 1$, then $\frac{k}{d} \mid z$, so $k \mid zd$. Write $zd = z'k$. Then $i = \frac{zn}{k} = \frac{zdl}{k} = z'kl/k = z'l$. 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

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

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

Thus, $\mathfrak{g}_k = \text{span}\{r, s_{jt} : 0 \leq t \leq d - 1, 0 \leq j \leq l - 1\}$. The Lie bracket relations are $[r, s_{jt}] = \omega^{nt} s_{(j+1)t}$, $[s_{jt}, s_{j't'}] = 0$, 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 Lie ideal in $\mathfrak{g}_k$ of codimension 1 and that $I = \oplus_{t=0}^{d-1} I_t$.

LEMMA 5.2. *Let $w \notin I$. Then*

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

(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 $w \notin I$, then $a \neq 0$, 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, then $ad(r)^m(v_t) = av_t$, 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 $ad(r)^l$, then $m \mid l$. 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

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

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

$$ac_j = \omega^{kmp+mnt} c_{j+(p-1)m}, \qquad 0 \leq j \leq m-1 \tag{3}$$

$$ac_j = \omega^{mnt} c_{j-m}, \qquad m \leq j \leq pm-1. \tag{4}$$

Let i be minimal such that $c_i \neq 0$. If $c_j = 0$ for all $j < m$, then (4) implies that $v = 0$. Therefore, $i < m$. An easy induction gives us, using (4), 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 (3) 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 pth roots of both sides. Notice, since $p \mid l$ and $l \mid n$, that all the pth roots of unity are in K. We have $a = \omega^{(kl+lnt)/p} \cdot (p\text{th root of}$

unity), and so $\omega^{(kl+lnt)/p} \in K$. We must then have $n \mid \frac{kl+lnt}{p}$. Since $p \mid l$, then $n \mid \frac{lnt}{p}$. This forces $n \mid \frac{kl}{p}$. But $kl = n(\frac{k}{d})$, so we must have $p \mid \frac{k}{d}$.

But recall that $\gcd(\frac{k}{d}, l) = 1$. Since, $p \mid l$ and $p \mid \frac{k}{d}$, then $p = 1$, and so $m = l$. This gives us (ii), and the proof is complete. ∎

PROPOSITION 5.2. *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. For (i), suppose that $1 \le k, k' \le n$, with $\mathfrak{g}_k \cong \mathfrak{g}_{k'}$. Let $d = \gcd(n,k)$, $d' = \gcd(n,k')$, $l = \frac{n}{d}$, $l' = n/d'$. Also define $I' \lhd \mathfrak{g}_{k'}$ similarly as for $I \lhd \mathfrak{g}_k$. Without loss of generality, $l \le l'$. Let $\Phi: \mathfrak{g}_k \to \mathfrak{g}_{k'}$ be an isomorphism of Lie algebras. Since I, I' are the unique ideals of codimension 1 in their respective Lie algebras, we must have $\Phi(I) = I'$. By Lemma 5.2(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 Lemma 5.2(ii) gives us $l \ge l'$. Then $l = l'$, which implies that $d = d'$.

We now have $\gcd(n,k) = \gcd(n,k') = d$. Thus, $\mathfrak{g}_k = K\text{-span}\{r, s_{jt} : 0 \le j \le l-1, 0 \le t \le d-1\}$, $\mathfrak{g}_{k'} = K\text{-span}\{r', s'_{jt} : 0 \le j \le l-1, 0 \le t \le d-1\}$. 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

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

But since Φ is a homomorphism, then we get

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

This tells us that $\omega^{kl} b_{jt} = a^l \omega^{lnt+k'l} b_{jt}$ for all j, t. Since not all the b_{jt} are zero, then $a^l = \omega^{l(k-k'-nt)}$ for some t. But then $a = \omega^{k-k'-nt} \cdot$ (lth root of unity). The only way for $a \in K$ is if $k = k'$. 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

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

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

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

which gives us $a = (\sigma \cdot a)\omega^{-kn}$ 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 $a = (\sigma \cdot a)\omega^{-kn}$ gives us

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

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 $n \mid i - k$ 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. 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 c'_t / c_t is fixed by σ^l, and so $c'_t / c_t \in L^{\sigma^l} = K(\omega^k)$. 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 $r = \omega^k x + \sum_t b'_t y_t$, $r' = \omega^k x + \sum_t b''_t y_t \in [L \otimes \mathfrak{g}]^{KG}$. Subtracting these, we get $\sum_t (b'_t - b''_t) y_t \in [L \otimes \mathfrak{g}]^{KG}$, so by the $a = 0$ case, $r - r' \in \operatorname{span}\{s_{jt}\}$. Thus, r is unique modulo $\operatorname{span}\{s_{jt}\}$.

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 $\dim_K [L \otimes \mathfrak{g}]^{KG} = n + 1$, then 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 $\mathfrak{g}_k$. We use $c_{j(t+ik)} = \omega^{jk(in+1)} c_{0(t+ik)}$ (which we prove by induction), which gives us

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

The Lie product relations follow directly. ∎

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

6. FORMS OF DUALS OF HOPF ALGEBRAS

We turn our attention to determining forms for duals of finite-dimensional Hopf algebras. As we have seen in Proposition 2.1, we have a natural correspondence between forms of H and forms of H^* in which a form H' of H corresponds to the form $(H')^*$ of H^*.

In this section, we look at this question from the perspective of Theorem 4.1, and 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. By Proposition 4.1 and Theorem 4.1, all stable L-forms for H under W are obtained by finding appropriate commuting actions of W on H. We use these actions to help us compute forms of H^*. Specifically, given a commuting action of W on H, we construct a corresponding action on 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. The first step in this direction is finding a correspondence between W-actions on H and W^{cop}-actions on H^*. Recall that W^{cop} is the Hopf algebra with comultiplication $\Delta(w) = \sum w_2 \otimes w_1$. In the case W is cocommutative, $W^{\mathrm{cop}} = W$.

PROPOSITION 6.1. *Let W and H be Hopf algebras, and let H be a W-module algebra with a commuting action. Then H° is a left W^{cop}-module algebra with commuting action. Conversely, if H is finite dimensional, and if H^* is a left W^{cop}-module algebra with commuting action, then H is a left W-module algebra with commuting action.*

Note. We have that $H^\circ = \{f \in H^* : f(I) = 0$ for some ideal I of finite codimension$\}$ is a Hopf algebra [Mon93, 9.1.3]. 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 $w \cdot f \in H^\circ$ for all $w \in W^{\mathrm{cop}}$. We get

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

so $\Delta^*(w \cdot f) = \Sigma(w_2 \cdot f_1) \otimes (w_1 \cdot f_2) \in H^* \otimes H^*$. By [Mon93, 9.1.1], $w \cdot f \in H^\circ$. The above also shows that the action of w commutes with comultiplication in W^{cop}.

We now show that it is an action. We have, for all $w, w' \in W$, $f \in H^\circ$, $h \in H$,

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

For the rest of the requirements for a W-module algebra, we have

$$(w \cdot \varepsilon)(h) = \varepsilon(S(w) \cdot h) = \varepsilon(S(w))\varepsilon(h) = \varepsilon(w)\varepsilon(h) = (\varepsilon(w)\varepsilon)(h)$$

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

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

Now we must show that we have a commuting action.

$$\varepsilon^*(w \cdot f) = (w \cdot f)(1_H) = f(S(w) \cdot 1_H) = \varepsilon(w)\varepsilon^*(f)$$

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

so 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 $\{h_1, \dots, h_n\}$ be a basis for H, and let $\{h_1^*, \dots, h_n^*\}$ be 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 $h_i \cdot w = \sum_j a_{ji}(S^{-1}(w)) h_j$.

Claim 6.1. 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 $f = h_i^*$, $h = h_k$, since they form bases for their respective Hopf algebras. We have

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

$$= h_i^* \left(\sum_j a_{jk}(w) h_j \right) = h_i^*(S(w) \cdot h_k),$$

which proves the claim. ∎

Let $f \in H^*$, $h \in H$, and $w, w' \in W$. We have

$$f(ww' \cdot h) = \left(S^{-1}(ww') \cdot f\right)(h) = \left(S^{-1}(w')\left[S^{-1}(w) \cdot f\right]\right)(h)$$
$$= \left(S^{-1}(w) \cdot f\right)(w' \cdot h) = f(w \cdot [w' \cdot w']).$$

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

Now we see how this fits in with the general theory of L-forms. Let H be a finite-dimensional K-Hopf algebra, and let $K \subseteq L$ be a W^*-Galois extension of fields, such that H is a W-module algebra with commuting action. Then W is cocommutative by Proposition 2.2, so $W = W^{\mathrm{cop}}$. Thus, by Proposition 6.1, we have a correspondence between commuting actions of W on H and commuting actions of W on H^*. We attempt to extend this to a correspondence between L-forms of H and L-forms of H^*.

Recall that $\mathscr{S}_{L,W}(H)$ is the set of all stable L-forms of H under W. Define Φ: $\mathscr{S}_{L,W}(H) \to \mathscr{S}_{L,W}(H^*)$ as follows. Let $H' \in \mathscr{S}_{L,W}(H)$. Then $H' = [L \circ H]^W$ for some H-stable commuting action of W on $L \circ H$. From the previous, we have a corresponding commuting action of W on H^* and $K \subseteq L$ is W^*-Galois. We define $\Phi([L \circ H]^W) = [L \circ H^*]^W$. Since the commuting actions on H are in 1-1 correspondence with the commuting actions on H^*, we also define $\Psi([L \circ H^*]^W) = [L \circ H]^W$.

It is not clear that either of these maps is well defined on the subspaces of $L \circ H$, let alone on Hopf-isomorphism classes of these subspaces, since the function depends on the choice of action. It is clear that if they are well defined, then $\Psi = \Phi^{-1}$, which would give us a correspondence.

To make things more manageable, we'll restrict ourselves to a context which includes the case where W and H are both group algebras. Suppose that the commuting action of W on H is 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 $G(H)$. 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.

So let $\{h_1, \dots, h_n\}$ be a basis for H, and let $\{h_1^*, \dots, h_n^*\}$ 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 on H^* looks like, we have

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

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

A direct consequence of this nice relationship between the actions of W on H and the actions of W on H^* is the following.

PROPOSITION 6.2. $\sum_i l_i h_i \in [L \circ H]^W$ *if and only if* $\sum_i l_i h_i^* \in [L \circ H^*]^W$.

We can think of L-forms of H in two ways. In light of Theorem 4.1, we can think of them as subspaces of $L \circ H$. Another way is to think of them as Hopf-isomorphism classes of these subspaces. Thus, when we ask whether $\Phi\colon \mathscr{S}_{L,W}(H) \to \mathscr{S}_{L,W}(H^*)$ is a bijection, we can consider this question from two perspectives. When we consider Φ as a map between subspaces, we do get a bijection.

THEOREM 6.1. *Suppose that for all commuting actions of W on H that w and $S(w)$ act as transpose matrices for all $w \in W$. Then the map $\Phi\colon \mathscr{S}_{L,W}(H) \to \mathscr{S}_{L,W}(H^*)$ is a bijection, where we consider $\mathscr{S}_{L,W}(H)$ to be the invariant subspaces of $L \circ H$ arising from commuting actions on H which make $L \circ H$ a W-module algebra (similarly for $\mathscr{S}_{L,W}(H^*)$).*

Proof. Recall that $\Phi([L \circ H]^W) = [L \circ H^*]^W$. For clarity, if the action of W on H is given by $\cdot$, then we write $[L \circ H]^W = [L \circ H]^W_{\cdot}$. Suppose there are two actions $\cdot$ and $*$ such that $[L \circ H]^W_{\cdot} = [L \circ H]^W_{*}$. Let $\sum_i l_i h_i^* \in [L \circ H^*]^W_{\cdot}$. By the above, $\sum_i l_i h_i \in [L \circ H]^W = [L \circ H]^W_{*}$. Again by the above, $\sum_i l_i h_i^* \in [L \circ H^*]^W_{*}$, so $[L \circ H]^W_{\cdot} \subseteq [L \circ H^*]^W_{*}$. By symmetry, equality holds, and so the map is well defined. An almost identical argument gives us bijectivity. ∎

Now we address the question of whether Φ is well defined and bijective when considered as a map between isomorphism classes of L-forms of H. In the case where $W = KG$, not only does this occur, but there is also a nice matching of actions of W on $L \circ H$ and $L \circ H^*$ with the correspondence of L-forms given by Proposition 2.1. But we first need a lemma.

LEMMA 6.1. *Let H be a finite-dimensional Hopf algebra which is also a W-module algebra making $L \circ H$ a W-module algebra. Suppose also that w and $S(w)$ act as transpose matrices for all $w \in W$. Let $\{h_i\}$ be a basis for H with dual basis $\{h_i^*\}$, and suppose that $\sum_i b_i h_i \in [L \circ H]^W$, $\sum_i c_i h_i^* \in [L \circ H]^W$. 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 $\sum_i b_i h_i \in [L \circ H]^W$. We have

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

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

For (iii), we have

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

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. ∎

THEOREM 6.2. *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 $H' = [L \circ H]^W$ with corresponding L-form $\overline{H}' = [L \circ H^*]^W$ of H^*. Then $\overline{H}' \cong (H')^*$.*

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 $\phi\colon \overline{H}' \to (H')^*$ by $\phi(f)(\alpha) = \sum_i b_i c_i$. It is clear to see that ϕ is just the restriction of the isomorphism in Proposition 2.1 to $\overline{H}'$. We must first show that $\sum_i b_i c_i \in K$. We have, for each $g \in G$,

$$\begin{aligned}\sum_i b_i c_i &= \sum_{i,j,k} a_{ji}(g) a_{ki}(g)(g \cdot b_j)(g \cdot c_k), \qquad \text{by Lemma 6.1(i), (ii)}\\ &= \sum_{j,k} \delta_{j,k}(g \cdot b_j)(g \cdot c_k), \qquad \text{by Lemma 6.1(iii)}\\ &= g \cdot \left(\sum_j b_j c_j \right).\end{aligned}$$

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 Proposition 2.1 is an L-Hopf algebra isomorphism. ∎

EXAMPLE 6.1. Let $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, and so $K \subseteq L$ is W^*-Galois, where $W = K\mathbb{Z}_2$, $\mathbb{Z}_2 = \langle \tau \rangle$. Let $H = K\mathbb{Z}_n$, $\mathbb{Z}_n = \langle \sigma \rangle$. Then the commuting actions of W on H are given by $\tau \cdot \sigma = \sigma^k$, where $k^2 \equiv 1 \pmod n$. Let $d = \gcd(k-1, n)$. Since $[L \circ H]^W$ is spanned by elements of the form $t \cdot \sigma^j$ and $t \cdot i\sigma^j$, where $t = 1 + \tau \in \int_W^l$, then we get the form

$$H_k = \operatorname{span}\left\{ \sigma^{tn/d}, \sigma^j + \sigma^{kj}, i\sigma^j - i\sigma^{kj} : 0 \le t \le d-1, \right. \\ \left. 0 \le j \le n-1, j \ne \frac{tn}{d} \right\}.$$

In order to make the above spanning set a basis, we require that $j < kj \bmod n$. This weeds out redundant elements. To determine the Hopf algebra structure, let $c_j = \sigma^j + \sigma^{kj}$, $s_j = i\sigma^j - i\sigma^{kj}$. Then

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

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

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

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 $k^2 \equiv 1 \pmod n$. Let $d = \gcd(k-1, n)$. We get the form

$$\overline{H}_k = \operatorname{span}\left\{ p_{tn/d}, p_j + p_{kj}, ip_j - ip_{kj} : 0 \le t \le d-1, 0 \le j \le n-1, \right. \\ \left. j \notin \left(\frac{tn}{d}\right)\mathbb{Z}, j < kj \right\}.$$

Similarly, as before, let $\bar{c}_j = p_j + p_{kj}$, $\bar{s}_j = ip_j - ip_{kj}$. The multiplication is thus given by

$$\bar{c}_j \bar{c}_m = (\delta_{j,m} + \delta_{kj,m}) \bar{c}_m$$

$$\bar{c}_j \bar{s}_m = (\delta_{j,m} + \delta_{kj,m}) \bar{s}_m$$

$$\bar{s}_j \bar{s}_m = (\delta_{kj,m} - \delta_{j,m}) \bar{c}_m.$$

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

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

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

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

By Theorem 6.2, we have that $\overline{H}_k \cong H_k^*$. 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 $\overline{H}_K \to H_k^*$.

Most of the proof of Theorem 6.2 can be duplicated for general W. We need only show that $\sum_i b_i c_i \in K$. So we ask

QUESTION 6.5. *If $\sum_i b_i h_i \in [L \circ H]^W$, $\sum_i c_i h_i^* \in [L \circ H^*]^W$, does this imply that $\sum_i b_i c_i \in K$?*

This is not obvious in the general case, since Lemma 6.1 does not seem to be helpful if W is not a group algebra.

7. ADJOINT FORMS

As mentioned in Section 4, 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 Proposition 6.1. We demonstrate this on the group algebra KD_{2n}.

EXAMPLE 7.1. Let ω be a primitive nth root of unity, and let α be a real nth root of 2. Let $K = \mathbb{Q}(\omega + \omega^{-1})$, $L = K(\alpha, \omega)$. If we let $H = KD_{2n}$, where $D_{2n} = \langle \sigma, \tau : \sigma^n = 1, \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$ is the dihedral group of order $2n$, then $K \subseteq L$ is H^*-Galois, where the action of D_{2n} on L is given by $\sigma \cdot \alpha = \omega\alpha$, $\sigma \cdot \omega = \omega$, $\tau \cdot \alpha = \alpha$, $\tau \cdot \omega = \omega^{-1}$. We obtain a form of H by letting H act on itself via the adjoint action, so $\sigma \cdot \tau = \sigma^2\tau$, $\tau \cdot \sigma = \sigma^{-1}$. We then compute $H' = [L \circ H]^H$ 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.

Some easy computations give us that the elements $e_k = \frac{1}{n}\sum_{i=0}^{n-1} \omega^{ki}\sigma^i$, $e'_k = \frac{1}{2}\alpha^{2k}e_k\tau$ are 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

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

Let $0 \le m \le n-1$. The coefficient of σ^m is $1/n^2\sum_i \omega^{ki+l(m-i)} = (1/n^2)\omega^{lm}\sum_i \omega^{i(k-l)}$. But ω^{k-l} is an nth 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 $\{e_k, e'_k : 0 \le k \le n-1\}$ 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 $0 \le j \le n-1$,

$$0 = e_j\left(\sum_k a_k e_k + \sum_k b_k e'_k\right) = a_j e_j + b_j e'_j$$

and so clearly $a_j = b_j = 0$. This gives us $H' = K\text{-span}\,\{e_k, e'_k = \frac{1}{2}\alpha^{2k}e_k\tau : 0 \le k \le n-1, e_k e_l = \delta_{k,l}e_l\}$

To finish off the multiplication table, we first compute

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

We then have

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

$$e_k e'_l = e_k\alpha^{2l}e_l\tau = \delta_{k,l}\alpha^{2l}e_l\tau = \delta_{k,l}e'_l$$

$$e'_k e_l = \frac{1}{2}\alpha^{2k}e_k\tau, \qquad e_l = \frac{1}{2}\alpha^{2k}e_k e_{n-l}\tau = \frac{1}{2}\delta_{k+l,n}\alpha^{2k}e_k\tau = \delta_{k+l,n}e'_k.$$

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 $M_k \cong M_2(K)$ 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 $e_k e'_k = e'_k e_k = e'_k$, $e_k^2 = e'^2_k = e_k$, so e_k acts like identity and $R \cong K[\mathbb{Z}_2]$. For n odd, this gives us

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

and for n even, we have

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

For the rest of the Hopf algebra structure, direct computation gives us, for each $0 \leq k \leq n-1$, $\Delta(e_k) = \sum_{j=0}^{n-1} e_j \otimes e_{k-j}$, $\varepsilon(e_k) = \delta_{k,0}$, $S(e_k) = e_{n-k}$. 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 $S(e'_k) = e'_k$.

We can also find corresponding forms for H^*. Let the form corresponding to the induced action on H^* be $\overline{H}$. From Proposition 6.2, we have the basis $\bar{e}_k = \sum_i \omega^{ki} p_{\sigma^i}$, $\bar{e}'_k = \sum_i \alpha^{2k}\omega^{ki} p_{\sigma^i\tau}$ 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

$$\Delta(\bar{e}_k) = \bar{e}_k \otimes \bar{e}_k + \frac{1}{4}\bar{e}'_k \otimes \bar{e}'_{n-k}, \qquad \Delta(\bar{e}'_k) = \bar{e}_k \otimes \bar{e}'_k + \bar{e}'_k \otimes \bar{e}_{n-k}$$

$$\varepsilon(\bar{e}_k) = 1, \qquad \varepsilon(\bar{e}'_k) = 0, \qquad S(\bar{e}_k) = \bar{e}_{n-k}, \qquad S(\bar{e}'_k) = \bar{e}'_k.$$

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

REFERENCES

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

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

[Coh94] M. Cohen, Quantum commutativity and central invariants, *in* "Advances in Hopf Algebras" (J. Bergen and S. Montgomery, Eds.), pp. 25–38, Dekker, New York, 1994.

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

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

[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] N. Jacobson, "Lectures in Abstract Algebra," Vol. 3, Van Nostrand, Princeton, NJ, 1964.

[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, MA, 1966.

[Mon93] S. Montgomery, "Hopf Algebras and Their Actions on Rings," Am. Math. Soc., Providence, 1993.

[Nic94] W. D. Nichols, Cosemisimple Hopf algebras, *in* "Advances in Hopf Algebras" (J. Bergen and S. Montgomery, Eds.), pp. 135–151, Dekker, New York, 1994.

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

[PQ] D. S. Passman and D. Quinn, "Elementary Bialgebra Properties of Group Rings and Enveloping Rings," preprint.

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

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

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