An Introduction to Hopf Algebras and Hopf-Galois Theory for Separable Extensions of Fields

Kyle Mickelson

Last updated: May 2, 2024

Contents

❖ Algebras and Coalgebras

In this introductory section we shall introduce two fundamental objects in our study of Hopf algebras: algebras and coalgebras. Familiarizing ourselves with the structural properties of algebras and coalgebras will enable us to dive deeper into Hopf algebras later on, and we shall provide proofs for a number of propositions and theorems which will turn out to be crucial in our eventual development of so-called Hopf-Galois theory for separable field extensions.

In this section we shall primarily follow the exposition in [Und15], sometimes invoking results from [Und11] as well when necessary. We do not go too far into this field (it is vast, and encompassing by itself), but take only what will be necessary for the building of intuition and later theory. A good reference for this chapter is [DNR00], where a significant deal more detail is provided on the theory of algebras and coalgebras.

1.1 Algebras

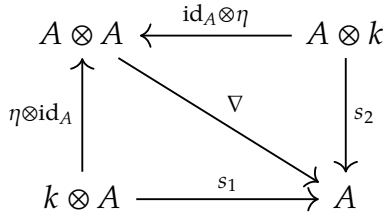
The reader is probably familiar with more general algebras over rings. In this section, and in further developments, we shall only concern ourselves with the notion of algebras over a field. We do not lose much in specifying to this case, and in fact for later theory the case for fields suffices.

To start, we diagrammatize the definition of an algebra over a field, stripping away all of the essential ingredients bare, so to speak, in a bid to flip arrows (and define coalgebras) later on.

Definition 1.1. Let k be a field. We refer to a k-vector space A equipped with k-linear homomorphisms $\nabla : A \otimes A \to A$ and $\eta : k \to A$ as a *k-algebra* if the following diagrams

$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{\mathrm{id}_A \otimes \nabla} & A \otimes A \\ \downarrow{\scriptstyle \nabla \otimes \mathrm{id}_A} & & \downarrow{\scriptstyle \nabla} \\ A \otimes A & \xrightarrow{\nabla} & A \end{array}$$

and



commute, where $s_1 : k \otimes_k A \to A$ is defined by $s_1(r \otimes a) = ra$ and $s_2 : A \otimes_k k \to A$ is defined by $s_2(a \otimes r) = ra$. In other words, we have that

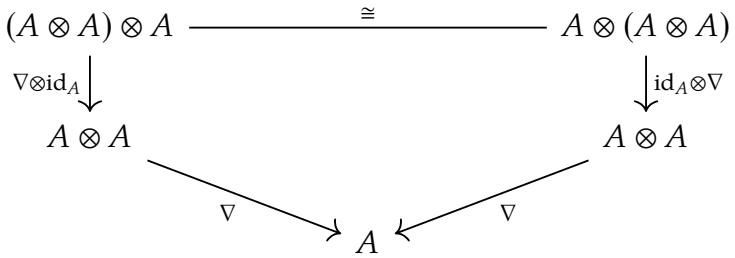
$$(\nabla \circ (\nabla \otimes \mathrm{id}_A))(a_1 \otimes a_2 \otimes a_3) = (\nabla \circ (\mathrm{id}_A \otimes \nabla))(a_1 \otimes a_2 \otimes a_3)$$

$$(\nabla \circ (\eta \otimes \mathrm{id}_A))(r \otimes a) = ra = (\nabla \circ (\mathrm{id}_A \otimes \eta))(a \otimes r)$$

holds for all $a_1, a_2, a_3, a \in A$ and $r \in k$. The first equation is referred to as the *associative property* for A, and the second equation is referred to as the *unit property* of A. We call the map ∇ the *multiplication map*, and we call the map η the *unit map*.

For brevity, a k-algebra A with multiplication map ∇ and unit map η is sometimes denoted simply by the ordered triple (A, ∇, η). When we are working with multiple k-algebras simultaneously, we often attach subscripts to the maps corresponding to the underlying k-vector space, for instance (B, ∇_B, η_B), in order to differentiate between multiplication and unit maps for different k-algebras.

Let (A, ∇, η) be a k-algebra. The diagrams in the definition of a k-algebra above merit further discussion. Consider the diagram



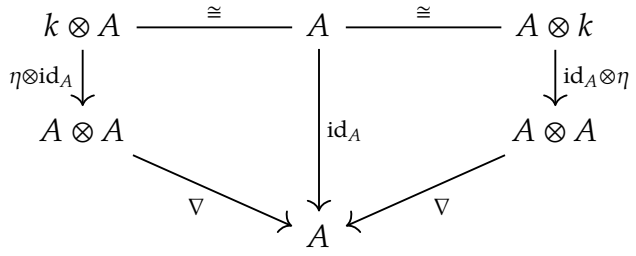
Where we have the canonical isomoprhism of k-vector spaces $(A \otimes A) \otimes A \cong A \otimes (A \otimes A)$ from elementary vector space theory. In our initial definition of a k-algebra, we simply identified these isomorphic vector spaces with one another, writing $A \otimes A \otimes A$. Regardless, the commutativity of the above diagram encodes the familiar associative property of a k-algebra, and in fact tells us much more.

Informally, we may identify the product $\nabla(a \otimes b)$ with the symbol ab for all elements $a, b \in A$. The above diagram, if it commutes, states that the product

a_1a_2 (really the element $\nabla(a_1 \otimes a_2)$) with a_3 should be identical to the product a_1 with a_2a_3 (really the element $\nabla(a_2 \otimes a_3)$), which equates to the simple relationship $(a_1a_2)a_3 = a_1(a_2a_3)$.

As we can see, the commutativity of the diagram above (the associative property of the k-algebra) provides us with an associative binary operation on the k-vector space A. We observe that A as a k-vector space is, by definition, an additive abelian group $(A, +)$, and that the associative binary operation of multiplication above satisfies the distributive laws. In particular, this means that A has the structure of a ring

In a completely analagous manner, the second diagram in the definition of a k-algebra may be rewritten as follows:



Where we have the canonical isomorphisms of k-vector spaces $k \otimes A \cong A$ and $A \otimes k \cong A$, defined by $r \otimes a \leftrightarrow ra$ and $a \otimes r \leftrightarrow ra$, respectively. If the above diagram commutes (the unit property in the definition of a k-algebra), then the product $\eta(r)a$ and $a\eta(r)$ are equal, with their shared value being ra. On the one hand, this implies $\eta(k) \subseteq Z(A)$, where $Z(A)$ denotes the center of the ring A. On the other hand, taking $r = 1_k \in k$ gives $\eta(1_k)a = a$, so that $\eta(1_k) = 1_A$, where 1_k and 1_A denote the additive identity elements of k and A, respectively. Furthermore, we have $\eta(r_1r_2) = r_1r_2$. Since the unit map η is, by definition, a k-linear map, this proves that η is a ring homomorphism from k to A.

To summarize the above discussion, given a k-algebra (A, ∇, η) according to our initial definition, we have that A is a unital ring equipped with a ring homomorphism $\eta : k \to A$ mapping 1_k to 1_A such that $\eta(k)$ is contained in the center of A. Readers with prior exposure to the construction of an algebra over a ring may recognize this conclusion as the ordinary definition of an algebra over a ring! In fact, with a little extra work, it can be easily shown that the reverse is true, namely that an algebra over a field in the usual sense satisfies our initial definition in terms of structure maps.

Having encountered the definition of a k-algebra, and having verified that our definition coincides with the definition of an algebra over a field in the usual sense, we now present some examples with which to keep in mind during our

continued discussion.

Example 1.2. Let G be a finite group, and let 1_G denote the identity element of G. Recall that the group ring $k[G]$ is a k-module. We shall construct multiplication and unit maps which make $k[G]$ into a k-algebra.

Consider the map $\nabla_{k[G]} : k[G] \otimes_k k[G] \to k[G]$ defined by $g \otimes h \mapsto gh$, and the map $\eta_{k[G]} : k \to k[G]$ defined by $\alpha \mapsto \alpha 1_G$ for all $g, h \in G$ and $\alpha \in k$. It is immediately verified that both $\nabla_{k[G]}$ and $\eta_{k[G]}$ are k-module homomorphisms, and furthermore that the equations in the definition of a k-algebra are satisfied.

Note also that if G is an abelian group, then for all $g, h \in G$ we have $gh = hg$, and hence $\nabla_{k[G]}(g \otimes h) = \nabla_{k[G]}(h \otimes g)$.

The observation at the end of Example 1.2 merits further discussion, in light of which we make the following definition:

Definition 1.3. The k-algebra (A, ∇, η) is called *commutative* if the diagram

$$\begin{array}{ccc} A \otimes A & \xleftarrow{\quad\tau\quad} & A \otimes A \\ & {\scriptstyle\nabla}\searrow \quad \swarrow{\scriptstyle\nabla} & \\ & A & \end{array}$$

commutes. In other words, if the equation

$$(\nabla \circ \tau)(a \otimes b) = \nabla(a \otimes b)$$

holds for all $a, b \in A$, where $\tau : A \otimes A \to A \otimes A$ is defined by $\tau(a \otimes b) = b \otimes a$. The map τ is referred to as the *twist map*.

With the definition above it is easy to see that the group ring k-algebra $(k[G], \nabla_{k[G]}, \eta_{k[G]})$ is commutative if and only if G is abelian. We now present more examples of commutative k-algebras.

Example 1.4. Let k be a field. Clearly k is a k-module over itself. Furthermore, the maps $\nabla_k : k \otimes_k k \to k$ defined by $\nabla_k(r \otimes r') = rr'$ and $\eta_k : k \to k$ defined by $\eta_k(r) = r$ for all $r, r' \in k$ suffice to make k into a commutative k-algebra.

Example 1.5. Let K/k be an algebraic extension of fields. Suppose, moreover, that K/k is a simple extension, so that $K = k(\alpha)$ for some $\alpha \in K$. We can make the overfield K into a commutative k-algebra via usual multiplication in K, $\nabla_K : K \otimes_k K \to K$, with $\eta_K : k \to K$ defined by $r \mapsto r$ for all $r \in k$.

Definition 1.6. The k-algebra (k, ∇_k, η_k) of Example 1.4 is called the *trivial k-algebra*.

We conclude this section by introducing the subobjects of k-algebras. Given any k-algebra (A, ∇, η), and any k-subspace of A considered as a k-vector space, we can restrict the domain of the multiplication and unit maps to obtain k-linear maps

$$\nabla|_B : B \otimes B \to A$$

$$\eta|_B : k \to B$$

If it is the case that $\nabla(B) \subseteq B$, i.e., that products of elements of B are once again elements of B, then it is an easy exercise to see that $\nabla|_B$ satisfies the associative property in the definition of a k-algebra. Indeed, in this case we have that $(B, \nabla|_B, \eta|_B)$ is a k-algebra as well. We attach the following definition to this scenario:

Definition 1.7. Let (A, ∇, η) be a k-algebra. If B is a k-subspace of A such that $\nabla(B) \subseteq B$, then the k-algebra $(B, \nabla|_B, \eta|_B)$ is called a *k-subalgebra* of A.

1.2 Quotients and Homomorphisms of Algebras

In this section we define the maps between algebras as maps which are linear with respect to the underlying field and preserve the multiplication and unit maps of the algebras. We then abuse the fact that algebras are rings with additional structure to form quotients of algebras via ideals.

Definition 1.8. Let k be a field and let (A, ∇_A, η_A) and (B, ∇_B, η_B) be k-algebras. We refer to a k-linear mapping $\phi : A \to B$ as a *homomorphism of k-algebras* if the following diagrams

$$\begin{array}{ccc} A \otimes A & \xrightarrow{\phi\otimes\phi} & B \otimes B \\ {\scriptstyle \nabla_A}\downarrow & & \downarrow{\scriptstyle \nabla_B} \\ A & \xrightarrow{\phi} & B \end{array}$$

and

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ & {\scriptstyle \eta_A}\nwarrow \quad \nearrow{\scriptstyle \eta_B} & \\ & k & \end{array}$$

commute. In other words, the k-linear map $\phi : A \to B$ is a homomorphism of k-algebras if

$$(\phi \circ \nabla_A)(a \otimes a') = (\nabla_B \circ (\phi \otimes \phi))(a \otimes a')$$

$$(\phi \circ \eta_A)(r) = \eta_B(r)$$

for all $a, a' \in A$ and $r \in k$.

If (A, ∇_A, η_A) and (B, ∇_B, η_B) are k-algebras then it is clear from the above definition that any k-algebra homomorphism $\phi : A \to B$ is, in particular, a ring homomorphism which has the additional property of being linear with respect to the field k. Explicitly, the fact that ϕ is k-linear gives

$$\phi(a + a') = \phi(a) + \phi(a')$$

and, denoting the product in A, $a \otimes a'$, by aa', we have

$$\phi(aa') = \phi(a)\phi(a')$$

as well as $\phi(1_A) = 1_B$ from the second diagram. These are, of course, the familiar conditions for ϕ to be a ring homomorphism.

With the above in mind, we naturally have that $\ker\phi$ is a 2-sided ideal of A, as well as that the image $\operatorname{im}\phi$ is a k-subalgebra of B. We now work with ideals of A more generally, and show that we can use such constructions to form quotients of algebras.

Proposition 1.9. Let A be a k-algebra and let I be an ideal of A. Then the quotient k-module A/I is a k-algebra.

Proof. From elementary module theory, the quotient ring A/I is naturally a k-submodule of A, so in particular a k-module itself. We construct a multiplication map for A/I.

We have the canonical projection $\pi : A \to A/I$, which is easily seen to be a k-module homomorphism. The composition of k-module homomorphisms is once more a k-module homomorphism, and hence

$$\pi \circ \nabla : A \otimes A \to A/I$$

$$a \otimes a' \mapsto aa' + I$$

is a k-module homomorphism. Consider the k-submodule $I \otimes A + A \otimes I$ of $A \otimes A$. Let $r \otimes a + a' \otimes r' \in I \otimes A + A \otimes I$. Then

$$\pi(\nabla(r \otimes a + a' \otimes r')) = \pi(ra + a'r') = ra + a'r' + I = I$$

which follows since $r, r' \in I$ implies $ra + a'r' \in I$ by properties of ideals. Hence $I \otimes A + A \otimes I \subseteq \ker(\pi \circ \nabla)$. By the universal mapping property for kernels, there exists a k-module homomorphism

$$\overline{\pi \circ \nabla} : \frac{A \otimes A}{I \otimes A + A \otimes I} \to A/I$$

$$a \otimes a' + (I \otimes A + A \otimes I) \mapsto aa' + I$$

From module theory, we have the following k-module isomorphism

$$\Phi : A/I \otimes A/I \xrightarrow{\sim} \frac{A \otimes A}{I \otimes A + A \otimes I}$$

and hence we may compose to get

$$\overline{\pi \circ \nabla} \circ \Phi : A/I \otimes A/I \to A/I$$

$$(a + I) \otimes (a' + I) \mapsto aa' + I$$

Taking $\nabla_{A/I} = \overline{\pi \circ \nabla} \circ \Phi$, we see that $\nabla_{A/I}$ is our multiplication map for A/I. To construct the unit map for A/I, simply take $\eta_{A/I} = \pi \circ \eta$, so that $\eta_{A/I} : k \to A/I$. It is easy to check that these maps make the associative and unit properties hold; hence $(A/I, \nabla_{A/I}, \eta_{A/I})$ is a k-algebra. ∎

The k-algebras obtained from Proposition 1.9 are so important that we give them a name:

Definition 1.10. Let (A, ∇, η) be a k-algebra, and let I be an ideal of A. We call the k-algebra $(A/I, \nabla_{A/I}, \eta_{A/I})$ the *quotient k-algebra of A by I*.

1.3 Direct Sum and Tensor Product of Algebras

In this section we describe processes by which k-algebras may be combined, in some sense, to form new k-algebras, often carrying interesting structural information about their lesser components. These processes are none other than the direct sum and the tensor product. The savvy reader would do well to attempt proofs of these facts before we present them.

First, we prove that the direct sum of k-algebras form a new k-algebra.

Proposition 1.11. Let k be a field, and let (A, ∇_A, η_A) and (B, ∇_B, η_B) be k-algebras. Then the direct sum $A \oplus B$ is a k-algebra.

Proof. The direct sum $A \oplus B$ is naturally a k-vector space. We construct a multiplication map for $A \oplus B$. We claim the map

$$\nabla_{A\oplus B} : (A \oplus B) \otimes (A \oplus B) \to A \oplus B$$

$$(a, b) \otimes (a', b') \mapsto (aa', bb')$$

for all $a, a' \in A$ and $b, b' \in B$ suffices. The map $\nabla_{A\oplus B}$ is trivially a k-linear map, and the fact that $\nabla_{A\oplus B}$ satisfies the associative property is immediate. Further, for a unit map we may consider

$$\eta_{A\oplus B} : k \to A \oplus B$$

$$r \mapsto (\eta_A(r), \eta_B(r))$$

for all $r \in k$. The map $\eta_{A\oplus B}$ is k-linear, and for the unit property we have

$$\begin{aligned}(\nabla_{A\oplus B} \circ (\mathrm{id}_{A\oplus B} \otimes \eta_{A\oplus B}))((a, b) \otimes r) &= \nabla_{A\oplus B}((a, b) \otimes (\eta_A(r), \eta_B(r)) \\ &= (a\eta_A(r), b\eta_B(r)) \\ &= (\eta_A(r)a, \eta_B(r)b) \\ &= \nabla_{A\oplus B}((\eta_A(r), \eta_B(r)) \otimes (a, b)) \\ &= (\nabla_{A\oplus B} \circ (\eta_{A\oplus B} \otimes \mathrm{id}_{A\oplus B}))(r \otimes (a, b))\end{aligned}$$

With the above constructions, we have that $(A \oplus B, \nabla_{A\oplus B}, \eta_{A\oplus B})$ is a k-algebra. ∎

Next, we prove that the tensor product of k-algebras forms a new k-algebra.

Proposition 1.12. Let k be a field, and let (A, ∇_A, η_A) and (B, ∇_B, η_B) be k-algebras. Then the tensor product $A \otimes B$ is a k-algebra.

Proof. From module theory, the tensor product of the k-modules A and B, $A \otimes B$, is a k-module. We now construct a multiplication map for $A \otimes B$. We claim that the map

$$\nabla_{A\otimes B} : (A \otimes B) \otimes (A \otimes B) \to A \otimes B$$

$$(a \otimes b) \otimes (a' \otimes b') \mapsto aa' \otimes bb'$$

for all $a, a' \in A$ and $b, b' \in B$ suffices. To prove that $\nabla_{A\otimes B}$ is a k-linear map, we show it can be written as the composition of k-linear maps. observe

$$\begin{aligned}
\nabla_{A\otimes B}((a \otimes b) \otimes (a' \otimes b')) &= ((\nabla_A \otimes \nabla_B) \circ (\mathrm{id}_A \otimes \tau \otimes \mathrm{id}_B)((a \otimes b) \otimes (a' \otimes b'))) \\
&= ((\nabla_A \otimes \nabla_B) \circ (\mathrm{id}_A \otimes \tau \otimes \mathrm{id}_B))(a \otimes (b \otimes a') \otimes b') \\
&= (\nabla_A \otimes \nabla_B)(\mathrm{id}_A(a) \otimes \tau(b \otimes a') \otimes \mathrm{id}_B(b')) \\
&= (\nabla_A \otimes \nabla_B)(a \otimes a' \otimes b \otimes b') \\
&= \nabla_A(a \otimes a') \otimes \nabla_B(b \otimes b') \\
&= aa' \otimes bb'
\end{aligned}$$

Also, it is clear to see that the map $\nabla_{A\otimes B}$ satisfies the associative property, and one may check this directly.

For the unit map, we may take $\eta_{A\otimes B} : k \to A \otimes B$ defined by $\eta_{A\otimes B}(r) = \eta_A(r) \otimes 1$, where 1 here refers to the identity of B, for all $r \in k$. The unit property is naturally satisfied, see

$$\begin{aligned}
(\nabla_{A\otimes B} \circ (\mathrm{id}_{A\otimes B} \otimes \eta_{A\otimes B}))(a \otimes b \otimes r) &= \nabla_{A\otimes B}(a \otimes b \otimes \eta_A(r) \otimes 1) \\
&= a\eta_A(r) \otimes b1 \\
&= \eta_A(r)a \otimes 1b \\
&= \nabla_{A\otimes B}(\eta_A(r) \otimes 1 \otimes a \otimes b) \\
&= (\nabla_{A\otimes B} \circ (\eta_{A\otimes B} \otimes \mathrm{id}_{A\otimes B}))(r \otimes a \otimes b)
\end{aligned}$$

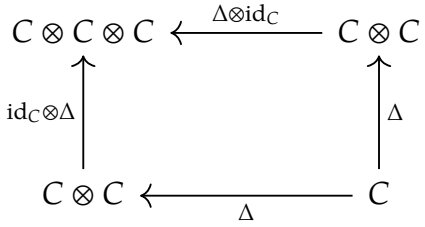
In particular, we have shown that $(A \otimes B, \nabla_{A\otimes B}, \eta_{A\otimes B})$ is a k-algebra. ∎

With the two propositions above, we have greatly increased our class of possible k-algebras. In particular, we are now able to build larger k-algebras from smaller ones, in a sense.

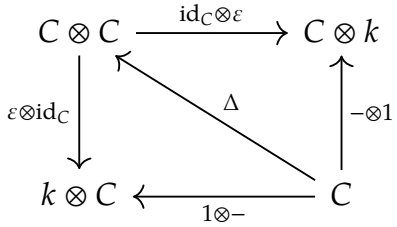
1.4 Coalgebras

Now we define what some might call the "dual" notion of a k-algebra. In particular, we define and provide examples of algebraic objects that reverse the arrows in the definition of k-algebra. As is common in category theory, we attach the prefix 'co' to k-algebras to indicate this flipping process.

Definition 1.13. Let k be a field. We refer to a k-vector space C equipped with k-linear map $\Delta : C \to C \otimes_k C$ and $\varepsilon : C \to k$ as a *k-coalgebra* if the following diagrams



and



commute, where the maps $1\otimes- : C \to k\otimes_k C$ takes $c \mapsto 1\otimes c$ and $-\otimes 1 : C \to C\otimes_k k$ takes $c \mapsto c \otimes 1$. In other words, we have that

$$((\mathrm{id}_C \otimes \Delta) \circ \Delta)(c) = ((\Delta \otimes \mathrm{id}_C) \circ \Delta)(c)$$

$$((\varepsilon \otimes \mathrm{id}_C) \circ \Delta)(c) = 1 \otimes c$$

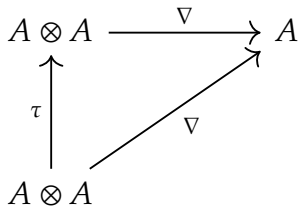
$$((\mathrm{id}_C \otimes \varepsilon) \circ \Delta)(c) = c \otimes 1$$

holds for all $c \in C$. The first equation is referred to as the *coassociative property* and the second and third equations are together referred to as the *counit property*. We call the map Δ the *comultiplication map*, and we call the map ε the *counit* map.

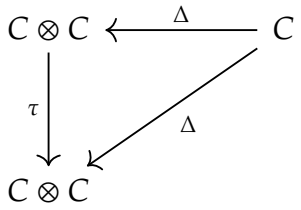
Similarly to k-algebras, we oftentimes write a k-coalgebra as an ordered triple (C, Δ, ε).

In our initial brush with k-algebras we precisely defined what we meant by a commutative k-algebra. Specifically, we said that a k-algebra (A, ∇, η) was commutative if $(\nabla \circ \tau)(a \otimes b) = \nabla(a \otimes b)$ for all $a, b \in A$. Equivalently, A is

commutative if and only if the following diagram



commutes. To define a corresponding notion of commutativity for k-coalgebras, we naturally reverse the arrows in the above diagram, as we did in defining a k-coalgebra, and require that such a diagram commute. In particular, letting (C, Δ, ε) be a k-coalgebra, we require that the diagram



commute. This requirement necessitates the following definition.

Definition 1.14. We say that a k-coalgebra (C, Δ, ε) is *cocommutative* if

$$(\tau \circ \Delta)(c) = \Delta(c)$$

holds for all $c \in C$, where τ denotes the twist map defined previously.

We now provide examples of cocommutative coalgebras.

Example 1.15. Let k be a field. Clearly k is a k-module over itself. Consider the map $\Delta_k : k \to k \otimes k$ taking $\alpha \mapsto \alpha \otimes 1$ and $\varepsilon_k : k \to k$ taking $\alpha \mapsto \alpha$. It is a simple check to prove that $(k, \Delta_k, \varepsilon_k)$ is a cocommutative k-coalgebra.

Example 1.16. Let V be an n-dimensional k-vector space, with a k-basis $\{v_1, \ldots, v_n\}$ Clearly V is a k-module. Consider the map $\Delta_V : V \to V \otimes_k V$ defined by

$$\Delta_V(v_j) = v_j \otimes v_j$$

for all $j \in \{1, \ldots, n\}$. Since Δ_V is defined on a k-basis for V, it is clear that the map Δ_V can be extended to a map on V. Now let $\varepsilon_V : V \to k$ be a map defined by

$$\varepsilon_V(v_j) = 1$$

for all $j \in \{1, \ldots, n\}$. Once again, ε_V can easily be extended to a k-linear map on all of V, since it is defined on a basis. Using these constructions, $(V, \Delta_V, \varepsilon_V)$ is a cocommutative k-coalgebra.

1.5 Sweedler Notation

We take a momentary respite from our line of inquiry to discuss an important piece of notation used in working with coalgebras. This notation, referred to as *Sweedler notation*, is useful for simplifying otherwise esoteric (and more importantly, ambiguous) computations involving coproducts in coalgebras.

Let k be a field. In the case of a k-algebra (A, ∇, ε), we assign to the product $a_1a_2a_3$ the (shared) value of the products $(a_1a_2)a_3$ and $a_1(a_2a_3)$, where $a_1, a_2, a_3 \in A$. The means by which we make this assignment come from the associative property in the definition of a k-algebra. More explicitly, the associative property states that

$$(\nabla \circ (\mathrm{id}_A \otimes \nabla))(a_1 \otimes a_2 \otimes a_3) = (\nabla \circ (\nabla \otimes \mathrm{id}_A))(a_1 \otimes a_2 \otimes a_3)$$

and hence that

$$\nabla(a_1 \otimes \nabla(a_2 \otimes a_3)) = \nabla(\nabla(a_1 \otimes a_2) \otimes a_3)$$

In other words, taking the product of a_1 with the product of a_2 and a_3 is the same as taking the product of a_1 with a_2 and a_3, which is equivalent to $(a_1a_2)a_3 = a_1(a_2a_3)$. If we instead consisder a coalgebra, then what can we say about coproducts?

Let (C, Δ, ε) be a k-coalgebra. Sweedler notation is defined as follows: for every $c \in C$, we set

$$\Delta(c) = \sum_{(c)} c_{(1)} \otimes c_{(2)}$$

Now recall the coassociative property in the definition of C, which states that

$$((\mathrm{id}_C \otimes \Delta) \circ \Delta)(c) = ((\Delta \otimes \mathrm{id}_C) \circ \Delta)(c)$$

for all $c \in C$. Now we use Sweedler notation to evaluate the left and right hand sides of the above equation. For the left hand side, we find

$$\begin{aligned}
((\mathrm{id}_C \otimes \Delta) \circ \Delta)(c) &= (\mathrm{id}_C \otimes \Delta)\left(\sum_{(c)} c_{(1)} \otimes c_{(2)}\right) \\
&= \sum_{(c)} \mathrm{id}_C(c_{(1)}) \otimes \Delta(c_{(2)}) \\
&= \sum_{(c)} c_{(1)} \otimes \left(\sum_{(c_{(2)})} c_{(2)_{(1)}} \otimes c_{(2)_{(2)}}\right) \\
&= \sum_{(c, c_{(2)})} c_{(1)} \otimes c_{(2)_{(1)}} \otimes c_{(2)_{(1)}}
\end{aligned}$$

While for the right, we have

$$\begin{aligned}((\Delta \otimes \mathrm{id}_C) \circ \Delta)(c) &= (\Delta \otimes \mathrm{id}_C)\left(\sum_{(c)} c_{(1)} \otimes c_{(2)}\right) \\ &= \sum_{(c)} \Delta(c_{(1)}) \otimes \mathrm{id}_C(c_{(2)}) \\ &= \sum_{(c)} \left(\sum_{(c_{(1)})} c_{(1)_{(1)}} \otimes c_{(1)_{(2)}}\right) \otimes c_{(2)} \\ &= \sum_{(c,c_{(1)})} c_{(1)_{(1)}} \otimes c_{(1)_{(2)}} \otimes c_{(2)}\end{aligned}$$

By the coassociative property, the left hand and right hand sides agree, and thus we have the equality

$$\sum_{(c,c_{(2)})} c_{(1)} \otimes c_{(2)_{(1)}} \otimes c_{(2)_{(1)}} = \sum_{(c,c_{(1)})} c_{(1)_{(1)}} \otimes c_{(1)_{(2)}} \otimes c_{(2)}$$

Once and for all, we define the (shared) value of the terms on the left and right of the above equation (which is an element of $C \otimes C \otimes C$) to be equal to

$$\sum_{(c)} c_{(1)} \otimes c_{(2)} \otimes c_{(3)}$$

It is easy to see how the above process may be iterated once more coproducts have been taken, i.e., by iteratively employing the coassociative property. For instance, we have

$$((\mathrm{id}_C \otimes \mathrm{id}_C \otimes \Delta) \circ (\mathrm{id}_C \otimes \Delta) \circ \Delta)(c) = ((\mathrm{id}_C \otimes \mathrm{id}_C \otimes \Delta) \circ (\Delta \otimes \mathrm{id}_C) \circ \Delta)(c)$$

In this manner, we can unambiguously obtain a notion of coassociativity for comultiplication, just as we obtained for associativity and multiplication. If the reader desires more information on Sweedler notation and its usage more broadly in the study of algebras and coalgebras, they may refer to [DNR00], where a (perhaps more) satisfactory treatment is to be found.

1.6 Quotients and Homomorphisms of Coalgebras

Having defined the concepts of a homomorphism of algebras and quotient algebras, one might be led to ask whether similar constructions hold for coalgebras. The answer to this question is in the positive, however we cannot simply work with ideals of algebras as we did above. For the correct subobject of a coalgebra, We must introduce a dual notion to that of an ideal. First we define the maps between coalgebras.

Definition 1.17. Let k be a field and let $(C, \Delta_C, \varepsilon_C)$ and $(D, \Delta_D, \varepsilon_D)$ be k-coalgebras. We refer to a k-linear mapping $\psi : C \to D$ as a *homomorphism of k-coalgebras* if the following diagrams

$$\begin{array}{ccc} C \otimes C & \xrightarrow{\psi \otimes \psi} & D \otimes D \\ {\scriptstyle \Delta_C}\uparrow & & \uparrow{\scriptstyle \Delta_D} \\ C & \xrightarrow{\psi} & D \end{array}$$

and

$$\begin{array}{ccc} C & \xrightarrow{\psi} & D \\ & {\scriptstyle \varepsilon_C}\searrow \quad \swarrow{\scriptstyle \varepsilon_D} & \\ & k & \end{array}$$

commute. In other words, the k-linear map $\psi : C \to D$ is a homomorphism of k-coalgebras if

$$((\psi \otimes \psi) \circ \Delta_C)(c) = (\Delta_D \circ \psi)(c)$$
$$\varepsilon_C(c) = (\varepsilon_D \circ \psi)(c)$$

for all $c \in C$.

Now we proceed to our definition of the dual notion of an ideal in an algebra, which will allow us to form quotients of coalgebras.

Definition 1.18. Let (C, Δ, ε) be a k-coalgebra. If a k-submodule I of C satisfies the containment

$$\Delta(I) \subseteq I \otimes C + C \otimes I$$

in addition to $\varepsilon(I) = 0$, then we call I a *coideal* of C.

Next we prove that coideals play the same role for coalgebras as ideals did for algebras.

Proposition 1.19. Let (C, Δ, ε) be a k-coalgebra, and let I be a coideal of C. Then the quotient k-module C/I is a k-coalgebra.

Proof. By construction, the coideal I is a k-submodule of C, and hence a k-module itself. Once more, let

$$\pi : C \otimes C \to \frac{C \otimes C}{I \otimes C + C \otimes I}$$

be the canonical projection map. Composing π with the comultiplication map of C, we have the k-module homomorphism

$$\pi \circ \Delta : C \to \frac{C \otimes C}{I \otimes C + C \otimes I}$$

Since $\Delta(I) \subseteq I \otimes C + C \otimes I$ by definition of a coideal, we have that $I \subseteq \ker(\pi \circ \Delta)$, and hence by the universal mapping property of kernels, there exists a k-module homomorphism

$$\overline{\pi \circ \Delta} : C/I \to \frac{C \otimes C}{I \otimes C + C \otimes I}$$

$$c + I \mapsto \Delta(c) + (I \otimes C + C \otimes I)$$

Once again from module theory, we have a k-module isomorphism

$$\Phi' : \frac{C \otimes C}{I \otimes C + C \otimes I} \xrightarrow{\sim} C/I \otimes C/I$$

and upon composing Φ' with $\overline{\pi \circ \Delta}$ we have

$$\Phi' \circ \overline{\pi \circ \Delta} : C/I \to C/I \otimes C/I$$

$$c + I \mapsto \sum_{(c)} (c_{(1)} + I) \otimes (c_{(2)} + I)$$

Set $\Delta_{C/I} = \Phi' \circ \overline{\pi \circ \Delta}$. Then $\Delta_{C/I}$ satisfies the coassociative property.

For the counit map, the fact that I is a coideal necessitates that $\varepsilon(I) = 0$, so $I \subseteq \ker(\varepsilon)$, and hence we may once again apply the universal mapping property of kernels to assert the existence of a map $\overline{\varepsilon} : C/I \to k$ defined by $c + I \mapsto \varepsilon(c)$. Taking $\varepsilon_{C/I} = \overline{\varepsilon}$ gives us our counit map. Therefore $(C/I, \Delta_{C/I}, \varepsilon_{C/I})$ is a k-coalgebra. ∎

Definition 1.20. Let (C, Δ, ε) be a k-coalgebra. If I is a coideal of C then the k-coalgebra $(C/I, \Delta_{C/I}, \varepsilon_{C/I})$ is called the *quotient k-coalgebra of C by I*.

1.7 Direct Sum and Tensor Product of Coalgebras

Now we outline how the tensor product of the underlying vector spaces of two coalgebras may be given the structure of a coalgebra.

Proposition 1.21. Let k be a field, and let $(C, \Delta_C, \varepsilon_C)$ and $(D, \Delta_D, \varepsilon_D)$ be k-coalgebras. Then the tensor product $(C \otimes D, \Delta_{C\otimes D}, \varepsilon_{C\otimes D})$ is a k-coalgebra, where $\Delta_{C\otimes D} = (\mathrm{id}_C \otimes \tau \otimes \mathrm{id}_D) \circ (\Delta_C \otimes \Delta_D)$ and $\varepsilon_{C\otimes D} : C \otimes D \to k$ is defined by $\varepsilon_{C\otimes D}(c \otimes d) = \varepsilon_C(c)\varepsilon_D(d)$ for all $c \in C$ and $d \in D$.

Proof. The tensor product $C \otimes D$ is a k-vector space, so we need only construct comultiplication and counit maps. We claim that the map

$$\Delta_{C\otimes D} : C \otimes D \to (C \otimes D) \otimes (C \otimes D)$$

$$c \otimes d \mapsto \sum_{(c),(d)} (c_{(1)} \otimes d_{(1)}) \otimes (c_{(2)} \otimes d_{(2)})$$

is our desired comultiplication. To show that $\Delta_{C\otimes D}$ is k-linear, we write it as a composition of k-linear maps: $\Delta_{C\otimes D} = (\mathrm{id}_C \otimes \tau \otimes \mathrm{id}_D) \circ (\Delta_C \otimes \Delta_D)$. Note

$$\begin{aligned}
\Delta_{C\otimes D}(c \otimes d) &= ((\mathrm{id}_C \otimes \tau \otimes \mathrm{id}_D) \circ (\Delta_C \otimes \Delta_D))(c \otimes d) \\
&= (\mathrm{id}_C \otimes \tau \otimes \mathrm{id}_D)(\Delta_C(c) \otimes \Delta_D(d)) \\
&= (\mathrm{id}_C \otimes \tau \otimes \mathrm{id}_D)\left(\sum_{(c),(d)} c_{(1)} \otimes c_{(2)} \otimes d_{(1)} \otimes d_{(2)}\right) \\
&= \sum_{(c),(d)} c_{(1)} \otimes \tau(c_{(2)} \otimes d_{(1)}) \otimes d_{(2)} \\
&= \sum_{(c),(d)} c_{(1)} \otimes d_{(1)} \otimes c_{(2)} \otimes d_{(2)} \\
&= \sum_{(c),(d)} (c_{(1)} \otimes d_{(1)}) \otimes (c_{(2)} \otimes d_{(2)})
\end{aligned}$$

holds for all $c \in C$ and $d \in D$. To check that $\Delta_{C\otimes D}$) satisfies the coassociative property, we have

$$\begin{aligned}
&((\Delta_{C\otimes D} \otimes \mathrm{id}_{C\otimes D}) \circ \Delta_{C\otimes D})(c \otimes d) \\
&\quad = (\Delta_{C\otimes D} \otimes \mathrm{id}_{C\otimes D})\left(\sum_{(c),(d)} (c_{(1)} \otimes d_{(1)}) \otimes (c_{(2)} \otimes d_{(2)})\right)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{(c),(d)} \left(\sum_{(c_{(1)}),(d_{(1)})} (c_{(1)_{(1)}} \otimes d_{(1)_{(1)}}) \otimes (c_{(1)_{(2)}} \otimes d_{(1)_{(2)}}) \right) \otimes (c_{(2)} \otimes d_{(2)}) \\
&= \sum_{(c),(d)} (c_{(1)} \otimes d_{(1)}) \otimes (c_{(2)} \otimes d_{(2)}) \otimes (c_{(3)} \otimes d_{(3)}) \\
&= \sum_{(c),(d)} (c_{(1)} \otimes d_{(1)}) \left(\sum_{(c_{(2)}),(d_{(2)})} (c_{(2)_{(1)}} \otimes d_{(2)_{(1)}}) \otimes (c_{(2)_{(2)}} \otimes d_{(2)_{(2)}}) \right) \\
&= (\mathrm{id}_{C\otimes D} \otimes \Delta_{C\otimes D}) \left(\sum_{(c),(d)} (c_{(1)} \otimes d_{(1)}) \otimes (c_{(2)} \otimes d_{(2)}) \right) \\
&= ((\mathrm{id}_{C\otimes D} \otimes \Delta_{C\otimes D}) \circ \Delta_{C\otimes D})(c \otimes d)
\end{aligned}
$$

for all $c \in C$ and $d \in D$. What remains is the counit map. We claim that

$$\varepsilon_{C\otimes D} : C \otimes D \to k$$

$$c \otimes d \mapsto \varepsilon_C(c)\varepsilon_D(d)$$

for all $c \in C$ and $d \in D$ suffices. We check the counit property directly as follows:

$$
\begin{aligned}
&((\mathrm{id}_{C\otimes D} \otimes \varepsilon_{C\otimes D}) \circ \Delta_{C\otimes D})(c \otimes d) \\
&\quad = (\mathrm{id}_{C\otimes D} \otimes \varepsilon_{C\otimes D}) \left(\sum_{(c),(d)} (c_{(1)} \otimes d_{(1)}) \otimes (c_{(2)} \otimes d_{(2)}) \right) \\
&\quad = \sum_{(c),(d)} (c_{(1)} \otimes d_{(1)}) \otimes \varepsilon_C(c_{(2)})\varepsilon_D(d_{(2)}) \\
&\quad = \sum_{(c),(d)} c_{(1)}\varepsilon_C(c_{(2)}) \otimes d_{(1)}\varepsilon_D(d_{(2)}) \otimes 1_k \\
&\quad = \sum_{(c)} c_{(1)}\varepsilon_C(c_{(2)}) \otimes \sum_{(d)} d_{(1)}\varepsilon_D(d_{(2)}) \otimes 1_k \\
&\quad = (c \otimes d) \otimes 1
\end{aligned}
$$

for all $c \in C$ and $d \in D$, where final equality follows from the counit property of $(C, \Delta_C, \varepsilon_C)$ and $(D, \Delta_D, \varepsilon_D)$. A completely analagous computation yields

$$((\varepsilon_{C\otimes D} \otimes \mathrm{id}_{C\otimes D}) \circ \Delta_{C\otimes D})(c \otimes d) = 1 \otimes (c \otimes d)$$

for all $c \in C$ and $d \in D$, so that the counit property indeed holds; hence we have that $(C \otimes D, \Delta_{C\otimes D}, \varepsilon_{C\otimes D})$ is a k-coalgebra. ∎

1.8 (Co-)Opposite (Co-)Algebras

Let k be a field. Given a k-algebra (A, ∇, η), note that there is an implicit ordering on the taking of products induced by the multiplication map ∇. By this we mean that ∇ takes tensors $a \otimes a'$ in $A \otimes A$ and outputs a product, which we often denote by aa'. However, we could just as well swap the order in which a and a' are multiplied. To refine this idea: take an algebra and, while maintaining the underlying vector space, swap the order in which elements are multiplied.

It is at once clear that this swapping gives a multiplication map, and hence gives an algebra structure on the underlying vector space and unit map of the algebra. We have the definition:

Definition 1.22. Let (A, ∇, η) be a k-algebra. Define $\nabla^{\text{opp}} = \nabla \circ \tau$, the composition of the multiplication map ∇ with the twist map τ. We call the resulting k-algebra $(A, \nabla^{\text{opp}}, \eta)$ the *opposite k-algebra of A*.

For a k-algebra (A, ∇, η), we oftentimes denote the opposite k-algebra of A, the k-algebra $(A, \nabla^{\text{opp}}, \eta)$, by simply A^{opp}. On rare occasions, we shall use the notation a^{opp} for an element of A^{opp}.

We remark that it is not always possible to find an isomorphism of algebras from an algebra to its opposite algebra. However, it is true that if (A, ∇, η) is a commutative k-algebra, then the identity map id_A is a homomorphism of k-algebras from A to A^{opp}. Indeed, the diagram

$$\begin{array}{ccc} A & \xrightarrow{\text{id}_A} & A^{\text{opp}} \\ {\scriptstyle\nabla}\uparrow & & \uparrow{\scriptstyle\nabla^{\text{opp}}=\nabla\circ\tau} \\ A \otimes A & \xrightarrow{\text{id}_A \otimes \text{id}_A} & A^{\text{opp}} \otimes A^{\text{opp}} \end{array}$$

commutes, since the commutativity of A forces $\nabla \circ \tau = \nabla$.

Example 1.23 (Enveloping Algebra)**.** We provide a brief example of a concept that, while not playing a role in our future discussion, does have far-reaching implications in other areas of study. For a k-algebra (A, ∇, η) alongside its opposite algebra A^{opp}, we can form the tensor product (which is again a k-algebra by Theorem 1.12) to get an algebra $A^{\text{env}} = A \otimes A^{\text{opp}}$, which is called the *enveloping algebra of A*.

The enveloping algebra of A is related to the study of $(A - A)$-bimodules, which are extremely important in the study of Hochschild homology and cohomology.

We also have the corresponding notion of an opposite algebra for coalgebras. This construction is used very often in the theory of coalgebras, and shall come up again and again in future sections.

Definition 1.24. Let (C, Δ, ε) be a k-coalgebra. Define $\Delta^{\text{copp}} = \tau \circ \Delta$. Then $\Delta^{\text{copp}} : C \to C \otimes C$ is a k-linear map defined by

$$\Delta^{\text{copp}}(c) = \sum_{(c)} c_{(2)} \otimes c_{(1)}$$

for all $c \in C$. The resulting k-coalgebra $(C, \Delta^{\text{copp}}, \varepsilon)$ is called the *co-opposite coalgebra of* C.

The verification that the co-opposite coalgebra is once again a coalgebra is immediate. For (C, Δ, ε).

As is the case for opposite algebras, for a k-coalgebra (C, Δ, ε), we often denote the co-opposite k-coalgebra $(C, \Delta^{\text{copp}}, \varepsilon)$ by simply C^{copp}.

Just as for opposite algebras, it is not always possible to find an isomorphism of coalgebras from a coalgebra to its co-opposite coalgebra. Once again, however, if a k-coalgebra (C, Δ, ε) is cocommutative, then the identity map id_C is a homomorphism of coalgebras from C to C^{copp}. To see this, consider the diagram

$$\begin{array}{ccc} C \otimes C & \xrightarrow{\text{id}_C \otimes \text{id}_C} & C^{\text{copp}} \otimes C^{\text{copp}} \\ \uparrow{\scriptstyle \Delta} & & \uparrow{\scriptstyle \Delta^{\text{copp}} = \tau \circ \Delta} \\ C & \xrightarrow{\text{id}_C} & C^{\text{copp}} \end{array}$$

which commutes, as the cocommutativity of C forces $\tau \circ \Delta = \Delta$, and hence we have that $\Delta^{\text{copp}} = \Delta$. In the case of coalgebras, the reverse is actually true. Namely, that if the identity id_C is a homomorphism of coalgebras, then (C, Δ, ε) is cocommutative, as can easily be checked.

1.9 Dual Algebras of a Coalgebras

For arbitrary coalgebras, the dual space of the underlying vector space naturally acquires the structure of an algebra by taking the transpose of the comultiplication and counit maps. We cannot simply take the tranpose of the comultiplication map directly, however, due to a subtle issue in terms of canonical maps. Nevertheless, alongside some minor modifications, we shall be able to make the necessary associative and unit properties of an algebra hold true.

Theorem 1.25. Let k be a field. If (C, Δ, ε) is a k-coalgebra, then $(C^*, \Delta^* \circ \iota, \varepsilon^*)$ is a k-algebra, where $\iota : C^* \otimes C^* \to (C \otimes C)^*$ is the natural injection map.

Proof. The dual space of the k-vector space C is naturally a k-vector space, so we need only construct multiplication and unit maps for C^* which satisfy the associative and unit properties. For the reader in a hurry, we quickly sketch the process by which the proof is obtained. We are given the k-coalgebra (C, Δ, ε), and hence coassociativity gives the diagram

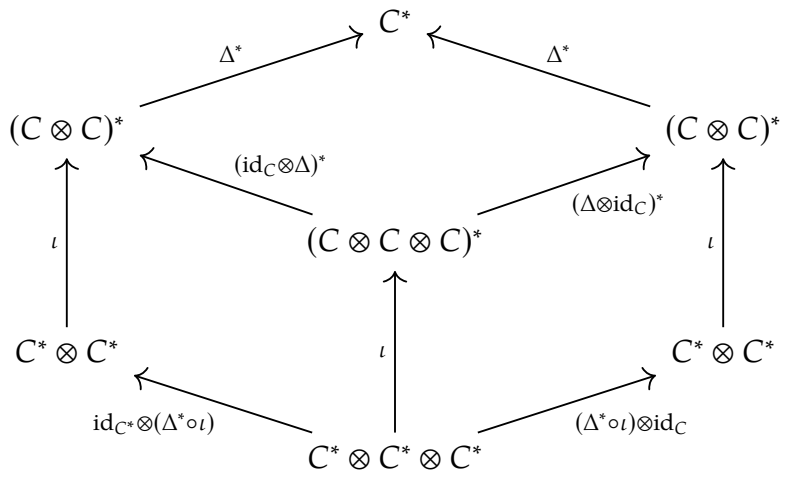
$$\begin{array}{ccc} C & \xrightarrow{\Delta} & C \otimes C \\ {\scriptstyle\Delta}\downarrow & & \downarrow{\scriptstyle\Delta\otimes \mathrm{id}_C} \\ C \otimes C & \xrightarrow{\mathrm{id}_C \otimes \Delta} & C \otimes C \otimes C \end{array}$$

which commutes. Dualizing, or flipping the arrows and going into dual spaces, yields the diagram

$$\begin{array}{ccc} C^* & \xleftarrow{\Delta^*} & (C \otimes C)^* \\ {\scriptstyle\Delta^*}\uparrow & & \uparrow{\scriptstyle(\Delta\otimes \mathrm{id}_C)^*} \\ (C \otimes C)^* & \xleftarrow{(\mathrm{id}_C \otimes \Delta)^*} & (C \otimes C \otimes C)^* \end{array}$$

which commutes. We may add in the canonical maps $\iota : C^* \otimes C^* \to (C \otimes C)^*$ and $\iota : C^* \otimes C^* \otimes C^* \to (C \otimes C \otimes C)^*$, all denoted by ι for convenience, between

k-vector spaces to obtain a new diagram



which commutes. The commutativity of the top square and the outside square give us the desired associative property. In more detail, the tranpose of the k-linear map $\Delta : C \to C \otimes C$ is defined by

$$\Delta^* : (C \otimes C)^* \to C^*$$

$$f \mapsto f \circ \Delta$$

for all linear functionals $f \in (C \otimes C)^*$. Let $\iota : C^* \otimes C^* \to (C \otimes C)^*$ denote the natural injection map. Post-composing ι with Δ^* yields the k-linear map

$$\Delta^* \circ \iota : C^* \otimes C^* \to C^*$$

$$f \otimes g \mapsto (f \otimes g) \circ \Delta$$

for all linear functionals $f, g \in C^*$. For all $c \in C$, we then have that

$$((f \otimes g) \circ \Delta)(c) = (f \otimes g)(\Delta(c)) = (f \otimes g)\left(\sum_{(c)} c_{(1)} \otimes c_{(2)}\right) = \sum_{(c)} f(c_{(1)})g(c_{(2)})$$

Once and for all, define $\nabla_{C^*} = \Delta^* \circ \iota$. We may observe that

$$\begin{aligned}
(\nabla_{C^*} \circ (\mathrm{id}_{C^*} \otimes \nabla_{C^*}))(f \otimes g \otimes h)(c) &= \nabla_{C^*}((f \otimes \nabla_{C^*}(g \otimes h))(c)) \\
&= \nabla_{C^*}(f \otimes ((g \otimes h)(\Delta(c)) \\
&= \sum_{(c)} f(c_{(1)})(g \otimes h)(\Delta(c_{(2)}) \\
&= \sum_{(c)} f(c_{(1)}) \sum_{(c_{(2)})} g(c_{(2)_{(1)}})h(c_{(2)_{(1)}}) \\
&= \sum_{(c,c_{(2)})} f(c_{(1)})g(c_{(2)_{(1)}})h(c_{(2)_{(2)}}) \\
&= (f \otimes g \otimes h)\left(\sum_{(c,c_{(2)})} c_{(1)} \otimes c_{(2)_{(1)}} \otimes c_{(2)_{(2)}}\right)
\end{aligned}$$

Now we may invoke the coassociative property of the k-coalgebra (C, Δ, ε) to get the equality

$$\sum_{(c,c_{(2)})} c_{(1)} \otimes c_{(2)_{(1)}} \otimes c_{(2)_{(2)}} = \sum_{(c,c_{(2)})} c_{(1)_{(1)}} \otimes c_{(1)_{(2)}} \otimes c_{(2)}$$

The above equality, combined with our initial work, allows us to write that

$$\begin{aligned}
(\nabla_{C^*} \circ (\mathrm{id}_{C^*} \otimes \nabla_{C^*}))(f \otimes g \otimes h)(c) &= (f \otimes g \otimes h)\left(\sum_{(c,c_{(2)})} c_{(1)_{(1)}} \otimes c_{(1)_{(2)}} \otimes c_{(2)}\right) \\
&= \sum_{(c,c_{(1)})} f(c_{(1)_{(1)}})g(c_{(1)_{(2)}})h(c_{(2)}) \\
&= \sum_{(c)} \sum_{(c_{(1)})} f(c_{(1)_{(1)}})g(c_{(1)_{(2)}})h(c_{(2)}) \\
&= \sum_{(c)} (f \otimes g)(\Delta(c_{(1)}))h(c_{(2)}) \\
&= \sum_{(c)} \nabla_{C^*}((f \otimes g)(c_{(1)}))h(c_{(2)}) \\
&= (\nabla_{C^*}(f \otimes g) \otimes h)(\Delta(c)) \\
&= \nabla_{C^*}(\nabla_{C^*}(f \otimes g) \otimes h)(c) \\
&= (\nabla_{C^*} \circ (\nabla_{C^*} \otimes \mathrm{id}_{C^*}))(f \otimes g \otimes h)(c)
\end{aligned}$$

Which shows that the map ∇_{C^*} satisfies the associative property.

In similar fashion to our quick sketch for the multiplication map, we outline the process for obtaining the unit map. The counit property from

(C, Δ, ε) gives a diagram

$$\begin{array}{ccccc} C \otimes C & \longleftarrow & C & \longrightarrow & C \otimes C \\ {\scriptstyle \varepsilon \otimes \mathrm{id}_C}\uparrow & & {\scriptstyle \mathrm{id}_C}\uparrow & & \uparrow{\scriptstyle \mathrm{id}_C \otimes \varepsilon} \\ k \otimes C & \xrightarrow{\cong} & C & \xrightarrow{\cong} & C \otimes k \end{array}$$

which commutes. We dualize once more, flipping arrows and going into dual spaces, obtaining the diagram

$$\begin{array}{ccccc} (C \otimes C)^* & \xrightarrow{\Delta^*} & C^* & \xleftarrow{\Delta^*} & (C \otimes C)^* \\ {\scriptstyle (\varepsilon \otimes \mathrm{id}_C)^*}\downarrow & & {\scriptstyle \mathrm{id}_C}\uparrow & & \uparrow{\scriptstyle (\mathrm{id}_C \otimes \varepsilon)^*} \\ (k \otimes C)^* & \xrightarrow{\cong} & C^* & \xrightarrow{\cong} & (C \otimes k)^* \end{array}$$

which commutes. Extending the diagram via the canonical maps featured above, we get the diagram

$$\begin{array}{ccccccccc} C^* \otimes C^* & \xrightarrow{\iota} & (C \otimes C)^* & \xrightarrow{\Delta^*} & C^* & \xleftarrow{\Delta^*} & (C \otimes C)^* & \xleftarrow{\iota} & C^* \otimes C^* \\ {\scriptstyle \varepsilon^* \otimes \mathrm{id}_C}\uparrow & & {\scriptstyle (\varepsilon \otimes \mathrm{id}_C)^*}\downarrow & & {\scriptstyle \mathrm{id}_C}\uparrow & & \uparrow{\scriptstyle (\mathrm{id}_C \otimes \varepsilon)^*} & & \uparrow{\scriptstyle \mathrm{id}_C \otimes \varepsilon^*} \\ k \otimes C^* & \xrightarrow{\cong} & (k \otimes C)^* & \xrightarrow{\cong} & C^* & \xrightarrow{\cong} & (C \otimes k)^* & \xrightarrow{\cong} & C^* \otimes k \end{array}$$

The inner two squares commute by the counit property, and the outer two squares commute, as we shall prove now.

Take the transpose of $\varepsilon : C \to k$ to get $\varepsilon^* : k^* \to C^*$ defined by $\varepsilon^*(f)(c) = f(\varepsilon(c))$ for all $c \in C$ and $f \in k^*$. We have the isomorphism $k^* \cong k$, and hence may write $\varepsilon^* : k \to C^*$ where $\varepsilon^*(r)(c) = r\varepsilon(c)$ for all $r \in k$ and $c \in C$.

With these constructions in mind, observe

$$\begin{aligned}
(\nabla_{C^*} \circ (\mathrm{id}_{C^*} \otimes \varepsilon^*))(f \otimes r)(c) &= \nabla_{C^*}(f \otimes \varepsilon^*(r))(c) \\
&= (f \otimes \varepsilon^*(r))(\Delta(c)) \\
&= \sum_{(c)} f(c_{(1)})\varepsilon^*(r)(c_{(2)}) \\
&= \sum_{(c)} f(c_{(1)})r(\varepsilon(c_{(2)})) \\
&= r \sum_{(c)} f(c_{(1)})\varepsilon(c_{(2)}) \\
&= r \sum_{(c)} \varepsilon(c_{(2)})f(c_{(1)}) \\
&= r \sum_{(c)} f(\varepsilon(c_{(2)})c_{(1)}) \\
&= rf\left(\sum_{(c)} \varepsilon(c_{(2)})c_{(1)}\right) \\
&= rf(c)
\end{aligned}$$

Where the final line follows since ε satisfies the counit property for the k-algebra (C, Δ, ε), and so we know in particular that

$$c = \sum_{(c)} \varepsilon(c_{(2)})c_{(1)} = \sum_{(c)} c_{(2)}\varepsilon(c_{(1)})$$

must hold for all $c \in C$. Hence $(\nabla_{C^*} \circ (\mathrm{id}_{C^*} \otimes \varepsilon^*))(f \otimes r)(c) = rf(c)$ and a completely symmetric process gives us that $(\nabla_{C^*} \circ (\varepsilon^* \otimes \mathrm{id}_{C^*}))(f \otimes r)(c) = rf(c)$ holds, so that ε^* satisfies the unit property.

In sum, we have produced the required multiplication and unit maps for C^*, and thus may conclude that $(C^*, \nabla^*, \varepsilon^*)$ is a k-algebra. ∎

We have an easy corollary from the above theorem regarding how commutativity and cocommutativity work nicely together upon passing to the dual algebra.

Corollary 1.26. Let (C, Δ, ε) be a k-coalgebra. Then (C, Δ, ε) is cocommutative if and only if $(C^*, \Delta^* \circ \iota, \varepsilon^*)$ is a commutative k-algebra.

Proof. The cocommutativity of the k-coalgebra (C, Δ, ε) gives us the equality $(\tau \circ \Delta)(c) = \Delta(c)$ for all $c \in C$. Equivalently, we have that

$$\sum_{(c)} c_{(1)} \otimes c_{(2)} = \Delta(c) = \sum_{(c)} c_{(2)} \otimes c_{(1)}$$

To show that $(C^*, \Delta^* \circ \iota, \varepsilon^*)$ is commutative, we must show

$$((\Delta^* \circ \iota) \circ \tau)(f \otimes g)(c) = (\Delta^* \circ \iota)(f \otimes g)(c)$$

for all $f, g \in C^*$ and $c \in C$. To this end, observe

$$\begin{aligned}((\Delta^* \circ \iota) \circ \tau)(f \otimes g)(c) &= (\Delta^* \circ \iota)(g \otimes f)(c) \\ &= (g \otimes f)(\Delta(c)) \\ &= \sum_{(c)} g(c_{(1)}) f(c_{(2)}) \\ &= \sum_{(c)} f(c_{(2)}) g(c_{(1)}) \\ &= (f \otimes g)(\Delta(c)) \\ &= (\Delta^* \circ \iota)(f \otimes g)(c)\end{aligned}$$

where the line 4 follows from line 3 due to the cocommutativity detailed above. Hence we have the corollary. ∎

Our next result shows that coalgebra homomorphisms induce algebra homomorphisms on the dual of the coalgebras of Theorem 1.25. This result hints at a deeper connection between a coalgebra and its dual algebra, which we shall continue to explore in later sections.

Theorem 1.27. Let $(C, \Delta_C, \varepsilon_C)$ and $(D, \Delta_D, \varepsilon_D)$ be k-coalgebras, with both $(C^*, \Delta_C^* \circ \iota, \varepsilon_C^*)$ and $(D^*, \Delta_D^* \circ \iota, \varepsilon_D^*)$ the corresponding k-algebras. Then a homomorphism of k-coalgebras $\psi : C \to D$ induces a homomorphism of k-algebras $\psi^* : D^* \to C^*$.

Proof. Suppose $\psi : C \to D$ is a homomorphism of k-coalgebras. By definition, this means the diagram

$$\begin{array}{ccc} C \otimes C & \xrightarrow{\psi \otimes \psi} & D \otimes D \\ {\scriptstyle \Delta_C}\uparrow & & \uparrow{\scriptstyle \Delta_D} \\ C & \xrightarrow{\psi} & D \end{array}$$

commutes, or equivalently that

$$(\Delta_D \circ \psi)(c) = ((\psi \otimes \psi) \circ \Delta_C)(c)$$

for all $c \in C$, as wll as that $(\psi \circ \varepsilon_C)(r) = \varepsilon_D(r)$ for all $r \in k$. We claim that the transpose of the k-linear map $\psi : C \to D$, the map $\psi^* : D^* \to C^*$

defined by $\psi^*(f)(c) = f(\psi(c))$ for all $c \in C$ and $f \in D^*$, makes the diagram

$$\begin{array}{ccc} D^* \otimes D^* & \xrightarrow{\psi^* \otimes \psi^*} & C^* \otimes C^* \\ {\scriptstyle \Delta_D^* \circ \iota_D}\downarrow & & \downarrow{\scriptstyle \Delta_C^* \circ \iota_C} \\ D^* & \xrightarrow{\phi^*} & C^* \end{array}$$

commute, where $\iota_C : C^* \otimes C^* \to (C \otimes C)^*$ and $\iota_D : D^* \otimes D^* \to (D \otimes D)^*$ are the canonical injection maps. To this end, we observe that for all $f, g \in D^*$ we have

$$\begin{aligned} (\psi^* \circ (\Delta_D^* \circ \iota_D))(f \otimes g) &= \psi^*((f \otimes g) \circ \Delta_D) \\ &= (f \otimes g) \circ \Delta_D \circ \psi \\ &= (f \otimes g) \circ (\psi \otimes \psi) \circ \Delta_C \\ &= (\psi^* \otimes \psi^*) \circ (f \otimes g) \circ \Delta_C \\ &= ((\Delta_C^* \circ \iota_C) \circ (\psi^* \otimes \psi^*))(f \otimes g) \end{aligned}$$

where line 3 follows from line 2 since $\Delta_D \circ \psi = (\psi \otimes \psi) \circ \Delta_C$ by our above remarks on the k-coalgebra homomorphism ψ.

The second diagram in the definition of a k-coalgebra homomorphism is also satisfied by $\psi : C \to D$, i.e., the diagram

$$\begin{array}{ccc} C & \xrightarrow{\psi} & D \\ & {\scriptstyle \varepsilon_C} \searrow \quad \swarrow {\scriptstyle \varepsilon_D} & \\ & k & \end{array}$$

commutes, or equivalently that $\varepsilon_C(c) = (\varepsilon_D \circ \psi)(c)$ for all $c \in C$. We claim that the transpose map $\psi^* : D^* \to C^*$ defined above makes the following diagram

$$\begin{array}{ccc} D^* & \xrightarrow{\psi^*} & C^* \\ & {\scriptstyle \varepsilon_D^*} \nwarrow \quad \nearrow {\scriptstyle \varepsilon_C^*} & \\ & k & \end{array}$$

commute. To see this, we may observe that for all $f \in k^* \cong k$, we have

$$(\psi^* \circ \varepsilon_D^*)(f) = \psi^*(f \circ \varepsilon_D) = f \circ \varepsilon_D \circ \psi = f \circ \varepsilon_C = \varepsilon_C^*(f)$$

where line 3 follows from line 2 given that $\varepsilon_D \circ \psi = \varepsilon_C$ from the above discussion. In particular, the k-linear map $\psi^* : D^* \to C^*$ satisfies the two conditions in the definition of a k-algebra homomorphism, finishing the proof. ∎

We finish this section with a proposition regarding the opposite algebra introduced at the end of Section 1. In the proposition, be careful to note the distinction between the superscripts "opp" and "copp" to denote the opposite algebra and the co-opposite coalgebra, respectively.

Proposition 1.28. Let (C, Δ, ε) be a k-coalgebra. Then the k-algebras $(C^{\text{copp}})^*$ and $(C^*)^{\text{op}}$ are equal; the dual of the co-opposite coalgebra of C is equal to the opposite algebra of C^*.

Proof. The co-opposite of C is $C^{\text{copp}} = (C, \tau \circ \Delta, \varepsilon)$, which is a k-coalgebra, and hence by Theorem 1.25, we have that $(C^{\text{copp}})^*$ is a k-algebra, where $(C^{\text{copp}})^* = (C^*, (\tau \circ \Delta)^*, \varepsilon^*)$.

By the same theorem, $(C^*, \Delta^*, \varepsilon^*)$ is a k-algebra, and hence we may take its opposite algebra via $(C^*)^{\text{opp}}$, where $(C^*)^{\text{opp}} = (C^*, \tau \circ \Delta^*, \varepsilon^*)$.

Thus, to show equality of the k-algebras in question, we need only prove that $(\tau \circ \Delta)^* = \tau \circ \Delta^*$, i.e., that the multiplication maps agree on all elements of C^*. Note that for any $f, g \in C^*$, and all $c \in C$, we have

$$\begin{aligned}
(\tau \circ \Delta)^*(f \otimes g)(c) &= ((f \otimes g) \circ (\tau \circ \Delta))(c) \\
&= (f \otimes g)\tau\left(\sum_{(c)} c_{(1)} \otimes c_{(2)}\right) \\
&= (f \otimes g)\left(\sum_{(c)} c_{(2)} \otimes c_{(1)}\right) \\
&= \sum_{(c)} f(c_{(2)}) \otimes g(c_{(1)}) \\
&= \sum_{(c)} f(c_{(2)})g(c_{(1)}) \otimes 1_k
\end{aligned}$$

where the final implication follows from the fact that $f, g : C \to k$ are linear functionals, so $f(c_{(2)})$ and $g(c_{(1)})$ are both elements of k, and hence commute with the tensor. Similarly,

$$\begin{aligned}
(\tau \circ \Delta^*)(f \otimes g)(c) &= \tau(f \otimes g)(\Delta(c)) \\
&= (g \otimes f)(\Delta(c)) \\
&= \sum_{(c)} g(c_{(1)}) \otimes f(c_{(2)}) \\
&= \sum_{(c)} g(c_{(1)})f(c_{(2)}) \otimes 1_k
\end{aligned}$$

where the last line again follows for the same reason as above. In particular, since elements of k, here $f(c_{(2)})$ and $g(c_{(1)})$, commutes with all elements of C, the two values agree, proving the proposition. ■

1.10 Finite Duals

We pause our treatment of the material briefly before discussing the process of dualizing algebras, which turns out to be considerably more nuanced than the case for coalgebras. To prepare for this discussion, we shall construct and define several notions which will allow us to answer the question of how (and if at all) more general algebras can be dualized into coalgebras.

We first recall some terminology.

Definition 1.29. Let (A, ∇, η) be a k-algebra. We say that an ideal I of A has *finite codimension* if the quotient k-vector space A/I is finite dimensional.

We now define a special subspace of the dual space for a given vector space.

Definition 1.30. Let (A, ∇, η) be a k-algebra. We call the subspace of A^* defined as

$$A^\circ = \{ f \in A^* \mid f(I) = 0 \text{ for some ideal } I \subseteq A \text{ of finite codimension } \}$$

the *finite dual of* A.

While the above definition may appear mysterious at first, we shall see below that the finite dual of a vector space has useful properties upon considering dimensions. In particular, when the a vector space is finite dimensional, the notion of a dual space and a finite dual coincide.

Proposition 1.31. Let (A, ∇, η) be a k-algebra. If A is a finite dimensional as a k-vector space, then $A^\circ = A^*$.

Proof. Suppose $\dim_k(A) < \infty$. We have the inclusion $A^\circ \subseteq A^*$, so we need only show the reverse containment. Take $f \in A^*$. Let $I = (0)$, the zero ideal of A. Clearly we have $A/I \cong A$, which, by assumption, is finite dimensional as a k-vector space; hence I has finite codimension, and furthermore $f(I) = 0$ since $f(0) = 0$ by the requirement that f is k-linear. This suffices to show that $f \in A^\circ$, so that $A^* \subseteq A^\circ$. ∎

Next we shall prove three propositions which shall aid us greatly in the next section. The first concerns taking the tranpose of the natural projection map from a ring to its quotient ideal, and the second concerns images under this tranpose. The third will follow naturally from the first two.

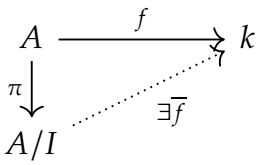
Proposition 1.32. Let (A, ∇, η) be a k-algebra. Let I be an ideal of A and let $\pi : A \to A/I$ be the canonical projection map. Then $\pi^* : (A/I)^* \to A^*$ is injective.

Proof. Taking the tranpose of the k-linear map $\pi : A \to A/I$ yields the k-linear map $\pi^* : (A/I)^* \to A^*$ defined by $\pi^*(f)(a) = (f \circ \pi)(a)$ for all $f \in (A/I)^*$ and $a \in A$.

Assume $\pi^*(f) = \pi^*(g)$. Then $f \circ \pi = g \circ \pi$ and hence for all $a \in A$ we have that $f(\pi(a)) = g(\pi(a))$, or equivalently $f(a+I) = g(a+I)$. Since f and g agree on all cosets $a + I \in A/I$, this shows $f = g$; hence π^* is injective. ∎

Proposition 1.33. Let (A, ∇, η) be a k-algebra. Let $f \in A^\circ$ and suppose that $f(I) = 0$ for an ideal I of A. Then there exists a unique element $\overline{f} \in (A/I)^*$ such that $\pi^*(\overline{f}) = f$.

Proof. Let $f \in A^\circ$ and take I to be the ideal of A for which $f(I) = 0$. We have the linear functional $f : A \to k$, which is a k-linear map, and we also have that $I \subseteq \ker f$ since $f(r) = 0$ for all $r \in I$ by assumption. Let $\pi : A \to A/I$ be the natural projection map. By the universal mapping property for kernels, there exists a k-linear map $\overline{f}$ such that the diagram



commutes. In particular, we have that $\pi^*(\overline{f}) = \overline{f} \circ \pi = f$. Now we must prove that such an $\overline{f}$ is unique. However this is clear, for if $\overline{g} \in (A/I)^*$ satisfied $\pi^*(\overline{g}) = f$, then necessarily $\pi^*(\overline{f}) = \pi^*(\overline{g})$, and by Proposition 1.32, the injectivity of π^* gives $\overline{f} = \overline{g}$. ∎

Now we come to the most important of the three propositions. This proposition will prove exceedingly helpful in the next section, where we discuss the process of dualizing algebras.

We preface this proposition with a quick remark. For (A, ∇, η) a k-algebra, we may take the tranpose of the multiplication map ∇ to obtain

$$\nabla^* : A^* \to (A \otimes A)^*$$

$$f \mapsto f \circ \nabla$$

For convenience, we define $(f \circ \nabla)(a \otimes b) = f(ab)$ for all $f \in A^*$ and $a, b \in A$.

Proposition 1.34. Let (A, ∇, η) be a k-algebra. Then, with the transpose of the multiplication map ∇ is given by $\nabla^* : A^* \to (A \otimes A)^*$, we have the containment $\nabla^*(A^\circ) \subseteq A^\circ \otimes A^\circ$.

Proof. Suppose $f \in A^\circ$. Then there exists an ideal I of A with finite codimension for which $f(I) = 0$. Take this ideal and form the quotient k-algebra $(A/I, \nabla_{A/I}, \eta_{A/I})$ via Proposition 1.9. Recall that

$$\nabla_{A/I} : A/I \otimes A/I \to A/I$$

$$a + I \otimes b + I \mapsto ab + I$$

for all $a, b \in A$. Since A/I is finite dimensional as a k-vector space, we know that $(A/I \otimes A/I)^* = (A/I)^* \otimes (A/I)^*$, and hence that the transpose of $\nabla_{A/I}$ satisfies

$$\nabla^*_{A/I} : (A/I)^* \to (A/I \otimes A/I)^* = (A/I)^* \otimes (A/I)^*$$

With the above in mind, note that Proposition 1.33 asserts the existence of a linear functional $\overline{f} \in (A/I)^*$ for which $\pi^*(\overline{f}) = f$, i.e., for which $\overline{f} \circ \pi = f$. Observe

$$\begin{aligned}
\nabla^*(f)(a \otimes b) &= (f \circ \nabla)(a \otimes b) \\
&= (\overline{f} \circ \pi \circ \nabla)(a \otimes b) \\
&= (\overline{f} \circ \pi)(ab) \\
&= \overline{f}(ab + I) \\
&= (\overline{f} \circ \nabla_{A/I})(a + I \otimes b + I) \\
&= \nabla^*_{A/I}(\overline{f})(a + I \otimes b + I) \\
&= \nabla^*_{A/I}(\overline{f})(\pi(a) \otimes \pi(b))
\end{aligned}$$

Now note that $\nabla^*_{A/I}(\overline{f}) \in (A/I)^* \otimes (A/I)^*$ may be represented as a product of linear functionals in $(A/I)^*$, in other words, there exists $f_i, g_i \in (A/I)^*$

for which $\nabla^*_{A/I}(\overline{f}) = \sum_i f_i \otimes g_i$. Using this fact, the above becomes

$$\begin{aligned}
\nabla^*(f)(a \otimes b) &= \nabla^*_{A/I}(\overline{f})(\pi(a) \otimes \pi(b)) \\
&= \left(\sum_i f_i \otimes g_i \right) (\pi(a) \otimes \pi(b)) \\
&= \sum_i (f_i \circ \pi)(a) \otimes (g_i \circ \pi)(b) \\
&= \sum_i \pi^*(f_i)(a) \otimes \pi^*(g_i)(b) \\
&= \left(\sum_i \pi^*(f_i) \otimes \pi^*(g_i) \right) (a \otimes b)
\end{aligned}$$

Now, in order to show that $\nabla^*(A^\circ) \subseteq A^\circ \otimes A^\circ$, we must show that $\pi^*(f_i)$ and $\pi^*(g_i)$ are elements of A°. It suffices to show that $\pi^*(f_i)$ and $\pi^*(g_i)$ both take I to 0. However, this is trivial, for

$$\pi^*(f_i)(I) = (f_i \circ \pi)(I) = f_i(\pi(I)) = f_i(0) = 0$$

since $\pi : A \to A/I$ has kernel I. The above holds for $\pi^*(g_i)$ as well. In particular, for $f \in A^\circ$ our work shows that

$$\nabla^*(f) = \sum_i \pi^*(f_i) \otimes \pi^*(g_i) \in A^\circ \otimes A^\circ$$

and hence $\nabla^*(A^\circ) \subseteq A^\circ \otimes A^\circ$, as desired. ■

In the next section we apply the propositions above to great effect.

1.11 Dual Coalgebras of Algebras

As much as we would like to recreate our success in dualizing coalgebras to form algebras, an algebra, in general, cannot be dualized into a coalgebra. The obstruction to this lies in an artifact from the theory of vector space duals. Namely, for a vector space V over a field k, we always have the containment $V^* \otimes V^* \subseteq (V \otimes V)^*$, but not necessarily that $V^* \otimes V^* = (V \otimes V)^*$. The condition for equality is that the k-vector space V is finite dimensional.

To see why this is an issue, if (A, ∇, η) is a k-algebra, then the tranpose of the multiplication map ∇ is given by

$$\nabla^* : A^* \to (A \otimes A)^*$$

$$f \mapsto f \circ \nabla$$

for all linear functionals $f \in A^*$. We cannot restrict the domain of the map ∇^* as we did for the dualizing of coalgebras, as this time $(A \otimes A)^*$ is the codomain of the function rather than the domain. Thus it is not always the case that the tranpose ∇^* gives a comultiplication map $A^* \to A^* \otimes A^*$.

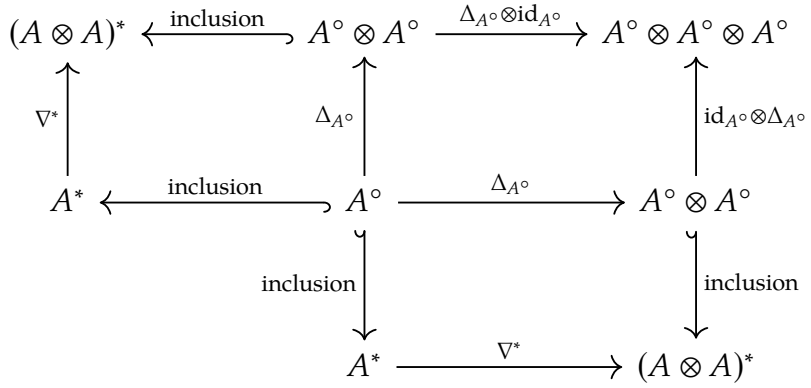
We discuss the best possible remedy to this issue in this section, and use the finite dual of a vector space considered in the previous section to aid us in our inquiry.

Theorem 1.35. Let (A, ∇, η) is a k-algebra, and let A° denote the finite dual of A. Then $(A^\circ, \Delta_{A^\circ}, \varepsilon_{A^\circ})$ is a k-coalgebra, where $\Delta_{A^\circ} = \nabla^*|_{A^\circ}$ and $\varepsilon_{A^\circ} = \eta^*|_{A^\circ}$.

Proof. Take the tranpose of the multiplication map ∇ as $\nabla^* : A^* \to (A \otimes A)^*$. We have $A^\circ \subseteq A^*$ by definition. From Proposition 1.34, we have $\nabla^*(A^\circ) \subseteq A^\circ \otimes A^\circ$. Now let $\Delta_{A^\circ} = \nabla^*|_{A^\circ}$. We have a commutative diagram

$$\begin{array}{ccc} A^\circ & \xrightarrow{\Delta_{A^\circ} = \nabla^*|_{A^\circ}} & A^\circ \otimes A^\circ \\ \text{inclusion} \downarrow & & \downarrow \text{inclusion} \\ A^* & \xrightarrow{\nabla^*} & (A \otimes A)^* \end{array}$$

Which we may extend to a diagram



If the square in the right hand top corner commutes, we have our comultiplication map. To start, Δ_{A° is a k-linear map, as it is the restriction of a k-linear map, and furthermore Δ_{A° is defined by

$$\Delta_{A^\circ} : A^\circ \to A^\circ \otimes A^\circ$$

$$f(a) \mapsto \nabla^*(f)(a)$$

for all linear functionals $f \in A^\circ$ and elements $a \in A$. We show that Δ_{A° satisfies the coassociative property. First, remark that since (A, ∇, η) is a k-algebra, we have the associative property

$$(\nabla \circ (\mathrm{id}_A \otimes \nabla))(a \otimes b \otimes c) = (\nabla \circ (\nabla \otimes \mathrm{id}_A))(a \otimes b \otimes c)$$

for all $a, b, c \in A$. Before we proceed, note that $\mathrm{id}_{A^\circ} = \mathrm{id}_{A^*}|_{A^\circ}$, where $\mathrm{id}_{A^*} = \mathrm{id}_A^*$. Under these identifications, observe that for all $a, b, c, \in A$ and linear functionals $f \in A^\circ$, we have

$$\begin{aligned}
((\mathrm{id}_{A^\circ} \otimes \Delta_{A^\circ}) \circ \Delta_{A^\circ})(f)(a \otimes b \otimes c) &= (\mathrm{id}_{A^\circ} \otimes \Delta_{A^\circ})(\nabla^*(f)(a \otimes b \otimes c)) \\
&= (\mathrm{id}_A^* \otimes \nabla^*)(\nabla^*(f)(a \otimes b \otimes c)) \\
&= \nabla^*(f)(\mathrm{id}_A \otimes \nabla)(a \otimes b \otimes c) \\
&= (f \circ \nabla \circ (\mathrm{id}_A \otimes \nabla))(a \otimes b \otimes c) \\
&= (f \circ \nabla \circ (\nabla \otimes \mathrm{id}_A))(a \otimes b \otimes c) \\
&= ((\nabla^* \otimes \mathrm{id}_A^*) \circ \nabla^*(f))(a \otimes b \otimes c) \\
&= (\Delta_{A^\circ} \otimes \mathrm{id}_{A^\circ})(\nabla^*(f)(a \otimes b \otimes c)) \\
&= ((\Delta_{A^\circ} \otimes \mathrm{id}_{A^\circ}) \circ \Delta_{A^\circ})(f)(a \otimes b \otimes c)
\end{aligned}$$

where line 5 follows from line 4 from the associative property of A. Hence the map Δ_{A° satisfies the coassociative property.

Next, we construct a counit map. The unit property of (A, ∇, η) gives us that

$$(\nabla \circ (\eta \otimes \mathrm{id}_A))(r \otimes a) = ra = (\nabla \circ (\mathrm{id}_A \otimes \eta))(a \otimes r)$$

Take the transpose of the unit map $\eta : k \to A$ given by $\eta^* : A^* \to k^* \cong k$. Now let $\varepsilon_{A^\circ} = \eta^*|_{A^\circ}$. We have a diagram

$$\begin{array}{ccc} A^\circ & \xrightarrow{\varepsilon_{A^\circ} = \eta^*|_{A^\circ}} & k^* \cong k \\ {\scriptstyle \text{inclusion}}\downarrow & & \| \\ A^* & \xrightarrow{\eta^*} & k^* \cong k \end{array}$$

which we may extend to the following

$$\begin{array}{ccccc} A^\circ \otimes A^\circ & \xrightarrow{\mathrm{id}_{A^\circ} \otimes \varepsilon_{A^\circ}} & A^\circ \otimes k^* \cong A^\circ \otimes k & & \\ {\scriptstyle \varepsilon_{A^\circ} \otimes \mathrm{id}_{A^\circ}}\downarrow & \nwarrow^{\Delta_{A^\circ}} & \uparrow{\scriptstyle -\otimes 1} & & \\ k^* \otimes A^\circ \cong k \otimes A^\circ & \xleftarrow{1 \otimes -} & A^\circ & \xrightarrow{\varepsilon_{A^\circ} = \eta^*|_{A^\circ}} & k^* \cong k \\ & & {\scriptstyle \text{inclusion}}\downarrow & & \| \\ & & A^* & \xrightarrow{\eta^*} & k^* \cong k \end{array}$$

Commutativity of the top left square gives the counit property, which we now prove. Note that

$$\varepsilon_{A^\circ}(f)(r) = \eta^*(f)(r) = f(\eta(r)) = f(r1_A) = rf(1_A) = f(1_A)(r)$$

which follows by taking $a = 1_A$ in the unit property above. With this in mind. observe that for all $r \in k$, $a \in A$, and linear functionals $f \in A^\circ$, we have

$$\begin{aligned} ((\varepsilon_{A^\circ} \otimes \mathrm{id}_{A^\circ}) \circ \Delta_{A^\circ})(f)(r \otimes a) &= (\eta^* \otimes \mathrm{id}_A^*)(\nabla^*(f)(r \otimes a)) \\ &= \nabla^*(f)(\eta \otimes \mathrm{id}_A)(r \otimes a) \\ &= (f \circ \nabla \circ (\eta \otimes \mathrm{id}_A))(r \otimes a) \\ &= f(ra) \\ &= rf(a) \\ &= (1 \otimes f)(r \otimes a) \end{aligned}$$

where line 4 follows from line 3 given the unit property mentioned previously. In a completely analagous manner, we obtain that

$$((\mathrm{id}_{A^\circ} \otimes \varepsilon_{A^\circ}) \circ \Delta_{A^\circ})(f)(a \otimes r) = (f \otimes 1)(a \otimes r)$$

And hence ε_{A° satisfies the counit property for A°. These verifications suffice to prove that $(A^\circ, \Delta_{A^\circ}, \varepsilon_{A^\circ})$ is a k-coalgebra. ∎

Theorem 1.35 is perhaps the best we can do in terms of dualizing algebras into coalgebras. By this we mean that if (A, ∇, η) is a k-algebra such that A is finite dimensional as a k-vector space, then Proposition 1.31 gives $A^\circ = A^*$, and by the theorem, $(A^*, \Delta_{A^*}, \varepsilon_{A^*})$ is a k-coalgebra. We cannot say anyhting definitive about the case where A is infinite dimensional, at least for now.

We have an easy consequence of Theorem 1.35 regarding commutativity.

Corollary 1.36. If (A, ∇, η) is a commutative k-algebra, then $(A^\circ, \Delta_{A^\circ}, \varepsilon_{A^\circ})$ is a cocommutative k-coalgebra.

Proof. To show that $(A^\circ, \Delta_{A^\circ}, \varepsilon_{A^\circ})$ is cocommutative, we need only show that

$$(\tau \circ \Delta_{A^\circ})(f)(a \otimes b) = \Delta_{A^\circ}(f)(a \otimes b)$$

for all $f \in A^\circ$ and $a, b \in A$. First we remark that the transpose of the twist map $\tau : A \otimes A \to A \otimes A$ is given by $\tau^* : A^* \otimes A^* \to A^* \otimes A^*$. We also remark that the commutativity of (A, ∇, η) gives $(\nabla \circ \tau)(a \otimes b) = \nabla(a \otimes b)$ for all $a, b \in A$. With this in mind, observe

$$\begin{aligned}
(\tau \circ \Delta_{A^\circ})(f)(a \otimes b) &= (\tau^* \circ \nabla^*(f))(a \otimes b) \\
&= (\nabla^*(f) \circ \tau)(a \otimes b)) \\
&= f((\nabla \circ \tau)(a \otimes b)) \\
&= f(\nabla(a \otimes b)) \\
&= \nabla^*(f)(a \otimes b) \\
&= \Delta_{A^\circ}(f)(a \otimes b)
\end{aligned}$$

where line 4 follows from line 3 from the commutativity of (A, ∇, η). Hence $(A^\circ, \Delta_{A^\circ}, \varepsilon_{A^\circ})$ is cocommutative. ∎

❖ Hopf Algebras and Bialgebras

2.1 Bialgebras

Definition 2.1. Let k be a field. A k-vector space B equipped with four k-linear maps ∇, η, Δ, and ε is called a *k-bialgebra* if the following conditions hold:

1. (B, ∇, η) is a k-algebra.
2. (B, Δ, ε) is a k-coalgebra.
3. The maps Δ and ε are homomorphisms of k-algebras.

Fix a field k. In keeping with our current notational tradition, we often denote a k-bialgebra by $(B, \nabla, \eta, \Delta, \varepsilon)$. When we wish to emphasize the underlying k-algebra or k-coalgebra structure of the k-bialgebra $(B, \nabla, \eta, \Delta, \varepsilon)$, we shall use the shortened tuple (B, ∇, η) and (B, Δ, ε), respectively.

Condition (3) in the definition of a bialgebra may seem curious at first, however passing to Sweedler notation will quickly make clear its purpose. For a k-bialgebra $(B, \nabla, \eta, \Delta, \varepsilon)$, we know that $\Delta : B \to B \otimes B$ is homomorphisms of the k-algebras (B, ∇, η) and $(B \otimes B, \nabla_{B\otimes B}, \eta_{B\otimes B})$ from Theorem 1.12. This fact ensures that the diagrams

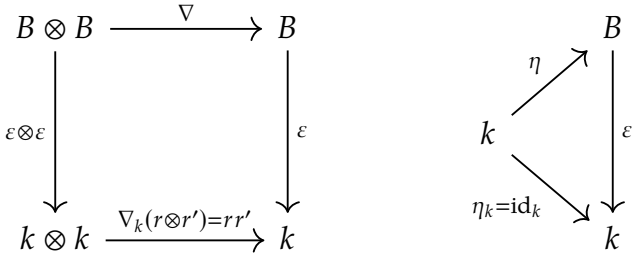
$$\begin{array}{ccc} B \otimes B & \xrightarrow{\nabla} & B \\ {\scriptstyle \Delta\otimes\Delta}\downarrow & & \downarrow{\scriptstyle \Delta} \\ (B \otimes B) \otimes (B \otimes B) & \xrightarrow{\nabla_{B\otimes B}} & B \otimes B \end{array} \qquad \begin{array}{ccc} & & B \\ & {\scriptstyle \eta}\nearrow & \downarrow{\scriptstyle \Delta} \\ k & & \\ & {\scriptstyle \eta_{B\otimes B}}\searrow & \\ & & B \otimes B \end{array}$$

commute, where $\eta_{B\otimes B}(r) = \eta(r) \otimes 1$. In other words, if we let $\nabla(a \otimes b) = ab$ for all $a, b \in B$, then $(\Delta \circ \nabla)(ab) = \Delta(ab)$, and so we have that

$$\begin{aligned} \Delta(ab) &= \sum_{(ab)} (ab)_{(1)} \otimes (ab)_{(2)} \\ &= \Delta(a)\Delta(b) \\ &= \left(\sum_{(a)} a_{(1)} \otimes a_{(2)} \right) \left(\sum_{(b)} b_{(1)} \otimes b_{(2)} \right) \\ &= \sum_{(a,b)} a_{(1)}b_{(1)} \otimes a_{(2)}b_{(2)} \end{aligned}$$

for all $a, b \in B$. Hence the requirement that Δ be a k-algebra homomorphism ensures that the comultiplication map Δ works nicely with the multiplication

map ∇. The requirement that $\varepsilon : B \to k$ be a k-algebra homomorphism from (B, ∇, η) to (k, ∇_k, η_k) from Example 1.4 means that the diagrams



commute. In other words, if we denote $\nabla(a \otimes b) = ab$ for all $a, b \in B$, so that $(\varepsilon \circ \nabla)(a \otimes b) = \varepsilon(ab)$, we have

$$\varepsilon(ab) = (\nabla_k \circ (\varepsilon \otimes \varepsilon))(ab) = \varepsilon(a)\varepsilon(b)$$

for all $a, b \in B$. As we can see, condition (3) in the definition of a k-bialgebra encodes much useful information and relations, each of which will aid us greatly in future computations.

Given our previous notions of a commutative algebra and a cocommutative coalgebra, and the fact that a bialgebra combines these structures, we make the following definition.

Definition 2.2. We refer to a k-bialgebra $(B, \nabla, \eta, \Delta, \varepsilon)$ as *bicommutative* if (B, ∇, η) is a commutative k-algebra and (B, Δ, ε) is a cocommutative k-coalgebra.

Now we present a slew of examples of bialgebras.

Example 2.3 (*Group Ring*)**.** Let k be a field, let G be a group. Then the group ring $k[G]$ can be given the structure of a k-bialgebra. For the multiplication map, consider $\nabla_{k[G]} : k[G] \otimes k[G] \to k[G]$ defined by $\nabla_{k[G]}(a \otimes b) = ab$ for all $a, b \in k[G]$. For the unit map, consider $\eta_{k[G]} : k \to k[G]$ defined by $\eta_{k[G]}(r) = r$ for all $r \in k$.

For a comultiplication map, consider $\Delta_{k[G]} : k[G] \to k[G] \otimes k[G]$ defined by

$$\sum_{g \in G} \alpha_g [g] \mapsto \sum_{g \in G} \alpha_g [g \otimes g]$$

and for the counit map, consider $\varepsilon_{k[G]} : k[G] \to k$ defined by

$$\sum_{g \in G} \alpha_g [g] \mapsto \sum_{g \in G} \alpha_g$$

With the constructions above, it is an easy check to see that $(k[G], \nabla_{k[G]}, \eta_{k[G]})$ is a k-algebra and $(k[G], \Delta_{k[G]}, \varepsilon_{k[G]})$ is a k-coalgebra. Furthermore, it is easy

to see that $\Delta_{k[G]}$ and $\varepsilon_{k[G]}$ are k-algebra homomorphisms; hence we have that $(k[G], \nabla_{k[G]}, \eta_{k[G]}, \Delta_{k[G]}, \varepsilon_{k[G]})$ is a k-bialgebra, which we refer to as the *group bialgebra*.

2.2 Dual Bialgebras

We now concern ourselves with the dual of a bialgebra, which can be naturally taken by virtue of the underlying algebra and coalgebra structure inherent in a bialgebra. First we show that the dual, in the usual sense, of a bialgebra is once more a bialgebra. Then we shall then prove a small result on commutativity and cocommutativity.

Theorem 2.4. Let k be a field. If $(B, \nabla, \eta, \Delta, \varepsilon)$ is a k-bialgebra such that B is finite dimensional as a k-vector space, then $(B^*, \Delta^*, \varepsilon^*, \nabla^*, \eta^*)$ is a k-bialgebra.

Proof. We have the underlying k-algebra (B, ∇, η) and the underlying k-coalgebra (B, Δ, ε). Proposition 1.25 asserts that $(B^*, \Delta^*, \varepsilon^*)$ is a k-algebra, and since B is finite dimensional, Proposition 1.35 asserts that (B^*, ∇^*, η^*) is a k-coalgebra. To prove that $(B^*, \Delta^*, \varepsilon^*, \nabla^*, \eta^*)$ is a k-bialgebra we need only show that ∇^* and η^* are homomorphisms of k-algebras.

To start, for any $f, g \in B^*$ and $a, b \in B$, we have

$$\begin{aligned}
\nabla^*(fg)(a \otimes b) &= (\nabla^* \circ \Delta^*)(f \otimes g)(a \otimes b) \\
&= \Delta^*(f \otimes g)(\nabla(a \otimes b)) \\
&= (f \otimes g)(\Delta(ab)) \\
&= (f \otimes g)\left(\sum_{(a,b)} a_{(1)}b_{(1)} \otimes a_{(2)}b_{(2)}\right) \\
&= \sum_{(a,b)} f(a_{(1)}b_{(1)}) \otimes g(a_{2)}b_{(2)}) \\
&= \sum_{(a,b)} f(\nabla(a_{(1)} \otimes b_{(1)})) \otimes g(\nabla(a_{(2)} \otimes b_{(2)})) \\
&= \sum_{(a,b)} \nabla^*(f)(a_{(1)} \otimes b_{(1)}) \otimes \nabla^*(g)(a_{(2)} \otimes b_{(2)}) \\
&= \Delta^* \circ (\nabla^*(f) \otimes \nabla^*(g))(\mathrm{id}_B \otimes \tau \otimes \mathrm{id}_B)\left(\sum_{(a,b)} a_{(1)} \otimes a_{(2)} \otimes b_{(1)} \otimes b_{(2)}\right) \\
&= (\Delta^* \circ (\nabla^*(f) \otimes \nabla^*(g))(\mathrm{id}_B \otimes \tau \otimes \mathrm{id}_B)(\Delta \otimes \Delta))(a \otimes b) \\
&= (\Delta^* \circ (\nabla^*(f) \otimes \nabla^*(g))(\mathrm{id}_B \otimes \tau \otimes \mathrm{id}_B) \circ \Delta_{B \otimes B})(a \otimes b)
\end{aligned}$$

Which follows since $\Delta_{B\otimes B} = (\mathrm{id}_B \otimes \tau \otimes \mathrm{id}_B) \circ (\Delta \otimes \Delta)$ by construction of the map back in Proposition 1.21. Now we can take the dual of $\Delta_{B\otimes B}$ to obtain

$$\Delta^*_{B\otimes B} = (\Delta^* \otimes \Delta^*) \circ (\mathrm{id}_{B^*} \otimes \tau \otimes \mathrm{id}_{B^*})$$

Substituting this fact into our above derivation, we get

$$\begin{aligned}
\nabla^*(fg)(a \otimes b) &= \Delta^*_{B\otimes B}(\nabla^*(f) \otimes \nabla^*(g)))(a \otimes b) \\
&= \nabla_{B^*\otimes B^*}(\nabla^*(f) \otimes \nabla^*(g)))(a \otimes b) \\
&= (\nabla^*(f)\nabla^*(g)))(a \otimes b)
\end{aligned}$$

In particular, we have proved that

$$\nabla^*(fg)(a \otimes b) = (\nabla^*(f)\nabla^*(g)))(a \otimes b)$$

which suffices to show that ∇^* is a homomorphism of k-algebras.

Now we prove that $\eta^* : B^* \to k$ is a homomorphism of k-algebras. For any $f, g \in B^*$ and $r \in k$ we have

$$\begin{aligned}
\eta^*(fg)(r) &= (\eta^* \circ \Delta^*)(f \otimes g)(r) \\
&= \Delta^*(f \otimes g)(\eta(r)) \\
&= r\Delta^*(f \otimes g)(1_B \\
&= r\Delta^*(f \otimes g)(\Delta(1_B) \\
&= r\Delta^*(f \otimes g)(1_B \otimes 1_B) \\
&= rf(1_B)g(1_B) \\
&= r\eta^*(f)\eta^*(g) \\
&= (\eta^*(f)\eta^*(g))(r)
\end{aligned}$$

Which follows since $f(1_B) = f(\eta(1_k)) = \eta^*(f)$ for both linear functionals f and g. Hence we have proven

$$\eta^*(fg)(r) = (\eta^*(f)\eta^*(g))(r)$$

and so η^* is a homomorphism of k-algebras as well; these two facts suffice to make $(B^*, \Delta^*, \varepsilon^*, \nabla^*, \eta^*)$ a k-bialgebra, as desired. ∎

Corollary 2.5. Let $(B, \nabla, \eta, \Delta, \varepsilon)$ be a finite dimensional k-bialgebra. If we know that $(B, \nabla, \eta, \Delta, \varepsilon)$ is commutative, then $(B^*, \Delta^*, \varepsilon^*, \nabla^*, \eta^*)$ is cocommutative. If $(B, \nabla, \eta, \Delta, \varepsilon)$ is cocommutative, then $(B^*, \Delta^*, \varepsilon^*, \nabla^*, \eta^*)$ is commutative.

Proof. If $(B, \nabla, \eta, \Delta, \varepsilon)$ is commutative, then we know that the underlying k-algebra (B, ∇, η) is commutative. Proposition 1.36 asserts that (B^*, ∇^*, η^*) is a cocommutative k-coalgebra; hence the k-bialgebra of Theorem 2.4 given by $(B^*, \Delta^*, \varepsilon^*, \nabla^*, \eta^*)$ is cocommutative.

Alternatively, if (B, Δ, ε) is cocommutative, then by Proposition 1.26 we have that the k-algera $(B^*, \Delta^*, \varepsilon^*)$ is commutative, and hence that the k-bialgebra $(B^*, \Delta^*, \varepsilon^*, \nabla^*, \eta^*)$ is commutative. ■

2.3 Convolution Monoids and the Convolution Product

Before we can proceed in defining our desired object of study, we introduce a conveninent product, which will turn out to be a multiplication map for a special algebra, on the set of linear transformations between two vector spaces, which, as we may recall, is also a vector space over the base field.

Definition 2.6. Let k be a field. Let (A, ∇, η) be a k-algebra and let (C, Δ, ε) be a k-coalgebra. For any k-linear maps $f, g \in \mathrm{Hom}_k(C, A)$, the *convolution product* is the k-linear map defined by

$$(f * g)(c) = (\nabla \circ (f \otimes g) \circ \Delta)(c)$$

for all $c \in C$.

The above definition may seem mysterious at first, however the purpose of such a construction becomes clear once we place the above in the context of Sweedler notation. For a field k, with (A, ∇, η) a k-algebra and (C, Δ, ε) a k-coalgebra, we have

$$\begin{aligned}(f * g)(c) &= (\nabla \circ (f \otimes g) \circ \Delta)(c) \\ &= \nabla(f \otimes g)\left(\sum_{(c)} c_{(1)} \otimes c_{(2)}\right) \\ &= \nabla\left(\sum_{(c)} f(c_{(1)}) \otimes g(c_{(2)})\right) \\ &= \sum_{(c)} f(c_{(1)}) g(c_{(2)})\end{aligned}$$

for all $f, g \in \mathrm{Hom}_k(C, A)$ and $c \in C$. In a sense, the convolution product allows functions from $C \to A$ to work nicely with the comultiplication of a coalgebra.

The convolution product defined above gives a special structure to the set of linear transformations on the underlying vector spaces of an algebra and a coalgebra. This structure is that of a monoid, which, as we may recall, is a set which is closed under an associative binary operation equipped with an identity element. Monoids may be thought of as a generalization of groups, but without the requirement that each element have an inverse in the group.

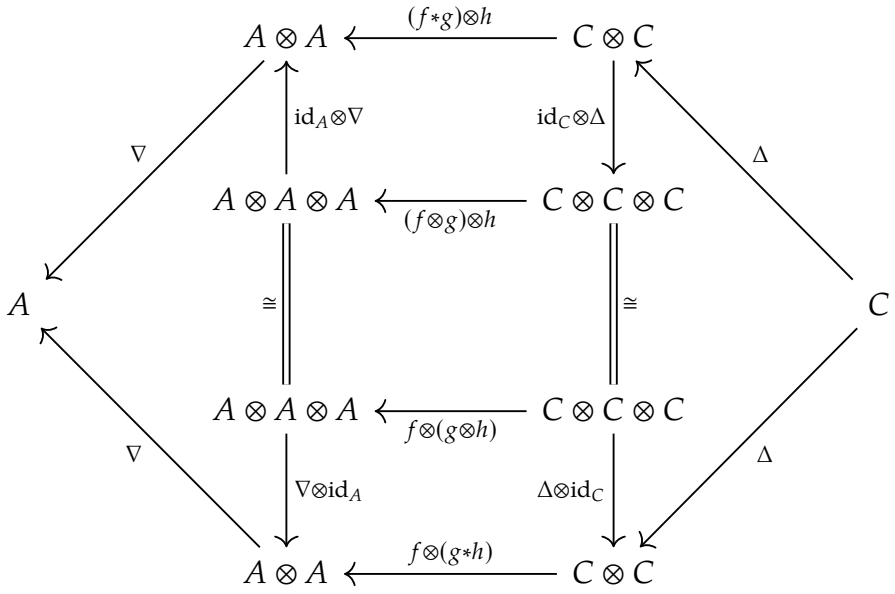
Theorem 2.7. Let (A, ∇, η) be a k-algebra and let (C, Δ, ε) be a k-coalgebra. Then $\mathrm{Hom}_k(C, A)$ equipped with the convolution product $*$ is a monoid, with identity element given by the map $\eta \circ \varepsilon = \eta \circ \varepsilon$.

Proof. For $f, g \in \mathrm{Hom}_k(C, A)$, the convolution product $f * g$ is defined as the composition of k-linear maps, and is hence also an element of $\mathrm{Hom}_k(C, A)$, giving closure under $*$. Now we must show that $(f * g) * h) = f * (g * h)$ for all maps $f, g, h \in \mathrm{Hom}_k(C, A)$, i.e., that $*$ is an associative binary operation.

The assumed associative property of (A, ∇, η), and the coassociative property of (C, Δ, ε), give us that the following diagrams

$$\begin{array}{ccc} A \otimes A & \xleftarrow{\mathrm{id}_A \otimes \nabla} & A \otimes A \otimes A \\ {\scriptstyle\nabla}\downarrow & & \downarrow{\scriptstyle \nabla \otimes \mathrm{id}_A} \\ A & \xleftarrow{\nabla} & A \otimes A \end{array} \qquad \begin{array}{ccc} C \otimes C \otimes C & \xleftarrow{\mathrm{id}_C \otimes \Delta} & C \otimes C \\ {\scriptstyle\Delta \otimes \mathrm{id}_C}\uparrow & & \uparrow{\scriptstyle \Delta} \\ C \otimes C & \xleftarrow{\Delta} & C \end{array}$$

commute. Combining these diagrams together using the k-linear maps induced by the convolution product yields the diagram



which necessarily commutes, where the isomorphisms on the left and right of the center square are given by the canonical ones $(A \otimes A) \otimes A \cong A \otimes (A \otimes A)$ and $(C \otimes C) \otimes C \cong C \otimes (C \otimes C)$. We could also show associativity directly,

as

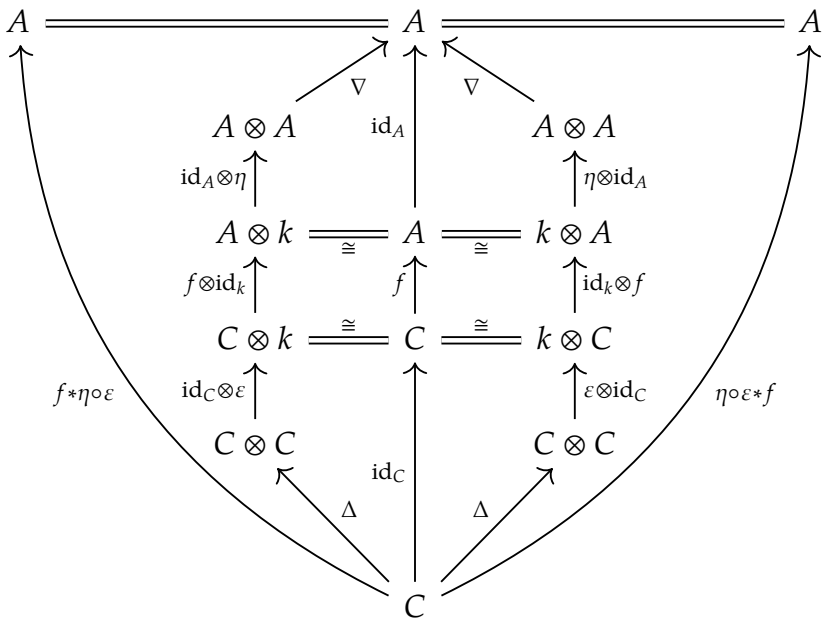
$$\begin{aligned}
(f*(g*h))(c) &= (\nabla\circ(f\otimes(g*h))\circ\Delta)(c)\\
&= \sum_{(c)} f(c_{(1)})(g*h)(c_{(2)})\\
&= \sum_{(c)} f(c_{(1)})(\nabla\circ(g\otimes h)\circ\Delta)(c_{(2)}))\\
&= \sum_{(c)} f(c_{(1)})\sum_{(c_{(2)})} g(c_{(2)_{(1)}})h(c_{(2)_{(2)}})\\
&= \sum_{(c)} f(c_{(1)})g(c_{(2)})h(c_{(3)})\\
&= \sum_{(c)} f(c_{(1)_{(1)}})g(c_{(1)_{(2)}})h(c_{(2)})\\
&= \sum_{(c)}\sum_{(c_{(1)})} f(c_{(1)_{(1)}})g(c_{(1)_{(2)}})h(c_{(2)})\\
&= \sum_{(c)}(f*g)(c_{(1)})h(c_{(2)})\\
&= (\nabla\circ((f*g)\otimes h)\circ\Delta)(c)\\
&= (f*(g*h))(c)
\end{aligned}$$

holds for all $f, g, h \in \mathrm{Hom}_k(C, A)$ and $c \in C$. What remains is to prove that $\eta\circ\varepsilon$ is an identity element for $\mathrm{Hom}_k(C, A)$, which is equivalent to showing $\eta\circ\varepsilon * f = f * \eta\circ\varepsilon = f$ for all $f \in \mathrm{Hom}_k(C, A)$. The unit property of (A, ∇, η) and the counit property of (C, Δ, ε) give us diagrams

$$\begin{array}{ccc} A\otimes A & \xleftarrow{\mathrm{id}_A\otimes\eta} & A\otimes k\\ {\scriptstyle \eta\otimes\mathrm{id}_A}\uparrow & \overset{\nabla}{\searrow} & \downarrow{\scriptstyle s_2}\\ k\otimes A & \xrightarrow[s_1]{} & A \end{array} \qquad \begin{array}{ccc} C\otimes k & \xleftarrow{\mathrm{id}_C\otimes\varepsilon} & C\otimes C\\ {\scriptstyle -\otimes 1}\uparrow & \overset{\Delta}{\nearrow} & \downarrow{\scriptstyle \varepsilon\otimes\mathrm{id}_C}\\ C & \xrightarrow[1\otimes -]{} & k\otimes C \end{array}$$

which commute. Combining these diagrams with maps $f \in \mathrm{Hom}_k(C, A)$

and $\eta \circ \varepsilon * f$ and $f * \eta \circ \varepsilon$ yields the following diagram



which commutes, where the isomorphisms above are the canonical ones, $A \otimes k \cong k \otimes A \cong A$, and likewise $C \otimes k \cong k \otimes C \cong C$. To see the above commutativity directly, we can observe

$$\begin{aligned}
((\eta \circ \varepsilon) * f)(c) &= (\nabla \circ (\eta \circ \varepsilon \otimes f) \circ \Delta)(c) \\
&= \sum_{(c)} (\eta \circ \varepsilon)(c_{(1)}) f(c_{(2)}) \\
&= \sum_{(c)} \eta(\varepsilon(c_{(1)})) f(c_{(2)}) \\
&= \sum_{(c)} \varepsilon(c_{(1)}) \eta(1_k) f(c_{(2)}) \\
&= \sum_{(c}) \varepsilon(c_{(1)}) f(c_{(2)}) \\
&= \sum_{(c)} f(\varepsilon(c_{(1)}) c_{(2)}) \\
&= f\left(\sum_{(c)} \varepsilon(c_{(1)}) c_{(2)} \right) \\
&= f(c)
\end{aligned}$$

holds for all $f \in \mathrm{Hom}_k(C, A)$ and $c \in C$, where the last line follows given the counit property of (C, Δ, ε), which when viewed using Sweedler notation

states that

$$c = \sum_{(c)} \eta(c_{(1)})c_{(2)} = \sum_{(c)} \eta(c_{(2)})c_{(1)}$$

The above shows that $\eta \circ \varepsilon$ is a left identity element for $\mathrm{Hom}_k(C, A)$. In a completely analagous manner as to the above calculation, we can obtain that $f * (\eta \circ \varepsilon) = f$, i.e., that $\eta \circ \varepsilon = \eta \circ \varepsilon$ is a right identity, and hence the desired identity element. Thus we may conclude that $(\mathrm{Hom}_k(C, A), *)$ is a monoid. ■

In fact, the monoid structure on the set of linear transformations from a coalgebra to an algebra, which is induced by the convolution product, in addition to the composition of the unit and counit maps shown in the theorem, give the set of transformations the structure of an algebra as well.

Corollary 2.8. Let (A, ∇, η) be a k-algebra and let (C, Δ, ε) be a k-coalgebra. Then $(\mathrm{Hom}_k(C, A), *, \eta \circ \varepsilon)$ is a k-algebra, where $\eta \circ \varepsilon = \eta \circ \varepsilon$.

Proof. The set $\mathrm{Hom}_k(C, A)$ is a k-vector space since A and C are both k-vector spaces. Theorem 2.7 gives the associative property, while an easy check shows that $\eta \circ \varepsilon = \eta \circ \varepsilon$ works with $*$ to satisfy the unit property; hence $(\mathrm{Hom}_k(C, A), *, \eta \circ \varepsilon)$ is a k-algebra. ■

Definition 2.9. If (A, ∇, η) is a k-algebra and (C, Δ, ε) is a k-coalgebra, then the k-algebra $(\mathrm{Hom}_k(C, A), *, \eta \circ \varepsilon)$ is called the *convolution algebra*.

While the notion of a convolution algebra may seem somewhat obtuse, in fact we have already seen an example of a convolution algebra. Namely, the algebra obtained by dualizing a coalgebra.

Example 2.10. Let $(A, \nabla, \eta) = (k, \nabla_k, \eta_k)$ be the trivial k-algebra and let (C, Δ, ε) be a k-coalgebra. Recall that $\eta_k = \mathrm{id}_k$ and $\nabla_k(r \otimes r') = rr'$ for all $r, r' \in k$, so that $\eta \circ \varepsilon = \eta_k \circ \varepsilon = \mathrm{id}_k \circ \varepsilon = \varepsilon^*$ and $* = \Delta^*$. In particular, we have $C^* = \mathrm{Hom}_k(C, k)$ and hence the k-algebra $(C^*, \Delta^*, \varepsilon^*)$ of Theorem 1.25 coincides with the convolution algebra $(\mathrm{Hom}_k(C, k), *, \eta \circ \varepsilon)$.

Example 2.11. Let $(B, \nabla, \eta, \Delta, \varepsilon)$ be a k-bialgebra. Then, in particular, (B, ∇, η) is a k-algebra and (B, Δ, ε) is a k-coalgebra, and so in view of Corollary 2.8, take $B = A = C$ to get the convolution algebra $(\mathrm{Hom}_k(B, B), *, \eta \circ \varepsilon)$. We oftentimes denote this k-algebra by $(\mathrm{End}(B), *, \eta \circ \varepsilon)$.

The example above will lead us to the definition of a special type of linear map which will be the cornerstone of our future study of Hopf algebras.

2.4 Antipodes

Definition 2.12. Let $(B, \nabla, \eta, \Delta, \varepsilon)$ be a k-bialgebra. An endomorphism $S \in \mathrm{End}(B)$ is called an *antipode* for the k-bialgebra $(B, \nabla, \eta, \Delta, \varepsilon)$ if

$$S * \mathrm{id}_B = \mathrm{id}_B * S = \eta \circ \varepsilon$$

where $*$ denotes the convolution product defined in the last section. In other words, if S is a left and right inverse for id_B in the convolution algebra $(\mathrm{End}(B), *, \eta \circ \varepsilon)$.

Equivalently, an endomorphism S is an antipode if the equation

$$(\nabla \circ (S \otimes \mathrm{id}_B) \circ \Delta)(c) = (\eta \circ \varepsilon)(c) = (\nabla \circ (\mathrm{id}_B \otimes S) \circ \Delta)(c)$$

holds for all $c \in B$. For convenience, we remark that $(\eta \circ \varepsilon)(c) = \varepsilon(c)1_B$.

For convenience, we may place the definition of an antipode for a bialgebra in the context of Sweedler notation, which may make the usefulness of the definition more apparent. For the k-bialgebra $(B, \nabla, \eta, \Delta, \varepsilon)$ together with an antipode S, we have that

$$(\nabla \circ (S \otimes \mathrm{id}_B) \circ \Delta)(c) = \nabla\left(\sum_{(c)} S(c_{(1)}) \otimes c_{(2)}\right) = \sum_{(c)} S(c_{(1)})c_{(2)}$$

$$(\nabla \circ (\mathrm{id}_B \otimes S) \circ \Delta)(c) = \nabla\left(\sum_{(c)} c_{(1)} \otimes S(c_{(2)})\right) = \sum_{(c)} c_{(1)}S(c_{(2)})$$

and since $(\eta \circ \varepsilon)(c) = \varepsilon(c)1_B$, the definition of an antipode forces

$$\sum_{(c)} S(c_{(1)})c_{(2)} = \varepsilon(c)1_B = \sum_{(c)} c_{(1)}S(c_{(2)})$$

Not every bialgebra has an antipode, but an antipode exists for a bialgebra, then it is necessarily unique.

Proposition 2.13. Let $(B, \nabla, \eta, \Delta, \varepsilon)$ be a k-bialgebra. If S is an antipode for $(B, \nabla, \eta, \Delta, \varepsilon)$, then S is unique.

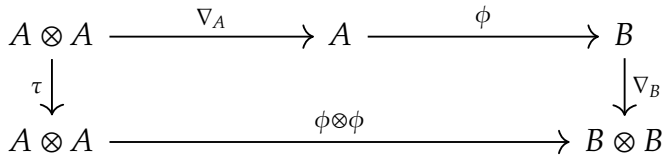
Proof. Suppose $S' : H \to H$ was another antipode for the k-bialgebra $(B, \nabla, \eta, \Delta, \varepsilon)$. Then we have that

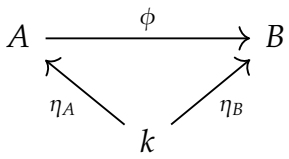
$$S' = S' * \eta \circ \varepsilon = S' * (\mathrm{id}_B * S) = (S' * \mathrm{id}_B) * S = \eta \circ \varepsilon * S = S$$

where the first and last equalities follow since $\eta \circ \varepsilon = \eta \circ \varepsilon$ is the identity element of the convolution algebra $(\mathrm{End}(B), *, \eta \circ \varepsilon)$, and the inner equalities follow from the definition of an antipode. ∎

Before developing the theory of antipodies further, we recall the following useful definition: an *anti-homomorphism* is a map that switches the order of multiplication. Specifically, we have the following definition.

Definition 2.14. Let (A, ∇_A, η_A) and (B, ∇_B, η_B) be k-algebras. A k-linear mapping $\phi : A \to B$ is called a *k-algebra anti-homomorphism* if the diagrams





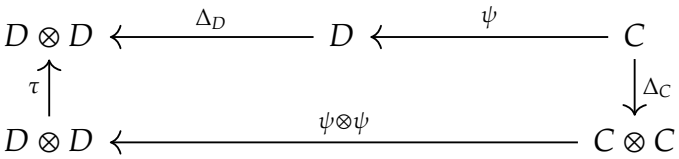
commute. In other words, if

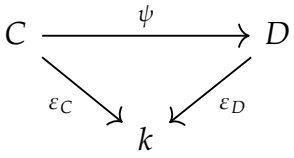
$$(\phi \circ \nabla_A)(a \otimes a') = (\nabla_B \circ (\phi \otimes \phi) \circ \tau)(a \otimes a')$$

$$(\phi \circ \eta_A)(r) = \eta_B(r)$$

hold for all $a, a' \in A$ and $r \in k$.

Similarly, if $(C, \Delta_C, \varepsilon_C)$ and $(D, \Delta_D, \varepsilon_D)$ are k-coalgebras, then a k-linear mapping $\psi : C \to D$ is called a *k-coalgebra anti-homomorphism* if the diagrams





commute. In other words if

$$(\tau \circ (\psi \otimes \psi) \circ \Delta_C)(c) = (\Delta_D \circ \psi)(c)$$

$$\varepsilon_C(c) = (\varepsilon_D \circ \psi)(c)$$

for all $c \in C$.

We now show that an antipode for a bialgebra is actually an anti-homomorphism of the underlying algebra structure of the bialgebra.

Proposition 2.15. Let $(B, \nabla, \eta, \Delta, \varepsilon)$ be a k-bialgebra with antipode S. Then the following properties hold:

1. $S(ab) = S(b)S(a)$ for all $a, b \in B$,
2. $S(1_B) = 1_B$.

That is, the antipode S is a k-algebra anti-homomorphism. of (B, ∇, η) with itself.

Proof. Consider the convolution algebra $(\mathrm{Hom}_k(B \otimes B, B), *, \eta \circ \varepsilon)$. We are interested in three elements of $\mathrm{Hom}_k(B \otimes B, B)$, namely the usual multiplication map $\nabla : B \otimes B \to B$, as well as

$$S \circ \nabla : B \otimes B \to B$$

$$a \otimes b \mapsto S(ab)$$

and

$$\Phi = \nabla \circ (S \otimes S) \circ \tau : B \otimes B \to B$$

$$a \otimes b \mapsto S(b)S(a)$$

We will also require the k-coalgebra structure of the tensor product $B \otimes B$, the k-coalgebra $(B \otimes B, \Delta_{B\otimes B}, \varepsilon_{B\otimes B})$ from Proposition 1.21. In view of this, note that $\eta \circ \varepsilon = \eta \circ \varepsilon_{B\otimes B}$ is the identity in the convolution algebra $(\mathrm{Hom}_k(B \otimes B, B), *, \eta \circ \varepsilon)$.

To prove (1) we must show $S \circ \nabla = \Phi$ holds in the convolution algebra. To this end, we prove that

$$\nabla * \Phi = \eta \circ \varepsilon_{B\otimes B} = \Phi * \nabla$$

and that

$$\nabla * S \circ \nabla = \eta \circ \varepsilon_{B\otimes B} = S \circ \nabla * \nabla$$

If we can show that the above relations hold true, then equality of the above two equations gives

$$\begin{aligned}
\nabla * \Phi = \nabla * S \circ \nabla &\iff \Phi * \nabla * \Phi = \Phi * \nabla * S \circ \nabla \\
&\iff \eta \circ \varepsilon_{B\otimes B} * \Phi = \eta \circ \varepsilon_{B\otimes B} * S \circ \nabla \\
&\iff \eta \circ \varepsilon * \Phi = \eta \circ \varepsilon * S \circ \nabla \\
&\iff \Phi = S \circ \nabla
\end{aligned}$$

which is the desired statement of (1). To show that the equations hold, observe

$$\begin{aligned}
(\nabla * \Phi)(a \otimes b) &= \nabla * (\nabla \circ (S \otimes S) \circ \tau)(a \otimes b) \\
&= (\nabla \circ (\nabla \otimes \nabla \circ (S \otimes S) \circ \tau) \circ \Delta_{B\otimes B})(a \otimes b) \\
&= \nabla\left(\sum_{(a),(b)} \nabla(a_{(1)} \otimes b_{(1)}) \otimes \nabla(S \otimes S)\tau(a_{(2)} \otimes b_{(2)})\right) \\
&= \nabla\left(\sum_{(a),(b)} \nabla(a_{(1)} \otimes b_{(1)}) \otimes \nabla(S(b_{(2)} \otimes S(a_{(2)}))\right) \\
&= \sum_{(a),(b)} a_{(1)}b_{(1)}S(b_{(2)})S(a_{(2)}) \\
&= \sum_{(a)} a_{(1)}\varepsilon(b)1_B S(a_{(2)}) \\
&= \sum_{(a)} \varepsilon(b)a_{(1)}S(a_{(2)}) \\
&= \varepsilon(b)\varepsilon(a)1_B \\
&= (\eta \circ \varepsilon_{B\otimes B})(a \otimes b)
\end{aligned}$$

for all $a, b \in B$, where the antipode relations from S give the equalities from line 5 to line 6, and from line 6 to line 7. A completely analagous computation yields that $\Phi * \nabla = \eta \circ \varepsilon_{B\otimes B}$ as well.

For the second desired equation, observe that

$$\begin{aligned}
(\nabla * S \circ \nabla)(a \otimes b) &= (\nabla \circ (\nabla \otimes S \circ \nabla) \circ \Delta_{B\otimes B})(a \otimes b) \\
&= \nabla\left(\sum_{(a),(b)} \nabla(a_{(1)} \otimes b_{(1)}) \otimes S(a_{(2)}b_{(2)})\right) \\
&= \sum_{(a),(b)} a_{(1)}b_{(1)}S(a_{(2)}b_{(2)}) \\
&= \nabla \circ (\mathrm{id}_B \otimes S)\left(\sum_{(a),(b)} a_{(1)}b_{(1)} \otimes a_{(2)}b_{(2)}\right) \\
&= (\nabla \circ (\mathrm{id}_B \otimes S) \circ \Delta_{B\otimes B})(ab) \\
&= \varepsilon(ab)1_H \\
&= \varepsilon(a)\varepsilon(b)1_H \\
&= (\eta \circ \varepsilon_{B\otimes B})(a \otimes b)
\end{aligned}$$

holds for all $a, b \in B$, where line 5 follows from line 4 given the relations

from the antipode S. Hence (1) is proved.

For (2), we use the antipode relation from S. Note that $(\eta \circ \varepsilon)(c) = (\mathrm{id}_B * S)(c)$ holds, as well as $(\eta \circ \varepsilon)(c) = \varepsilon(c)1_B$ for all $c \in B$; choosing $c = 1_B$, it is easy to observe that

$$\begin{aligned} 1_B &= 1_k 1_B \\ &= \varepsilon(1_B)1_B \\ &= (\mathrm{id}_B * S)(1_B) \\ &= (\nabla \circ (\mathrm{id}_k \otimes S) \circ \Delta)(1_B) \\ &= (\nabla \circ (\mathrm{id}_B \otimes S))(1_B \otimes 1_B) \\ &= S(1_B) \end{aligned}$$

Which suffices to prove (2), and hence the proposition. ∎

In fact, we can go further. An antipode for a bialgebra actually constitutes an anti-homomorphism of the underlying coalgebra structure of the bialgebra.

Proposition 2.16. Let $(B, \nabla, \eta, \Delta, \varepsilon)$ be a k-bialgebra with antipode S. Then the following properties hold:

1. $\tau \circ (S \otimes S) \circ \Delta = \Delta \circ S$,
2. $\varepsilon \circ S = \varepsilon$.

That is, the antipode S is a k-coalgebra anti-homomorphism from the k-coalgebra (B, Δ, ε) to itself.

Proof. Consider the convolution algebra $(\mathrm{Hom}_k(B, B \otimes B), *, \eta \circ \varepsilon)$. We are interested in three elements of $\mathrm{Hom}_k(B, B \otimes B)$. Namely, the usual comultiplication map $\Delta : B \to B \otimes B$, as well as

$$\Theta = \tau \circ (S \otimes S) \circ \Delta : B \to B \otimes B$$

$$b \longmapsto \sum_{(b)} S(b_{(2)}) \otimes S(b_{(1)})$$

and

$$\Delta \circ S : B \to B \otimes B$$

$$b \longmapsto \sum_{(S(b))} (S(b))_{(1)} \otimes (S(b))_{(2)}$$

We will also require the k-algebra structure of the tensor product algebra $B \otimes B$, given by $(B \otimes B, \nabla_{B\otimes B}, \eta_{B\otimes B})$ from Proposition 1.12. In view of

this, note that $\eta \circ \varepsilon = \eta_{B\otimes B} \circ \eta$ is the identity in the convolution algebra $(\mathrm{Hom}_k(B, B \otimes B), *, \eta \circ \varepsilon)$.

To obtain (1) we prove two preliminary equations given as follows

$$\Delta * \Theta = \eta_{B\otimes B} \circ \varepsilon = \Theta * \Delta$$

and

$$\Delta * \Delta \circ S = \eta_{B\otimes B} \circ \varepsilon = \Delta * \Delta \circ S$$

We shall use these relations to derive our desired result using relations in the convolution algebra. For now, observe that

$$\begin{aligned}
(\Delta * \Theta)(b) &= (\nabla_{B\otimes B} \circ (\Delta \otimes \Theta) \circ \Delta)(b) \\
&= (\nabla_{B\otimes B} \circ (\Delta \otimes \Theta)) \left(\sum_{(b)} b_{(1)} \otimes b_{(2)} \right) \\
&= \nabla_{B\otimes B} \left(\sum_{(b)} \Delta(b_{(1)}) \otimes \Theta(b_{(2)}) \right) \\
&= \nabla_{B\otimes B} \left(\sum_{(b)} b_{(1)} \otimes b_{(2)} \otimes S(b_{(4)}) \otimes S(b_{(3)}) \right) \\
&= \sum_{(b)} b_{(1)} S(b_{(4)}) \otimes b_{(2)} S(b_{(3)})
\end{aligned}$$

Now recall the antipode property for S, which gives us

$$\nabla \circ (S \otimes \mathrm{id}_B) \circ \Delta = \eta \circ \varepsilon = \nabla \circ (\mathrm{id}_B \otimes S) \circ \Delta$$

and hence the above equation becomes

$$\begin{aligned}
(\Delta * \Theta)(b) &= \nabla_{B\otimes B} \left(\sum_{(b)} b_{(1)} \otimes b_{(2)} \otimes S(b_{(4)}) \otimes S(b_{(3)}) \right) \\
&= \sum_{(b)} b_{(1)} S(b_{(4)}) \otimes b_{(2)} S(b_{(3)}) \\
&= \sum_{(b)} b_{(1)} S(b_{(3)}) \otimes \varepsilon(b_{(2)}) 1_B \\
&= \sum_{(b)} \varepsilon(b_{(2)}) b_{(1)} S(b_{(3)}) \otimes 1_B \\
&= \sum_{(b)} b_{(1)} S(b_{(2)}) \otimes 1_B \\
&= \varepsilon(b) 1_B \otimes 1_B \\
&= (\eta_{B\otimes B} \circ \varepsilon)(b)
\end{aligned}$$

A completely analagous argument shows that $(\Theta * \Delta)(b) = (\eta_{B\otimes B} \circ \varepsilon)(b)$ as well. Next we show that $\Delta * \Delta \circ S = \Delta \circ S * \Delta = \eta_{B\otimes B} \circ \varepsilon$. Observe

$$\begin{aligned}
(\Delta * \Delta \circ S)(b) &= (\nabla_{B\otimes B} \circ (\Delta \otimes \Delta \circ S) \circ \Delta)(b) \\
&= \nabla_{B\otimes B}\left(\sum_{(b)} \Delta(b_{(1)}) \otimes \Delta(S(b_{(2)}))\right) \\
&= \nabla_{B\otimes B}\left(\sum_{(b)} b_{(1)} \otimes b_{(2)} \otimes S(b_{(3)}) \otimes S(b_{(4)})\right) \\
&= \sum_{(b)} b_{(1)}S(b_{(3)}) \otimes b_{(2)}S(b_{(4)}) \\
&= \sum_{(b)} b_{(1)}S(b_{(3)} \otimes \varepsilon(b_{(3)})1_B \\
&= \sum_{(b)} \varepsilon(b_{(3)})b_{(1)}S(b_{(3)}) \otimes 1_B \\
&= \sum_{(b)} b_{(1)}S(b_{(2)}) \otimes 1_B \\
&= \varepsilon(b)1_B \otimes 1_B \\
&= (\eta_{B\otimes B} \circ \varepsilon)(b)
\end{aligned}$$

and so we have proved both equations. Now note that we have

$$\Theta * (\Delta * \Theta) = \Theta * (\Delta * \Delta \circ S)$$

and hence

$$(\Theta * \Delta) * \Theta = (\Theta * \Delta) * \Delta \circ S$$

and now from the above we substitute to find

$$(\eta_{B\otimes B} \circ \varepsilon) * \Theta = (\eta_{B\otimes B} \circ \varepsilon) * \Delta \circ S$$

And now, since $\eta_{B\otimes B} \circ \varepsilon$ is the identity in the convolution algebra, we have finally that $\Theta = \Delta \circ S$, hence proving (1).

Now for (2), observe that for all $b \in B$ we have

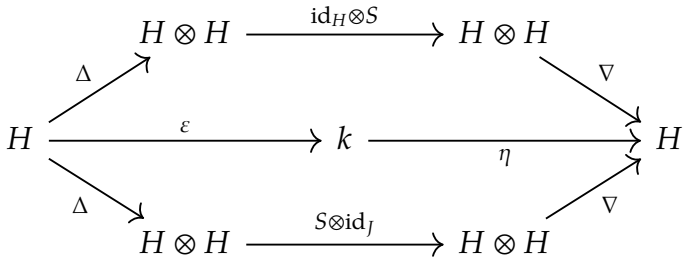
$$\begin{aligned}
\eta(b) &= \eta(b)1_k \\
&= \eta(b)\eta(1_B) \\
&= \eta(\eta(b)1_B) \\
&= \eta\left(\sum_{(b)} b_{(1)}S(b_{(2)})\right) \\
&= \sum_{(b)} \varepsilon(b_{(1)})\varepsilon(S(b_{(2)})) \\
&= \sum_{(b)} \varepsilon(S(\varepsilon(b_{(1)}b_{(2)})) \\
&= \varepsilon(S(b)) \\
&= (\varepsilon \circ S)(b)
\end{aligned}$$

where the last line follows from the counit property, and the third line follows from the second from the antipode property, hence proving (2). Whence the proposition. ■

2.5 Hopf Algebras

In this section we finally define our central object of study, the notion of a Hopf algebra over a field. We shall see that Hopf algebras are an example of bialgebras, specifically, those bialgebras with antipode.

Definition 2.17. Let k be a field. If there exists an antipode S for the k-bialgebra $(H, \nabla, \eta, \Delta, \varepsilon)$, then we say that $(H, \nabla, \eta, \Delta, \varepsilon)$ is a *k-Hopf algebra*. To recall, the existence of an antipode S is equivalent to there being a k-linear map $S : H \to H$ which makes the following diagram



commute. Equivalently, we have that

$$(\nabla \circ (\mathrm{id}_H \otimes S) \circ \Delta)(h) = \varepsilon(h)1_H = (\nabla \circ (S \otimes \mathrm{id}_H) \circ \Delta)(h)$$

for all $h \in H$. We call the condition that the diagram above commute the *antipode property*.

To be clear, a Hopf algebra is not a bialgebra with additional structure, but rather a particular subset of bialgeras, those with a (necessarily) unique antipode. For a field k, we often denote a k-Hopf algebra by $(H, \nabla, \eta, \Delta, \varepsilon, S)$, where S is the antipode of the underlying k-bialgebra.

Definition 2.18. The k-Hopf algebra $(H, \nabla, \eta, \Delta, \varepsilon, S)$ is called *commutative* if the k-algebra (H, ∇, η) is commutative, and *cocommutative* if the k-coalgebra (H, Δ, ε) is cocommutative.

We now present the prototypical example of a Hopf algebra: that of the group ring.

Example 2.19 (*Group Ring*)**.** Let k be a field and let G be a finite group. Recall the group ring k-bialgebra $(k[G], \nabla_{k[G]}, \eta_{k[G]}, \Delta_{k[G]}, \varepsilon_{k[G]})$ of Example 2.3. Consider the map $S_{k[G]} : k[G] \to k[G]$ defined by

$$\sum_{g \in G} \alpha_g [g] \mapsto \sum_{g \in G} \alpha_g [g^{-1}]$$

A quick check shows that $S_{k[g]}$ is an antipode for the group k-bialgebra, and hence that

$$(k[G], \nabla_{k[G]}, \eta_{k[G]}, \Delta_{k[G]}, \varepsilon_{k[G]}, S_{k[G]})$$

is a k-Hopf algebra. This k-Hopf algebra is cocommutative, and commutative if and only if G is abelian.

A quick glance shows that the antipode of the group ring Hopf algebra described above has order 2. One might ask whether this is true of all antipodes. As it turns out, the answer is a resounding 'no'. To be more specific, we have the following proposition:

Proposition 2.20. If the k-Hopf algebra $(H, \nabla, \eta, \Delta, \varepsilon, S)$ is cocommutative, then $S^2 = \mathrm{id}_H$; the antipode S has order 2.

Proof. We work in the convolution algebra $(\mathrm{End}(H), *, \eta \circ \varepsilon)$. Clearly S, S^2, id_H, and $\eta \circ \varepsilon$ are all elements of $\mathrm{End}(H)$. Since $(H, \nabla, \eta, \Delta, \varepsilon, S)$ is cocummutative, we know that for all $h \in H$

$$(\tau \circ \Delta)(h) = \Delta(h)$$

for all $h \in H$. With this in mind, observe that

$$\begin{aligned}
(S * S^2)(h) &= (\nabla \circ (S \otimes S^2) \circ \Delta)(h) \\
&= (\nabla \circ (S \otimes S^2) \circ \tau \circ \Delta)(h) \\
&= \nabla\left(\sum_{(h)} S(h_{(2)}) \otimes S(S(h_{(1)}))\right) \\
&= \sum_{(h)} S(h_{(2)}) S(S(h_{(1)})) \\
&= \sum_{(h)} S(S(h_{(1)}) h_{(2)}) \\
&= S(\varepsilon(h) 1_H) \\
&= \varepsilon(h) 1_H \\
&= (\eta \circ \varepsilon)(h)
\end{aligned}$$

where the second line follows from the first due to cocommutativity, the fifth line follows from the fourth due to Proposition 2.15(1), and the sxith follows from the fifth by (2) of the same proposition. Using the above, we see

$$\mathrm{id}_H * (S * S^2) = \mathrm{id}_H * \eta \circ \varepsilon = \mathrm{id}_H$$

since $\eta \circ \varepsilon$ is the identity in the convolution algebra. From the definition of an antipode, we also have that $\mathrm{id}_H * S = \eta \circ \varepsilon$, and hence

$$\mathrm{id}_H * (S * S^2) = (\mathrm{id}_H * S) * S^2 = \eta \circ \varepsilon * S^2 = S^2$$

Since the convolution product $*$ is associative in $\mathrm{End}(H)$, it follows that $S^2 = \mathrm{id}_H$, as desired. ■

We have seen that the dual of a bialgebra is once more a bialgebra. A natural question becomes whether we can dualize Hopf algebras in a similar manner. All we need to show is that the dual antipode defines an antipode for the underlying dual bialgebra.

Proposition 2.21. Let $(H, \nabla, \eta, \Delta, \varepsilon, S)$ be a finite dimensional k-Hopf algebra. Then the k-bialgebra $(H^*, \nabla^*, \eta^*, \Delta^*, \varepsilon^*)$ equipped with antipode S^* is a k-Hopf algebra.

Proof. ■

2.6 Grouplike Elements

In this section we briefly return to the world of coalgebras over a field, and introduce special elements of coalgebras which act, in a sense, like elements in a group. These considerations will automatically apply to Hopf algebras given the underlying coalgebra structure.

Definition 2.22. Let (C, Δ, ε) be a k-coalgebra. A *grouplike element* of C is an element $c \in C$ such that

$$\Delta(c) = c \otimes c \quad \text{and} \quad \varepsilon(c) = 1$$

We denote the set of all grouplike elements of C by $G(C)$.

In fact, sometimes the definition of a grouplike element of a k-coalgebra (C, Δ, ε) is simply given to those elements $c \in C$ satisfying the equation $\Delta(c) = c \otimes c$. To see this, let s_1 denote the usual juxtaposition map via $s_1(a \otimes b) = ab$. Since $(\varepsilon \otimes \mathrm{id}_C)\Delta(c) = 1 \otimes c$ from the counit property, we can find that

$$\begin{aligned} c &= (s_1 \circ (\varepsilon \otimes \mathrm{id}_C) \circ \Delta))(c) \\ &= (s_1 \circ (\varepsilon \otimes \mathrm{id}_C))(c \otimes c) \\ &= s_1(\varepsilon(c) \otimes c) \\ &= \varepsilon(c)c \end{aligned}$$

Now since $s_1(1 \otimes c) = 1c = c$ we have $c - \varepsilon(c)c = 0$ implies $(1 - \varepsilon(c))c = 0$, and since $c \neq 0$ with k a field, we require $1 - \varepsilon(c) = 0$, giving $\varepsilon(c) = 1$. Thus we could simply have relaxed the definition above without losing any additional information.

Now recall that a k-coalgebra is, in particular, a k-vector space over k. The importance of grouplike elements of a coalgebra lies in the fact that subsets consisting of grouplike elements are linearly independent over k, which we shall prove now.

Theorem 2.23. Let (C, Δ, ε) be a k-coalgebra. Then the set of grouplike elements $G(C)$ of C is linearly independent.

Proof. If the k-coalgebra C has no grouplike elements then $G(C) = \varnothing$, which is trivially linearly independent as a subset of the k-vector space C. If $G(C)$ contains one element c, then this element must be non-zero since $\varepsilon(0) = 0$, and so $G(C)$ is linearly independent. If not, then $G(C)$ contains at least two elements.

Assume, for contradiction that $G(C)$ is linearly dependent. Let $r \geq 1$ be the largest integer for which $S = \{g_1, \ldots, g_r\}$ is a linearly independent subset of $G(C)$. Take $g \in G(C) \setminus S$. Then there exists a linear dependence relation

$$a_1 g_1 + \cdots + a_r g_r = g$$

for $a_i \in k$ for all $i \in \{1, \ldots, r\}$. We know that $g \neq 0$ and that $a_i \neq 0$ for at least one i. We find

$$\Delta(g) = g \otimes g = \sum_{i=1}^{r} \sum_{j=1}^{r} a_i a_j (g_i \otimes g_j)$$

while also simultaneously requiring that

$$\Delta(g) = \sum_{i=1}^{r} a_i (g_i \otimes g_i)$$

to which

$$\sum_{i=1}^{r} \sum_{j=1}^{r} a_i a_j (g_i \otimes g_j) = \sum_{i=1}^{r} a_i (g_i \otimes g_i)$$

Now we know that the set of $g_i \otimes g_j$ for $i, j \in \{1, \ldots, r\}$ is linearly independent as a subset of the k-vector space $C \otimes C$, hence $a_i a_j = 0$ for all $i \neq j$ and $a_i^2 = a_i$ for all $i \in \{1, \ldots, r\}$. In particular, for any $r_i \neq 0$, since $r_i r_j = 0$ we require $r_j = 0$ for all $j \neq i$. By assumption, $r_i \neq 0$ for at least one i, which means all other $r_j = 0$, and hence $r_i^2 = r_i$ means $r_i = 1$. Thus $g = g_i$, which is a contradiction to our choice of g. Hence $G(C)$ is linearly independent. ∎

Example 2.24. Let k be a field let G be a finite group. Consider the k-Hopf algebra $k[G]$, the group ring Hopf algebra considered in Example 1.2. Since the dimension of $k[G]$ as a k-vector space is $|G|$, where the basis is given by those elements $\{[g] \mid g \in G\}$, we know that $G(k[G])$ must equal this set. That is, the grouplike elements of the k-Hopf algebra $k[G]$ may be identified with G.

We record for convenience two more important facts about grouplikes, each of which are interesting in their own right (but only the first of which we shall use in the coming discussion).

Proposition 2.25. Let H be a finite dimensional k-Hopf algebra. Then $f \in H^* = \mathrm{Hom}_k(H, k)$ is a grouplike element if and only if f is a k-algebra homomorphism $f : H \to k$.

Proof. We have $\Delta(f)(x \otimes y) = f(xy)$, and so $\Delta(f) = f \otimes f$ if and only if $f(xy) = f(x)f(y)$ for all $x, y \in H$. ∎

Proposition 2.26. Let $(C, \Delta_C, \varepsilon_C)$ and $(D, \Delta_D, \varepsilon_D)$ be k-coalgebras and suppose $\phi : C \to D$ is a homomorphism of k-coalgebras. Then if $c \in G(C)$, then $\phi(c) \in G(D)$. In other words, homomorphisms of coalgebras preserve grouplikes.

Proof. Recall that $\phi : C \to D$ being a homomorphism of k-coalgebras means that

$$((\phi \otimes \phi) \circ \Delta_C)(c) = (\Delta_D \circ \phi)(c)$$

for all $c \in C$. If $c \in G(C)$ then we know that

$$((\phi \otimes \phi) \circ \Delta_C)(c) = (\phi \otimes \phi)(c \otimes c) = \phi(c) \otimes \phi(c)$$

must be equal $\Delta_D(\phi(c))$, meaning that $\phi(c) \in G(D)$. ∎

2.7 Integrals

In this section we analyze the elements of a Hopf algebra which are invariant under left multiplication. It turns out that the set of all such invariants forms a subspace and an ideal of the Hopf algebra.

Definition 2.27. Let $(H, \nabla, \eta, \Delta, \varepsilon, S)$ be a k-Hopf algebra. A *left integral in H* is an element $y \in H$ such that

$$xy = \varepsilon(x)y$$

for all $x \in H$. Similarly, a *right integral in H* is an element $z \in H$ such that

$$zx = \varepsilon(x)z$$

for all $x \in H$. We use $\int_H^l$ to denote the set of all left integrals of H, and $\int_H^r$ to denote the set of right integrals of H.

We make some immediate observations for the set of left and right integrals of a Hopf algebra.

Proposition 2.28. Let $(H, \nabla, \eta, \Delta, \varepsilon, S)$ be a k-Hopf algebra. Then $\int_H^l$ and $\int_H^r$ are k-subspaces of the k-vector space H.

Proof. Since $x0 = 0 = \varepsilon(x)0$ for all $x \in H$, we have $0 \in \int_H^l$, to which $\int_H^l \neq \varnothing$. Let $y, z \in \int_H^l$. Then for all $x \in H$ we have that

$$x(y - z) = xy + xz = \varepsilon(x)y - \varepsilon(x)z = \varepsilon(x)(y - z)$$

hence $y - z \in \int_H^l$, so that $\int_H^l$ is an additive subgroup of H. Finally, let $r \in k$ and take $y \in \int_H^l$. Then

$$x(ry) = (xr)y = \varepsilon(xr)y = r\varepsilon(x)y = \varepsilon(x)ry = \varepsilon(ry)$$

for all $x \in H$, hence $ry \in \int_H^l$, which proves that $\int_H^l$ is a k-subspace of H. The proof that $\int_H^r$ is a k-subspace of H is completely symmetric. ∎

Proposition 2.29. Let $(H, \nabla, \eta, \Delta, \varepsilon, S)$ be a k-Hopf algebra. Then $\int_H^l$ and $\int_H^r$ are ideals of the ring H.

Proof. From Proposition 2.28, $\int_H^l$ is an additive subgroup of H. Thus to prove that $\int_H^l$ is an ideal of H it suffices to show that $z\int_H^l \subseteq \int_H^l$ and

$\int_H^l z \subseteq \int_H^l$ for all $z \in H$. So let $z \in H$ and $y \in \int_H^l$. Then for all $x \in H$ we have

$$x(zy) = (xz)y = \varepsilon(xz)y = \varepsilon(x)\varepsilon(z)y = \varepsilon(x)(zy)$$

$$x(yz) = (xy)z = (\varepsilon(x)y)z = \varepsilon(x)(yz)$$

and thus $zy, yz \in \int_H^l$. The proof that $\int_H^r$ is an ideal of H is a completely symmetric argument. ■

We are oftentimes interested in the case where the space of left and right integrals of a Hopf algebra coincide. To see why this is the case, consider a k-Hopf algebra $(H, \nabla, \eta, \Delta, \varepsilon, S)$. If $y \in \int_H^l$ and $y \in \int_H^r$ then

$$xy = \varepsilon(x)y = yx$$

for all $x \in H$. In other words, y commutes with all elements of H under multiplication, so $y \in Z(H)$, the center of the ring H.

Definition 2.30. A k-Hopf algebra $(H, \nabla, \eta, \Delta, \varepsilon, S)$ is called *unimodular* if $\int_H^l = \int_H^r$.

From our above discussion, it is clear that commutative Hopf algebras are unimodular. However, there do exist unimodular Hopf algebras which are not commutative.

❖ Actions on Modules and Coactions on Comodules

3.1 (Co-)Modules over (Co-)Algebras

In this section we would like to develop a notion of modules which admit actions of either algebras or coalgebras. To do this, we introduce the following definition which will provide compatability for the two structures.

Definition 3.1. Let (A, ∇, η) be a k-algebra. We call a k-vector space X equipped with a k-linear map $\Psi : A \otimes X \to X$ a *left A-module* if the following diagrams

$$\begin{array}{ccc} A \otimes A \otimes X & \xrightarrow{\nabla \otimes \mathrm{id}_X} & A \otimes X \\ {\scriptstyle \mathrm{id}_A \otimes \Psi}\downarrow & & \downarrow{\scriptstyle \Psi} \\ A \otimes X & \xrightarrow{\Psi} & X \end{array}$$

and

$$\begin{array}{ccc} A \otimes X & \xrightarrow{\Psi} & X \\ {\scriptstyle \eta \otimes \mathrm{id}_X}\uparrow & \nearrow_{s} & \\ k \otimes X & & \end{array}$$

commute, where $s : k \otimes X \to X$ is scalar multiplication defined by $s(r \otimes m) = rm$ for all $r \in k$ and $m \in X$. In other words, we have

$$(\Psi \circ (\mathrm{id}_A \otimes \Psi))(a \otimes b \otimes m) = (\Psi \circ (\nabla \otimes \mathrm{id}_X))(a \otimes b \otimes m)$$

$$(\Psi \circ (\eta \otimes \mathrm{id}_X))(r \otimes m) = rm$$

for all $r \in k$, $m \in X$, and $a, b \in A$.

We call the k-linear map $\Psi : A \otimes X \to X$ the *action of A on X*. When no confusion will arise, we often denote the action of A on X by $\Psi(a \otimes m) = a \cdot m$ for $a \in A$ and $m \in X$.

Let (A, ∇, η) be an k-algebra and let X be a left A-module. For convenience, we oftentimes denote a left A-module by the ordered pair (X, Ψ), where X is the k-vector space and $\Psi : A \otimes X \to X$ the action of A on X.

We take a moment to discuss the definition above. So consider the first equation in the definition above. The left hand side may be rewritten as follows

$$(\Psi \circ (\mathrm{id}_A \otimes \theta))(a \otimes b \otimes m) = \Psi(a \otimes b \cdot m) = a \cdot (b \cdot m)$$

while the right hand side becomes

$$(\Psi \circ (\nabla \otimes \mathrm{id}_M))(a \otimes b \otimes m) = \Psi(ab \otimes m) = (ab) \cdot m$$

for all $a, b \in A$ and $m \in X$. Thus the first equation states that

$$ab \cdot m = a \cdot (b \cdot m)$$

Similarly, in the second equation in the above definition, take $r = 1_k$. Then

$$(\Psi \circ (\eta \otimes \mathrm{id}_X))(1_k \otimes m) = \Psi(1_A \otimes m) = 1_A \cdot m$$

and thus the second equation states that $1_A \cdot m = m$ for all $m \in X$. Readers may recognize these two assertions as the axioms for a group action, which is precisely what we aimed to generalize here for k-algebras.

We have introduced the notion of a left A-module (X, Ψ) for a k-algebra (A, ∇, η). In the obvious way, there exists the notion of a right A-module (X, Ψ) where the action of A on X is given by $\Psi : X \otimes A \to X$. We work purely with left A-modules for this discussion, as we shall soon prove that left A-modules and right A-modules actually coincide in a natural way.

By dualizing the diagrams in the definition of an A-module, we obtain a "co" notion of an algebra acting on a vector space. Namely, that of a coalgebra acting on a vector space, which we now define.

Definition 3.2. Let (C, Δ, ε) be a k-coalgebra. We call a k-vector space Y equipped with a k-linear map $\Phi : Y \to Y \otimes C$ a *right C-comodule* if the diagrams

$$\begin{array}{ccc} Y & \xrightarrow{\Phi} & Y \otimes C \\ {\scriptstyle \Phi}\downarrow & & \downarrow{\scriptstyle \mathrm{id}_Y \otimes \Delta} \\ Y \otimes C & \xrightarrow{\Phi \otimes \mathrm{id}_C} & Y \otimes C \otimes C \end{array}$$

and

$$\begin{array}{ccc} Y \otimes C & \xleftarrow{\Phi} & Y \\ {\scriptstyle \mathrm{id}_Y \otimes \varepsilon}\downarrow & \swarrow{\scriptstyle -\otimes 1} & \\ Y \otimes k & & \end{array}$$

commute. In other words, if we have

$$((\Phi \otimes \mathrm{id}_C) \circ \Phi)(m) = ((\mathrm{id}_Y \otimes \Delta) \circ \Phi)(m)$$

$$((\mathrm{id}_Y \otimes \varepsilon) \circ \Phi)(m) = m \otimes 1$$

for all $m \in Y$.

We call the k-linear map $\Phi : Y \to Y \otimes C$ the *coaction* of C on Y, and shall say that C *coacts* on Y.

Once more, for a k-coalgebra C, we often denote a right C-comodule by the ordered pair (Y, Φ), where Y is the k-vector space and $\Phi : Y \to Y \otimes C$ is the coaction of C on Y.

Just as in the case of right A-modules for left A-modules discussed previously, there does exist a notion of a left C-comodule, which is a k-vector space Y with a k-linear map $\Phi : Y \to C \otimes Y$.

For clarity, we slightly extend our current notion of Sweedler notation for right C-comodules, as now instead of the tensorands both belonging to a coalgebra, the right hand tensorand belongs to the coalgebra while the left hand tensorand belongs to the comodule. In particular, for a right C-comodule (Y, Φ), and for $m \in Y$, we write

$$\Phi(m) = \sum_{(m)} m_{(1)} \otimes c_{(2)}$$

where $m_{(1)} \in Y$ and $c_{(2)} \in C$. Once more,

$$\Phi(m_{(1)}) = \sum_{(m_{(1)})} m_{(1)_{(1)}} \otimes c_{(1)_{(2)}}$$

Now, using the first equation in the definition above for a right C-comodule, the left hand side is

$$\begin{aligned}
((\Phi \otimes \mathrm{id}_C) \circ \Phi)(m) &= (\Phi \otimes \mathrm{id}_C)\left(\sum_{(m)} m_{(1)} \otimes c_{(2)}\right) \\
&= \sum_{(m)} \Phi(m_{(1)}) \otimes c_{(2)} \\
&= \sum_{(m)} \left(\sum_{(m_{(1)})} m_{(1)_{(2)}} \otimes c_{(1)_{(2)}}\right) \otimes c_{(2)} \\
&= \sum_{(m, m_{(1)})} m_{(1)_{(2)}} \otimes c_{(1)_{(2)}} \otimes c_{(2)}
\end{aligned}$$

while the right hand side states that

$$\begin{aligned}((\mathrm{id}_Y \otimes \Delta) \circ \Phi)(m) &= (\mathrm{id}_Y \otimes \Delta)\left(\sum_{(m)} m_{(1)} \otimes c_{(2)}\right) \\ &= \sum_{(m)} m_{(1)} \otimes \Delta(c_{(2)}) \\ &= \sum_{(m)} m_{(1)} \otimes \left(\sum_{(c_{(2)})} c_{(2)_{(1)}} \otimes c_{(2)_{(2)}}\right) \\ &= \sum_{(m,c_{(2)})} m_{(1)} \otimes c_{(2)_{(1)}} \otimes c_{(2)_{(2)}}\end{aligned}$$

Since, as the definition states, the left and right hand sides are equal, we necessarily have the equality

$$\sum_{(m,m_{(1)})} m_{(1)_{(2)}} \otimes c_{(1)_{(2)}} \otimes c_{(2)} = \sum_{(m,c_{(2)})} m_{(1)} \otimes c_{(2)_{(1)}} \otimes c_{(2)_{(2)}}$$

and for the common value of the left and right hand terms above, we write

$$\sum_{(m)} m_{(1)} \otimes c_{(2)} \otimes c_{(3)}$$

Just as in our initial section on Sweedler notation, the above convention may be extended to an arbitrary number of coaction computations.

We also briefly touch on the second equation in the definition for a right C-comodule, and put this definition into Sweedler notation as we have extended it above. We have

$$\begin{aligned}((\mathrm{id}_Y \otimes \varepsilon) \circ \Phi)(m) &= (\mathrm{id}_Y \otimes \varepsilon)\left(\sum_{(m)} m_{(1)} \otimes c_{(2)}\right) \\ &= \sum_{(m)} m_{(1)} \otimes \varepsilon(c_{(2)}) \\ &= \sum_{(m)} \varepsilon(c_{(2)}) m_{(1)} \otimes 1_C\end{aligned}$$

which, as per the definition, must be equal to $m \otimes 1$. Hence we require that

$$\sum_{(m)} \varepsilon(c_{(2)}) m_{(1)} = m$$

for all $m \in Y$.

Now, as for left C-comodules, we have the symmetric version of our extension of Sweedler notation. The details are nearly identical, and so we merely display the end results of the computations. For all $m \in M$, we set

$$\sum_{(c,c_{(1)})} c_{(1)_{(2)}} \otimes c_{(1)_{(2)}} \otimes m_{(2)} = \sum_{(c,m_{(2)}} c_{(1)} \otimes m_{(2)_{(1)}} \otimes m_{(2)_{(2)}} = \sum_{(m)} c_{(1)} \otimes c_{(2)} \otimes m_{(3)}$$

and we have

$$\sum_{(m)} \varepsilon(c_{(1)}) m_{(2)} = m$$

just as in the case of right C-comodules.

Now we present some examples of comodules over a coalgebra, as these objects are slightly more nuanced (and unintuitive) than modules over an algebra. We begin slow:

Example 3.3. Let (C, Δ, ε) be a k-coalgebra. Then (C, Δ) is both a left and right C-comodule; the coaction of C on C is given by the comultiplication map $\Delta : C \to C \otimes C$ in both cases, as can be easily verified by a check of the diagrams in the definition of a coalgebra.

Example 3.4. Let (C, Δ, ε) be a k-coalgebra and let X be an arbitrary k-vector space. We can endow the space $X \otimes C$ with a coaction of C, this coaction being $\mathrm{id}_X \otimes \Delta$. We have diagrams

$$\begin{array}{ccc} X \otimes C & \xleftarrow{\mathrm{id}_X \otimes \Delta} & X \otimes C \otimes C \\ \uparrow{\scriptstyle \mathrm{id}_X \otimes \Delta} & & \uparrow{\scriptstyle \mathrm{id}_X \otimes \Delta \otimes \Delta} \\ X \otimes C \otimes C & \xleftarrow{\mathrm{id}_X \otimes \Delta \otimes \Delta} & X \otimes C \otimes C \otimes C \end{array}$$

$$\begin{array}{ccc} X \otimes C \otimes C & \xleftarrow{\mathrm{id}_X \otimes \Delta} & X \otimes C \\ \downarrow{\scriptstyle \mathrm{id}_X \otimes \mathrm{id}_C \otimes \varepsilon} & \swarrow{\scriptstyle -\otimes -\otimes 1} & \\ X \otimes C \otimes k & & \end{array}$$

which commute, which can be seen due to the coassociative property of (C, Δ, ε). Hence $(X \otimes C, \mathrm{id}_X \otimes \Delta)$ is a right C-comodule.

Now that we have seen some examples of algebras over modules and comodules over coalgebras, we define the morphisms between them. We first begin

with morphisms of modules over algebras, and then, as should be instinctual at this point, dualize the respective diagrams to form the corresponding notion of a morphism of comodules over coalgebras.

Definition 3.5. Let (A, ∇, η) be a k-algebra, and let (X, Ψ_X) and (Q, Ψ_Q) be left A-modules. A k-linear map $f : X \to Q$ is called *morphism of A-modules* if the diagram

$$\begin{array}{ccc} A \otimes X & \xrightarrow{\mathrm{id}_A \otimes f} & A \otimes Q \\ \downarrow{\scriptstyle \Psi_X} & & \downarrow{\scriptstyle \Psi_Q} \\ X & \xrightarrow{f} & Q \end{array}$$

commutes. In other words, if we have

$$(f \circ \Psi_X)(a \otimes m) = (\Psi_Q \circ (\mathrm{id}_A \otimes f))(a \otimes m)$$

for all $a \in A$ and $m \in X$.

We can interpret the above definition in the following way: a morphism f of A-modules (X, Ψ_X) and (Q, Ψ_Q) satisfies

$$f(a \cdot m) = a \cdot f(m)$$

for all $a \in A$ and $m \in X$, where we have denoted the action of A on X and Q by symbol $\cdot$ for clarity.

We now flip the arrows in the above definition to describe the corresponding notion for comodules over a coalgebra.

Definition 3.6. Let (C, Δ, ε) be a k-coalgebra, and let (Y, Φ_Y) and (P, Φ_P) be right C-comodules. A k-linear map $g : Y \to P$ is called a *morphism of C-comodules* if the diagram

$$\begin{array}{ccc} P \otimes C & \xleftarrow{g \otimes \mathrm{id}_C} & Y \otimes C \\ \uparrow{\scriptstyle \Phi_P} & & \uparrow{\scriptstyle \Phi_Y} \\ P & \xleftarrow{g} & Y \end{array}$$

commutes. In other words, if we have that

$$(\Phi_P \circ g)(m) = ((g \otimes \mathrm{id}_C) \circ \Phi_Y)(m)$$

for all $m \in Y$.

Interpreting the above definition similarly as before: a morphism g of C-comodules (Y, Φ_Y) and (P, Φ_P) has the property that

$$((g \otimes \mathrm{id}_C) \circ \Phi_Y)(m) = (g \otimes \mathrm{id}_C)\left(\sum_{(m)} m_{(1)} \otimes c_{(2)}\right) = \sum_{(m)} g(m_{(1)}) \otimes c_{(2)}$$

must be equal to $\phi_P(g(m))$ for all $m \in Y$. Equivalently, we have

$$(\Phi_P \circ g)(m) = \sum_{(m)} g(m_{(1)}) \otimes c_{(2)}$$

for all $m \in Y$. Reflecting for a moment, the above assertion agrees with our intuitive sense for what "preserving the coaction" might mean, similarly to how morphisms of modules over an algebra preserve the action of the algebra on the modules.

3.2 Module and Comodule Categories

In the previous section, we defined a class of objects as well as morphisms between these objects. We are now at liberty to form a category. We form two categories: one for left modules over an algebra and one for right comodules over a coalgebra. In principle, however, we should be defining four categories, as we have also considered the notions of a right module over an algebra and a left comodule over a coalgebra. The reason we do not concern ourselves with these two additional categories is because we shall prove a result that will allow us to translate results from the category of left modules over an algebra (and right comodules over a coalgebra) to the cateogry of right modules over an algebra (and left comodules over a coalgebra).

We now define the categories mentioned above; they will occupy our time for the foreseeable future.

Definition 3.7. Let k be a field. For a k-algebra (A, ∇, η), we may form the *category of left A-modules*, denoted A**-Mod**, whose objects are left A-modules (X, Ψ) and whose morphisms are the morphisms of A-modules. Similarly, we may form the *category of right A-modules*, defined analagously, which we denote **Mod-**A.

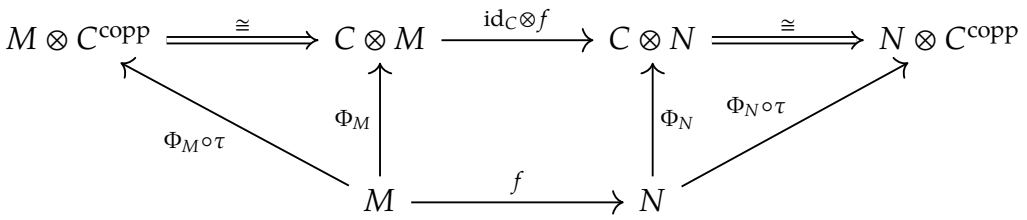
For a k-coalgebra (C, Δ, ε), we form the *category of right C-comodules*, denoted **CoMod-**C, whose objects are right C-comodules (Y, Φ) and whose morphisms are the morphisms of C-comodules. Similarly, the *category of left C-comodules* is denoted C**-CoMod**.

Theorem 3.8. Let (C, Δ, ε) be a k-coalgebra. Then the categories **C-CoMod** and **CoMod-**$C^{\mathbf{copp}}$ are isomorphic; the category of left C-comodules is isomorphic to the category of right C^{copp}-comodules.

Proof. Let (Y, Φ) be a left C-comodule. We may define a k-linear map $\Phi \circ \tau : Y \to Y \otimes C^{\mathrm{copp}}$ by $(\Phi \circ \tau)(m) = \sum_{(m)} m_{(1)} \otimes c_{(2)}$ for all $m \in Y$, and hence make (Y, Φ') a right C^{copp}-comodule.

Now let (M, Φ_M) and (N, Φ_N) be left C-comodules. If $f : M \to N$ is a morphism of left C-comodules, then set Φ'_M and Φ'_N as we did above. Then, since the underlying k-vector space of C and C^{copp} are identical, the

diagram



commutes; hence f is also a morphism of right C^{copp}-comodules. We use this fact to define a functor

$$\mathcal{F} : C\textbf{-CoMod} \to \textbf{CoMod-}C^{\mathbf{copp}}$$

$$(Y, \Phi) \mapsto (Y, \Phi \circ \tau)$$

Similarly, given a right C^{copp}-comodule (M, Φ)), define $\Phi \circ \tau : M \to C \otimes M$ by $(\Phi \circ \tau)(m) = \sum_{(m)} c_{(1)} \otimes m_{(2)}$ for all $m \in M$, and hence make $(M, \Phi \circ \tau)$ into a left C-comodule. A similar diagram to the above gives us a functor

$$\mathcal{G} : \textbf{CoMod-}C^{\mathbf{copp}} \to C\textbf{-CoMod}$$

$$(M, \Phi) \mapsto (M, \Phi \circ \tau)$$

It is immediate that $\mathcal{G}$ and $\mathcal{F}$ are inverses of one another, and hence we have our desired isomorphism. ■

The theorem above gives us a way to translate results regarding right comodules over coalgebras to left comodules over coalgebras, and hence we need only concern ourselves with one. By convention, the category selected will be that of the right comodules over a coalgebra.

3.3 The Category of Right Comodules

Now we go into more detail and describe properties of the category of right comodules over a coalgebra introduced in the previous section. We explore the subobjects and quotient objects in this category, prove a result that may be thought of as the "first isomorphism theorem for comodules over a coalgebra", and finish with a proof that the category of comodules over a coalgebra is an abelian category.

First we introduce the subobjects.

Definition 3.9. Let (C, Δ, ε) be a k-coalgebra, and let (M, Ψ) be a right C-comodule. We call a k-subspace N of M a *right C-subcomodule* if $\Psi(N) \subseteq N \otimes C$.

In other words, N is a right C-subcomodule of (M, Ψ) if the coaction $\Psi : M \to M \otimes C$ of C on M restricts to a coaction of C on N, i.e., we have that $(N, \Psi|_N)$ is a right C-comodule in its own right. Furthermore, since $N \subseteq M$, we have the inclusion map $\iota_N : N \hookrightarrow M$, and hence the diagram

$$\begin{array}{ccc} N & \xhookrightarrow{\iota_R} & M \\ {\scriptstyle \Psi|_N}\downarrow & & \downarrow{\scriptstyle \Psi} \\ N \otimes C & \xrightarrow{\iota_N \otimes \mathrm{id}_C} & M \otimes C \end{array}$$

commutes, which suffices to show that the inclusion map ι_N is a morphism of right C-comodules.

Proposition 3.10. Let (C, Δ, ε) be a k-coalgebra. Let (M, Ψ) be a right C-comodule with N a C-subcomodule of M. Then M/N has the structure of a right C-comodule.

Proof. Since $N \subseteq M$ is a k-subspace of M, we have the quotient space M/N a k-vector space. Let $\pi : M \to M/N$ be the canonical projection map. Since N is a right C-subcomodule, we know $\Psi(N) \subseteq N \otimes C$, and hence that

$$((\pi \otimes \mathrm{id}_C) \circ \Psi)(N) \subseteq (\pi \otimes \mathrm{id}_C)(N \otimes C) \subseteq \pi(N) \otimes C = 0 \otimes C = 0$$

and thus $N \subseteq \ker((\pi \otimes \mathrm{id}_C) \circ \Psi))$, and so by the universal property of the kernel there exists a k-linear map $\overline{\pi} : M/N \to M/N \otimes C$ such that the

diagram

$$\begin{array}{ccc} M & \xrightarrow{\pi} & M/N \\ {\scriptstyle\Psi}\downarrow & & \downarrow{\scriptstyle\overline{\pi}} \\ M \otimes C & \xrightarrow{\pi\otimes \mathrm{id}_C} & M/N \otimes C \end{array}$$

commutes. The map $\overline{\pi} : M/N \to M/N \otimes C$ is necessarily defined by

$$\overline{\pi}(m+N) = \sum_{(m)} \pi(m_{(1)}) \otimes c_{(2)} = \sum_{(m)} (m_{(1)} + N) \otimes c_{(2)}$$

for all cosets $m + N \in M/N$. Now note that for all $m + N \in M/N$ we have

$$\begin{aligned} ((\overline{\pi} \otimes \mathrm{id}_C) \circ \overline{\pi})(m+N) &= (\overline{\pi} \otimes \mathrm{id}_C)\left(\sum_{(m)} (m_{(1)} + N) \otimes c_{(2)}\right) \\ &= \sum_{(m)} (m_{(1)} + N) \otimes c_{(2)} \otimes c_{(3)} \\ &= (\mathrm{id}_{M/N} \otimes \Delta)\left(\sum_{(m)} (m_{(1)} + N) \otimes c_{(2)}\right) \\ &= ((\mathrm{id}_{M/N} \otimes \Delta) \circ \overline{\pi})(m+N) \end{aligned}$$

We also have

$$\begin{aligned} ((\mathrm{id}_{M/N} \otimes \varepsilon) \circ \overline{\pi})(m+N) &= \sum_{(m)} (m_{(1)} + N) \otimes \varepsilon(c_{(2)}) \\ &= \sum_{(m)} (m_{(1)} + N)\varepsilon(c_{(2)}) \otimes 1_k \\ &= (m+N) \otimes 1_k \end{aligned}$$

and hence $(M/N, \overline{\pi})$ is a right C-comodule. ∎

If we take a look at the diagram in our proof of Proposition 3.10, we will quickly realioze that the commutativity implies that $\overline{\pi}$ defined above is a morphism of right C-comodules from (M, Ψ) to $(M, \overline{\pi})$. The universal property of kernels invoked in the proof also gives us the uniqueness of the morphism $\overline{\pi}$ in the obvious way.

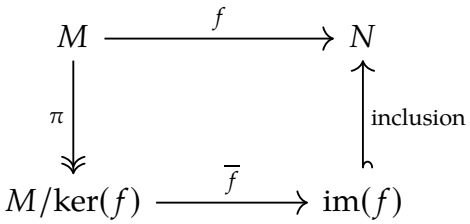
Definition 3.11. Let (C, Δ, ε) be a k-coalgebra, and let (M, Ψ) be a right C-comodule with C-subcomodule N. Then we call $(M/N, \overline{\pi})$ the *quotient C-comodule of M and N*, where $\overline{\pi}$ is the map defined in Proposition 3.10

Since our aim is to show that **CoMod-**C is an abelian category, we now show that the image of a morphism of comodules is a subcomodule of the target comodule, while the kernel of the morphism is a subcomodule of the source codmodule. More explicitly,

Proposition 3.12. Let (M, Ψ_M) and (N, Ψ_N) be right C-comodules, and suppose $f : M \to N$ is a morphism of comodules. Then $\ker(f)$ is a right C-subcomodule of M and $\mathrm{im}(f)$ is a right C-subcomodule of N.

Proof. A proof can be found in [DNR00]. ∎

Proposition 3.13. Let (M, Ψ_M) and (N, Ψ_N) be right C-comodules, and suppose $f : M \to N$ is a morphism of comodules. Let $\pi : M \to M/\ker(f)$ be the canonical projection map. Then there exists a unique isomorphism of right C-comodules $\overline{f} : M/\ker(f) \to \mathrm{im}(f)$ such that the diagram



commutes.

Proof. A proof can be found in [DNR00]. ∎

3.4 Hopf Algebras Acting on Algebras

In this section we analyze the ways in which Hopf algebras act on algebras. To do this, we first define a new object, a so-called Hopf module algebra, which will encode such an action.

Definition 3.14. Let $(H, \nabla, \eta, \Delta, \varepsilon, S)$ be a k-Hopf algebra. A k-algebra (A, ∇_A, η_A) is called a *left H-module algebra* if A is a left H-module with Hopf action $h \cdot a$ for all $h \in H$ and $a \in A$, and which satisfies

$$h \cdot (ab) = \sum_{(h)} (h_{(1)} \cdot a)(h_{(2)} \cdot b)$$

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

for all $a, b \in A$ and $h \in H$.

Let (A, ∇, η) be a k-algebra which admits a left H-module structure, with action of H on A given by

$$\nu : H \otimes A \to A$$

defined by $\nu(h \otimes a) = h \cdot a$ for all $h \in H$ and $a \in A$. The tensor product has the adjunction property, and hence there is a bijective correspondence

$$\mathrm{Hom}(H \otimes A, A) \longleftrightarrow \mathrm{Hom}(A, \mathrm{Hom}(H, A))$$

3.5 Smash Products

We now introduce a somewhat peculiar algebra which is associated to the action of a Hopf algebra on another algebra. This specific construction will prove crucial in our coming exploration of Hopf-Galois extensions later on.

Definition 3.15. Let H be a k-Hopf algebra and let A be a left H-module algebra with Hopf action $h \cdot a$ for all $h \in H$ and $a \in A$. Then the k-vector space $A \otimes H$ equipped with the operation $\# : (A \otimes H) \otimes (A \otimes H) \to A \otimes H$ defined by

$$\#(a \otimes h, b \otimes g) = \sum_{(h)} a(h_{(1)} \cdot b) \otimes h_{(2)}g$$

for all $a, b \in A$ and $h, g \in H$ is called the *smash product of A with H*, which we denote by $A\#H$. We also write elements of $A\#H$ as $a\#h$ for $a \in A$ and $h \in H$. Under this notation, the binary operation $\#$ is given by

$$(a\#h)(b\#g) = \sum_{(h)} a(h_{(1)} \cdot b)\#h_{(2)}g$$

for all $a, b \in A$ and $h, g \in H$.

3.6 Hopf Algebras Coacting on Coalgebras

In a similar fashion as we defined left module algebras, we may also define left comodule coalgebras.

Proposition 3.16. Let k be a field. Let H be a finite dimensional k-Hopf algebra and let A be a k-algebra. If

$$\Psi : A \to A \otimes H^*$$
$$a \longmapsto \sum_{(a)} a_{(0)} \otimes a_{(1)}$$

is a coaction, then we have

$$\Phi : A \otimes H \to A$$
$$h \otimes a \longmapsto \sum_{(a)} a_{(1)}(h) a_{(0)}$$

is an action. Furthermore, we have that (S, Φ) is a left H-module algebra if and only if (S, Ψ) is a left H-comodule algebra.

Proposition 3.17. Let H be a finite dimensional k-Hopf algebra and let A be a left H-module algebra. Then the map

$$j : A \otimes H \to \mathrm{End}_k(A)$$
$$j(a \otimes h)(b) = a(h \cdot b)$$

is a k-linear isomorphism of k-algebras if and only if the map

$$\Psi' : A \otimes A \to A \otimes H^*$$
$$a \otimes b \longmapsto \sum_{(b)} a b_{(0)} \otimes b_{(1)}$$

is a k-linear isomorphism.

❖ Hopf-Galois Theory

In this section we devote ourselves fully to the classification of so-called Hopf-Galois structures on separable field extensions. We perform this by means of a famous theorem of Greither and Pareigis, which quite effectively transforms the classification problem for Hopf-Galois extensions (to be defined presently) into a (usually non-)trivial group-theoretic problem. The original paper is [PG87], however we caution the reader to be wary; much is left to the imagination in this paper. In our treatment of the theory, we follow closely [Chi00]. We recommend as a reference to a more advanced reader the book [CGK+21].

Somewhat curiously, the Hopf-Galois theory associated with separable, not necessarily normal, field extensions, finds wide application in the case where a field extension is, in fact, normal as well. That is, we can apply the aforementioned theorem of Greither and Pareigis to Galois extensions of fields and obtain (and recover) many fascinating results.

We make a brief remark that applications of Hopf-Galois theory for separable field extensions, particularly in the realm of Galois module theory, may be found in [Chi89].

4.1 Hopf-Galois Structures

We begin our development of Hopf-Galois theory by first motivating the definition of Hopf-Galois structures on finite extensions of fields.

We prompt this motivation by letting K/k be a finite extension of fields. Let $\mathrm{Aut}_k(K)$ denote the group of automorphisms of K which leave the base field k fixed, that is the set of field isomorphisms $\sigma : K \to K$ such that $\sigma(a) = a$ for all $a \in k$. Now let G be a subgroup of $\mathrm{Aut}_k(K)$. We know from our initial brush with Hopf algebras that the group ring $k[G]$ then becomes a k-Hopf algebra in the usual way.

For convenience we restate this 'usual way' of placing a k-Hopf algebra structure on the group ring $k[G]$ as follows: $(k[G], \nabla, \eta, \Delta, \varepsilon, S)$ is a k-Hopf algebra where the associated structure maps are defined by:

$$\nabla\left(\sum_{g\in G} a_g[g] \otimes \sum_{g\in G} b_g[g]\right) = \left(\sum_{g\in G} a_g[g]\right)\left(\sum_{g\in G} b_g[g]\right)$$

for the multiplication map, so that multiplication is simply the usual multiplication in the group ring $k[G]$, which we shall oftentimes for simplicity write as

juxtaposition of elements, and, letting 1_G denote the identity element of G,

$$\eta(a) = a[1_G]$$

so that the unit map simply associates k with its isomorphic copy in the group ring, where we shall often drop the $[1_G]$ and write simply a for $a \in k$. Furthermore, we have for the comultiplication and counit maps:

$$\Delta\left(\sum_{g\in G} a_g[g]\right) = \sum_{g\in G} a_g[g \otimes g]$$

$$\varepsilon\left(\sum_{g\in G} a_g[g]\right) = \sum_{g\in G} a_g$$

Lastly, for the antipode map, we have the following:

$$S\left(\sum_{g\in G} a_g[g]\right) = \sum_{g\in G} a_g[g^{-1}]$$

In fact, under these conditions, we can make the extension field K into a left $k[G]$-module algebra, as we shall now see.

Proposition 4.1. Let K/k be a finite extension of fields and let G be a subgroup of $\mathrm{Aut}_k(K)$. Then K is a left $k[G]$-module algebra.

Proof. We already know that $k[G]$ is a k-Hopf algebra in the usual sense. To prove that K is a left $k[G]$-module algebra we must first show that K is a left $k[G]$-module: we have the obvious Hopf action given by $\cdot : k[G] \times K \to K$ via

$$\sum_{g\in G} a_g[g] \cdot \beta = \sum_{g\in G} a_g g(\beta)$$

for all $\beta \in K$ and $a_g \in k$. This Hopf action is easily seen to make K into a left $k[G]$-module algebra. To see this, note that for a basis element $[g] \in k[G]$ and any $\alpha, \beta \in K$ we have

$$[g] \cdot (\alpha\beta) = g(\alpha\beta) = g(\alpha)g(\beta) = ([g] \cdot \alpha)([g] \cdot \beta)$$

More generally, for an arbitrary element $h = \sum_{g\in G} a_g[g]$ in $k[G]$ we have

$$\begin{aligned} h\cdot(\alpha\beta) &= \sum_{g\in G} a_g[g]\cdot(\alpha\beta) \\ &= \sum_{g\in G} a_g g(\alpha\beta) \\ &= \sum_{g\in G} a_g g(\alpha)g(\beta) \\ &= \sum_{(h)} (h_{(1)}\cdot\alpha)(h_{(2)}\cdot\beta) \end{aligned}$$

and also

$$h\cdot 1_K = \sum_{g\in G} a_g g(1_K) = \sum_{g\in G} a_g 1_K = \varepsilon(h)1_K$$

where 1_K obviously denotes the identity element of K. Hence K is indeed a left $k[G]$-module algebra, the desired statement. ■

The above result should not seem too surprising, as it captures some fairly intuitive notions about how $\mathrm{Aut}_k(K)$, and its subgroups, should interact on the extension K. We can push this idea further so as to proceed with the theory. One may first note that a k-linear combination of automorphisms of K which fix k is not, in general, another automorphism of K fixing k, rather an endomorphism of K. We capture this idea with the fact that the k-Hopf algebra $k[G]$ acts on K as a left $k[G]$-module algebra, the above proposition. We are certainly getting somewhere, yes.

To make sure we are on the right track in defining what we will eventually refer to as a Hopf-Galois structure, we consider the case where the original finite extension of fields K/k is actually Galois. We have the following proposition.

Proposition 4.2. Let K/k be a finite extension of fields and let G be a subgroup of $\mathrm{Aut}_k(K)$. Then K/k is a Galois extension with $G = \mathrm{Gal}(K/k)$ if and only if the k-linear map

$$j : K\#k[G] \to \mathrm{End}_k(K)$$

from the smash product k-algebra $K\#k[G]$ to the endomorphism k-algebra $\mathrm{End}_k(K)$ defined by

$$j\left(\beta\#\sum_{g\in G} a_g[g]\right)(\alpha) = \beta\left(\sum_{g\in G} a_g[g]\cdot\alpha\right)$$

for all $\alpha, \beta \in K$ and $a_g \in k$ is an isomorphism of k-algebras.

Proof. Suppose first that K/k is Galois. Note that for $[g], [g'] \in k[G]$ and $\beta, \beta' \in K$ we have

$$(\beta\#[g])(\beta'\#[g']) = \beta g(\beta')\#[gg']$$

as the multiplication in the smash product algebra $K\#k[G]$. Now observe that

$$\begin{aligned} j\left(\beta g(\beta')\#[gg']\right)(\alpha) &= \beta g(\beta')(gg')(\alpha) \\ &= \beta g(\beta')g(g'(\alpha)) \\ &= \beta g(\beta' g'(\alpha)) \\ &= j(\beta\#[g])(\beta' g'(\alpha)) \\ &= j(\beta\#[g])(j(\beta'\#[g'](\alpha))) \\ &= (j(\beta\#[g]) \circ j(\beta'\#[g']))(\alpha) \end{aligned}$$

Recalling that the underlying ring structure of the k-algebra $\mathrm{End}_k(K)$ has multiplication given by function composition, we find that the map j above is indeed a ring homomorphism. In fact, we also have that

$$j(r\beta\#[g])(\alpha) = r\beta g(\alpha) = r\, j(\beta\#[g])(\alpha)$$

for all $r \in k$, $\beta \in K$, and $[g] \in k[G]$. In this way, the map j above is a veritable homomorphism of k-algebras. Now we must show that j is bijective. To this end, suppose that

$$j\left(\beta\# \sum_{g\in G} a_g[g]\right)(\alpha) = \beta\left(\sum_{g\in G} a_g(\alpha)\right) = \sum_{g\in G} \beta a_g g(\alpha) = 0$$

holds for all $\alpha \in K$. By Example 2.24, since we know that $G(k[G]) = \{[g] \mid g \in G\}$ is the set of grouplikes of the k-Hopf algebra $k[G]$, we have linear independence, which gives $\beta a_g = 0$ for each $g \in G$, whence the original element of $K\#k[G]$ is zero, giving injectivity. Since K/k is finite, let $n = \dim_k(K)$. By dimension considerations, we have

$$\dim_k(K\#k[G]) = \dim_k(K)\dim_k(k[G]) = n \cdot |G| = n^2 = \dim_k(\mathrm{End}_k(K))$$

which follows since K/k being Galois means $G = \mathrm{Gal}(K/k)$ satisfies $|G| = n$. Since the dimension of both the domain and the codomain coincide, alongside injectivity, we have surjectivity; hence j is an isomorphism of k-algebras.

For the converse, assume that j is an isomorphism. For the same dimension considerations as above, we require that $|G| = [K : k]$. Now take

$K = k(\alpha)$ and let $p(x)$ be the minimal polynomial for α over k having degree $n = [K : k]$. Since $|G| = n$ each element of G must take α to another root β for $p(x)$, i.e., K is the splitting field for $p(x)$ over k, hence K/k is Galois, and we require G be a subgroup of $\mathrm{Gal}(K/k)$. But $|\mathrm{Gal}(K/k)| = n$ and so $G = \mathrm{Gal}(K/k)$. ■

Now we are getting to the heart of the matter, the truly important observation to be made. In the scenario where the original extension K/k is actually Galois, the proposition above states that the tensor product of $K \otimes_k k[G]$ under a sort of twisted multiplication (this is the smash product $K\#k[G]$ above) coincides with the endomorphism ring of K over k. That is, we can, in some sense, extend the usual action of the Galois group on K to an action of the group ring $k[G]$, a k-Hopf algebra, tensored with K.

We take a moment to investigate the j map described above. Note that for K/k a Galois extension of fields with $G = \mathrm{Gal}(K/k)$, we have a sort of fixed ring given by the set

$$K^{k[G]} = \{\beta \in K \mid h \cdot \beta = \varepsilon(h)\beta \text{ for all } h \in k[G]\}$$

which one easily verifies to indeed carry the structure of a subring of K. We may rewrite the above fixed ring equivalently as follows:

$$K^{k[G]} = \{\beta \in K \mid \sum_{g \in G} a_g[g] \cdot \beta = \sum_{g \in G} a_g\beta \text{ for all } \sum_{g \in G} a_g[g] \in k[G]\}$$

so as to make our discussion more concrete. Since K/k is Galois, from the above proposition we know that the map $j : K\#k[G] \to \mathrm{End}_k(K)$ is an isomorphism of k-algebras. We claim that $K^{k[G]} = k$. One direction is clear, $k \subseteq K^{k[G]}$ since $\alpha \in k$

satisfies $g(\alpha) = \alpha$ for all $g \in G$. For the reverse inclusion, take $\beta \in K^{k[G]}$. Then

$$\begin{aligned}(\beta\#[1_G])\left(\beta'\# \sum_{g\in G} a_g[g]\right) &= \beta 1_G(\beta')\#[1_G] \cdot \sum_{g\in G} a_g[g] \\ &= \beta\beta'\# \sum_{g\in G} a_g[g] \\ &= \sum_{g\in G} (\beta\beta'\# a_g[g]) \\ &= \sum_{g\in G} (\beta' a_g \beta\#[g]) \\ &= \sum_{g\in G} (\beta' a_g g(\beta)\#[g]) \\ &= \beta' \sum_{g\in G} a_g g(\beta)\#[g] \\ &= \left(\beta'\# \sum_{g\in G} a_g[g]\right)(\beta\#[1_G])\end{aligned}$$

The reader is warned not to be confused with the passing of the scalars $a_g \in k$ over the # symbol, for in this context $\# = \otimes$ with a fancier multiplication, that of the twisted multiplication which encapsulates the smash product $K\#k[G]$. In particular, the above shows that any element of the form $\beta\#[1_G]$ for $\beta \in K$ commutes with all elements of $K\#k[G]$, so the set of such elements lies in the center of this k-algebra. Since the isomorphism j must take the center to the center, we know that every k-linear endomorphism of the form

$$j(\beta\#[1_G])(\alpha) = \beta(1_G \cdot \alpha) = \beta 1_G(\alpha) = \beta\alpha$$

for $\alpha \in K$ must lie in the center of $\mathrm{End}_k(K)$. Note that these maps are simply left multiplication (in the ring K) by an element of K. However recall that the center of $\mathrm{End}_k(K)$ is precisely isomorphic to k, for instance via the ring homomorphism

$$k \to \mathrm{End}_k(K)$$

$$r \longmapsto r\mathrm{id}_K$$

Then for any arbitrary $f \in \mathrm{End}_k(K)$, for any $r \in k$ we have that $k \subseteq Z(\mathrm{End}_k(K)$,

since

$$\begin{aligned}(r\mathrm{id}_K \circ f)(\alpha) &= r\mathrm{id}_K(f(\alpha)) \\ &= rf(\alpha) \\ &= f(r\alpha) \\ &= f(r\mathrm{id}_K(\alpha)) \\ &= (f \circ r\mathrm{id}_K)(\alpha)\end{aligned}$$

and in fact the converse is true as well, as can easily be shown. In particular, since we have shown that the k-linear endomorphism $j(\beta\#[1_G])$ lies in $Z(\mathrm{End}_k(K))$, we have also shown that $j(\beta\#[1_G])$ corresponds (isomorphically, since we have identified k with its image under the ring homomorphism into $\mathrm{End}_k(K)$ above) to an element of k, whence $K^{k[G]} \subseteq k$, giving us $K^{k[G]} = k$.

The winds have shifted, so to speak. Something deeper is going on here: to recount the discussion, a Galois extension of fields K/k corresponds to a strange action of the smash product algebra $K\#k[G]$ on the overfield K by endomorphisms, and the fixed ring associated to this action is precisely the base field k.

Having witnessed whatever happened above, we attempt to generalize. We would like to have some Hopf algebra associated to an extension of fields in some compatible way, so as to make the machinery above work. This will be the notion of a Hopf-Galois extension, or a Hopf-Galois structure on an extension of fields.

Definition 4.3. Let K/k be a finite extension of fields, and let H be a finite-dimensional k-Hopf algebra. Then the extension K/k is said to be an *H-Galois extension* if K is a left H-module algebra with Hopf action $h \cdot \alpha$ for all $h \in H$ and $\alpha \in K$, and the k-linear homomorphism

$$j : K \otimes_k H \to \mathrm{End}_k(K)$$

$$j(\beta \otimes h)(\alpha) = \beta(h \cdot \alpha)$$

is an isomorphism of k-algebras between the smash product algebra $K\#H$ and the endomorphism algebra $\mathrm{End}_k(K)$. More generally, we call the pair $(H, \cdot)$, where H is the k-Hopf algebra and $\cdot$ the Hopf action making K into a left H-module algebra, a *Hopf-Galois structure* on the extension.

We also translate our work with the fixed ring considered previously.

Definition 4.4. Let k be a field and let H be a finite dimensional k-Hopf algebra with counit ε. If A is left H-module with action $h \cdot \alpha$ for all $h \in H$ and $\alpha \in A$,

which is also finite dimensional as a k-vector space, then we define

$$A^H = \{\beta \in A \mid h \cdot \beta = \varepsilon(h)\beta \text{ for all } h \in H\}$$

which we refer to as the *fixed ring of A by H*.

Note immediately that if K/k is a Galois extension of fields then K/k is $k[G]$-Galois, where $G = \mathrm{Gal}(K/k)$, in particular since by definition K is a left $k[G]$-module which is also finite dimensional as a k-vector space, and so we recover the fixed ring $(k[G])^G = k$ previously mentioned.

For our sanity, it would do well for us to construct an example of the above definition of a Hopf-Galois structure, as well as the associated fixed ring, so as to ground ourselves. In the midst of the example, we shall discover something which makes these Hopf-Galois structures rather peculiar.

Example 4.5. Consider the extension $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$, which we know is a Galois extension with $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) \cong S_3$, the symmetric group on 3 letters (if one is unsure, note that $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ is the splitting field for the irreducible polynomial $x^3 - 2$ over $\mathbb{Q}$). Let $S_3 = \langle \sigma, \tau \rangle$, where the relations are given as $\sigma^3 = \tau^2 = 1$ and $\sigma\tau = \tau\sigma^{-1}$.

From our work in Proposition 4.1, we get that $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ is a left $\mathbb{Q}[S_3]$-module algebra, and from Proposition 4.2 the fact that the extension is Galois ensures that the j map is an isomorphism; hence $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ is a $\mathbb{Q}[S_3]$-Galois extension of fields. This gives us the usual, what some might call the 'classical' Hopf-Galois structure on the extension.

This is all well and good, however we entertain the following line of thought. Let S_3 act on the $\mathbb{Q}$-Hopf algebra $H = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)[S_3]$ by the usual Galois action on elements of $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ and composition of permutations on S_3. That is, define an action on generators for S_3 via

$$\sigma \cdot (a_1 + a_2[\sigma] + a_3[\sigma^2] + a_4[\tau] + a_5[\sigma\tau] + a_6[\sigma^2\tau])$$

$$= \sigma(a_1) + \sigma(a_2)[\sigma] + \sigma(a_3)[\sigma^2] + \sigma(a_4)[\tau] + \sigma(a_5)[\sigma\tau] + \sigma(a_6)[\sigma^2\tau]$$

and

$$\tau \cdot (a_1 + a_2[\sigma] + a_3[\sigma^2] + a_4[\tau] + a_5[\sigma\tau] + a_6[\sigma^2\tau])$$

$$= \tau(a_1) + \tau(a_2)[\sigma] + \tau(a_3)[\sigma^2] + \tau(a_4)[\tau] + \tau(a_5)[\sigma\tau] + \tau(a_6)[\sigma^2\tau]$$

on elements of H. Then we have a subset of H fixed by the action from S_3 given by

$$H^{S_3} = \{x \in H \mid \sigma(x) = \tau(x) = x\}$$

A somewhat lengthy computation yields that

$$H^{S_3} = \{a_1 + a_2[\sigma] + \tau(a_2)[\sigma^2] + a_3[\tau] + \sigma^2(a_3)[\sigma\tau] + \sigma(a_3)[\sigma^2\tau]\}$$

where $a_1 \in \mathbb{Q}$, $a_2 \in \mathbb{Q}(\zeta_3)$, and $a_3 \in \mathbb{Q}(\sqrt[3]{2})$ vary. One finds that this fixed subset is a 6-dimensional $\mathbb{Q}$-Hopf algebra which acts on $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ to turn this $\mathbb{Q}$-algebra into a left H^{S_3}-module algebra, and by dimension considerations, make the j map in this case an isomorphism. Now we have that $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ is an H^{S_3}-Galois extension. However, clearly we have $H^{S_3} \ncong \mathbb{Q}[S_3]$, and so we have a verifiably different Hopf-Galois structure on the original extension. Curious.

The example may answer some questions readers may have had by this point. Indeed, on an arbitrary finite extension of fields K/k, one can have multiple different Hopf-Galois structures corresponding to different k-Hopf algebras. This prompts a quick definition:

Definition 4.6. Let K/k be a finite extension of fields. If $(H, \cdot)$ and $(H', \cdot')$ are two Hopf-Galois structures on K/k, then we say that $(H, \cdot)$ and $(H', \cdot')$ are *isomorphic Hopf-Galois structures* if $H \cong H'$ as k-algebras which is compatible with the actions $\cdot$ and $\cdot'$ on K.

The usual Galois theory lacks this problem completely. For a given Galois extension, there is a unique Galois group acting on the overfield by automorphisms which fix the base field. However, as we just saw, even in the case where an extension is Galois, a Hopf-Galois extension may have several different (non-isomorphic) Hopf-Galois structures. This is perhaps worrisome, for now we would like to classify all such Hopf-Galois structures possible, and in general this is a computationally and emotionally intensive task.

Luckily there is theory to be found in the case where the original extension of fields is separable; this is of course via a theorem of Greither and Pareigis, which we now develop with zeal.

4.2 Normalizers and Regular Subgroups

Before we can fully develop and appreciate the classification theorem of Greither and Pareigis, we first recall several definitions and basic facts regarding so-called regular subgroups of permutation groups. These kinds of groups play a key role in the theorem itself, and many properties shall be employed in our proofs to come.

Let G be an arbitrary group, and let $A \subseteq G$ be a non-empty subset of G (not necessarily a subgroup of G).

Definition 4.7. Define $\text{Cent}_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$. This subset of G is called the *centralizer* of A in G. Since $gag^{-1} = a$ if and only if $ga = ag$, we can see that $\text{Cent}_G(A)$ is the set of elements of G which commute with every element of A.

Let 1_G denote the identity element of an arbitrary group G. We show that $\text{Cent}_G(A)$ is a subgroup of G for any $A \subseteq G$ with $A \neq \emptyset$. Firstly, $\text{Cent}_G(A) \neq \emptyset$ because $1_G \in \text{Cent}_G(A)$ is immediate, as the definition of the identity specifies that $1_G a = a 1_G$ for all $a \in G$, and so in particular for all $a \in A$. Secondly, if $x, y \in \text{Cent}_G(A)$, then $xax^{-1} = a$ and $yay^{-1} = a$ for all $a \in A$, and so

$$\begin{aligned}(xy)a(xy)^{-1} &= (xy)(y^{-1}x^{-1}) \\ &= x(yay^{-1})x^{-1} \\ &= xax^{-1} \\ &= a\end{aligned}$$

and hence $xy \in \text{Cent}_G(A)$, which means the centralizer is closed under products, meaning $\text{Cent}_G(A)$ is indeed a subgroup of G. For an example, note that if G is abelian then $\text{Cent}_G(A) = G$, as can be immediately verified.

Definition 4.8. Define $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. Define the *normalizer* of A in G to be the set $\text{Norm}_G(A) = \{g \in G \mid gAg^{-1} = A\}$.

Notice that if we have $g \in \text{Cent}_G(A)$, then $gag^{-1} = a \in A$ for all $a \in A$, and so $\text{Cent}_G(A)$ is a subgroup of $\text{Norm}_G(A)$. The proof that $\text{Norm}_G(A)$ is a subgroup of G follows identically as the proof above.

Definition 4.9. Let G be a group and let A and B be subgroups of G. It is said that A is *normalized* by B, or that B *normalizes* A, if for every $b \in B$ and $a \in A$, we have $bab^{-1} \in A$.

A quick check shows that the statement A is normalized by B is equivalent to $B \subseteq \mathrm{Norm}_G(A)$, i.e., that B is contained in the normalizer of A in G.

It is well-known in group theory that the fact that both of the above subsets of G, the centralizers and normalizers of non-empty subsets of G, are subgroups can be deduced as special cases of results on group actions. In a sense, the structure of G is reflected by the sets on which it acts.

Definition 4.10. Let G be a group and S a non-empty set and suppose G acts on S with action $g \cdot s$ for all $g \in G$ and $s \in S$. For any $s \in S$, define a subset of G

$$\mathrm{Stab}_G(s) = \{g \in G \mid g \cdot s = s\}$$

which we call the *stabilizer* of s in G.

The fact that the stabilizer of s in G is a subgroup easily follows from the axioms for group actions. Clearly $1_G \in \mathrm{Stab}_G(s)$. Also, if $y \in \mathrm{Stab}_G(s)$ then

$$\begin{aligned} s &= 1_G \cdot s \\ &= (y^{-1}y) \cdot s \\ &= y^{-1} \cdot (y \cdot s) \\ &= y^{-1} \cdot s \end{aligned}$$

and hence $y^{-1} \in \mathrm{Stab}_G(s)$, so that the stabilizer is closed under the taking of inverses. Now if $x, y \in \mathrm{Stab}_G(s)$ then

$$\begin{aligned} (xy) \cdot s &= x \cdot (y \cdot s) \\ &= x \cdot s \\ &= s \end{aligned}$$

Some minor details alongside the above facts give us that $\mathrm{Stab}_G(s)$ is a subgroup of G. As we mentioned previously, we can recover some facts about normalizers and centralizers via this view. If we let G act on S by conjugation, then the normalizer of A in G is precisely the stabilizer of A in G, $\mathrm{Norm}_G(A) = \mathrm{Stab}_G(A)$. Now if we let $\mathrm{Norm}_G(A)$ act on A by conjugation, then the kernel of this action is precisely $\mathrm{Cent}_G(A)$.

Definition 4.11. Let N be a subgroup of S_n, the group of permutations on n letters. Then N acts on $\{1, \ldots, n\}$, which we denote by $n(i)$ for $n \in N$ and $i \in \{1, \ldots, n\}$. We say the action of N on $\{1, \ldots, n\}$ is *transitive* if for every pair $i, j \in \{1, \ldots, n\}$ there exists $n \in N$ such that $n(i) = j$.

If the action of N on $\{1, \ldots, n\}$ is transitive, then we simply write that N is *transitive* as a subgroup of S_n.

Proposition 4.12. Let S be a non-empty finite set. Let $\mathrm{Perm}(S)$ denote the group of permutations of S. If N is a subgroup of $\mathrm{Perm}(S)$, then any two of the following conditions imply the third.

1. The cardinality of N is equal to that of S; $|N| = |S|$.
2. N is transitive as a subgroup of $\mathrm{Perm}(S)$.
3. For every $s \in S$, the stabilizer of s in N is trivial; $\mathrm{Stab}_N(s) = \{1_N\}$, where 1_N denotes the identity element of N.

Proof. Suppose (1) and (2) hold. Fix any $s \in S$. Consider the set-map $\phi : N \to S$ defined by $\phi(m) = m \cdot s$ for all $m \in N$. If $s' \in S$ is arbitrary, then since N is transitive there exists $n' \in N$ such that $n'(s) = s'$. Hence ϕ is surjective, and since $|N| = |S|$, we have a bijection. Since ϕ is injective, $n \cdot s = m \cdot s$ implies $n = m$ for all $n, m \in N$. In particular, if $n \in \mathrm{Stab}_N(s)$ then $n \cdot s = s$, and so $n \cdot s = 1_N \cdot s$ implies $n = 1_N$, meaning that $\mathrm{Stab}_N(s) = \{1_N\}$, which is (3).

Suppose (2) and (3) hold. We exploit the same map $\phi : N \to S$ as before. Since N is transitive, given $s' \in S$ there is some $n \in N$ for which $n \cdot s = s'$, and hence $\phi(n) = s'$, to which ϕ is surjective. Moreover, if $\phi(n) = \phi(m)$ then $n \cdot s = m \cdot s$ and so $m^{-1}n \cdot s = 1_N \cdot s = s$ as before, and so (3) gives that $m^{-1}n = 1_N$ to which $m = n$. Hence ϕ is injective, and so must be a bijection, giving $|N| = |S|$, which is (1).

Lastly, suppose (1) and (3) hold. As we saw previously, (3) gives that $\phi : N \to S$ is injective, and since $|N| = |S|$ by (1), we have surjectivity as well, which is equivalent to (2) as before. ∎

Definition 4.13. Let S be a non-empty finite set and let $\mathrm{Perm}(S)$ denote once again the group of permutations of S. A subgroup N of $\mathrm{Perm}(S)$ is called *regular* if any two conditions in Proposition 4.12 hold.

In the proof of Proposition 4.12 we exploted (quite heavily) the set-map $\phi : N \to S$ given by $\phi(n) = n \cdot s$ for all $n \in N$, and where $s \in S$ is fixed. To capture the idea of a regular subgroup N of $\mathrm{Perm}(S)$ more explicitly, we have the following:

Proposition 4.14. Let S be a non-empty finite set and let $\mathrm{Perm}(S)$ denote the group of permutations on S. Then N acts on S, say by $n \cdot s$ for all $n \in N$ and $s \in S$. A subgroup N of $\mathrm{Perm}(S)$ is regular if and only if for all $s \in S$ the set-map $\phi : N \to S$ defined by $\phi(n) = n \cdot s$ is bijective.

Proof. The proof is simply a rephrasing of what we showed in that of Proposition 4.12, and so we leave it to the reader. ■

We sometimes casually refer to such regular subgroups as regular permutations groups (the fact that they are subgroups of some permutation group is implicit, and should be clear from the context we are working in).

With the above preliminaries in mind, we are ready to proceed to the theory which we are primarily concerned with: Hopf-Galois structures on separable extensions of fields.

4.3 Base Changing Hopf-Galois Extensions

In order to properly attack the theorem of Greither and Pareigis, we cover a specific instance of base change. For a rough outline of what we hope to accomplish: given a separable extension of fields K/k with a Hopf-Galois structure given by H a k-Hopf algebra, we would like to show that the extension $\widetilde{K} \otimes_k K/K$ is also Hopf-Galois, where $\widetilde{K}$ denotes the normal closure of K. This necessitates base changing the original k-Hopf algebra H in some way, which we now explain.

Proposition 4.15. Let K/k be a finite extension of fields and let H be a k-Hopf algebra. Then the scalar extension $K \otimes_k H$ is a K-Hopf algebra.

Proof. Clearly K is a finite dimensional k-vector space, and so too is the k-Hopf algebra H, hence we may consider the tensor product $K \otimes_k H$ as a K-vector space where scalar multiplication is given by

$$\alpha(\beta \otimes h) = r\beta \otimes h$$

for all $\alpha, \beta \in K$, and $h \in H$, simply left multiplication by elements of K on the K portion of $K \otimes_k H$. Now recall that K is a K-Hopf algebra over itself (the trivial Hopf algebra). We know that given any k-linear map $\phi : V \to W$ where V and W are K-vector spaces, we have that $\phi \otimes \mathrm{id}_K : K \otimes_k V \to K \otimes_k W$ is a K-linear map under this scalar multiplication above. In particular, we can take all of the K-linear maps making K into a K-Hopf algebra over itself, and tensor them with the k-Hopf algebra H to obtain K-linear maps, sufficing to make $K \otimes_k H$ into a K-Hopf algebra. ∎

With the above in mind, we now show that given a Hopf-Galois structure on an extension of fields, we can base change up and tensor over the normal closure of the overfield to obtain yet another Hopf-Galois structure, one which will prove crucial in our upcoming developments.

Theorem 4.16. Let H be a k-Hopf algebra and let K/k be an H-Galois extension of fields with Hopf action of H given by $h \cdot \alpha$ for $h \in H$ and $\alpha \in K$. Let $\widetilde{K}$ denote the normal closure of K. Then the extension $(\widetilde{K} \otimes_k K)/\widetilde{K}$ is an $(\widetilde{K} \otimes_k H)$-Galois extension, where the Hopf action of $\widetilde{K} \otimes_k H$ is given by

$$* : (\widetilde{K} \otimes_k H) \otimes_{\widetilde{K}} (\widetilde{K} \otimes_k K) \to \widetilde{K} \otimes_k K$$

$$(\widetilde{\beta} \otimes h) * (\widetilde{\gamma} \otimes \alpha) = (\widetilde{\beta}\widetilde{\gamma}) \otimes (h \cdot \alpha)$$

for all $\widetilde{\beta}, \widetilde{\gamma} \in \widetilde{K}$, $h \in H$, and $\alpha \in K$.

Proof. We know from Proposition 4.15 that $\widetilde{K} \otimes_k H$ is a K-Hopf algebra since $\overline{K}/K/k$ is a tower of fields. We make a brief note that $\widetilde{K} \otimes_k K$ is a finite extension of K, which can be seen for if $\{e_1, \ldots, e_n\}$ is a k-basis for K over k, then $\{1_{\widetilde{K}} \otimes e_1, \ldots, 1_{\widetilde{K}} \otimes e_n\}$ is an $\widetilde{K}$-basis of $\widetilde{K} \otimes_k K$. What remains is to check that $\widetilde{K} \otimes_k K$ is a left $(\widetilde{K} \otimes_k H)$-module algebra and that the respective j map is an isomorphism of $\widetilde{K}$-algebras.

For the first, note that by assumption K is a left H-module algebra, and so we have the commutative diagrams associated to this definition. Tensoring with $\widetilde{K}$ the maps are K-linear and commutative, giving us immediately that $\widetilde{K} \otimes_k K$ is also a left $(\widetilde{K} \otimes_k H)$-module algebra.

Now we treat the second requirement. Since K/k is H-Galois, we have a k-linear isomorphism

$$j : K \otimes_k H \to \mathrm{End}_k(K)$$

$$j(\beta \otimes h)(\alpha) = \beta(h \cdot \alpha)$$

Tensoring alongside $\widetilde{K}$ gives the $\widetilde{K}$-linear isomorphism

$$1 \otimes j : \widetilde{K} \otimes_k \otimes_k K \otimes_k H \to \widetilde{K} \otimes_k \mathrm{End}_k(K)$$

Note that since $K \otimes_{\widetilde{K}} \widetilde{K} \cong K$, as extending scalars by nothing leaves the ring fixed, we have

$$\widetilde{K} \otimes_k K \otimes_k H \cong \widetilde{K} \otimes_k (K \otimes_{\widetilde{K}} \widetilde{K}) \otimes_k H \cong (\widetilde{K} \otimes_k K) \otimes_{\widetilde{K}} (\widetilde{K} \otimes_k H)$$

Now note that a k-basis for $\mathrm{End}_k(K)$ is given by

$$\{\rho_{ij} \mid i, j \in \{1, \ldots, n\}\}$$

where $\rho_{ij} : K \to K$ is defined by $\rho_{ij}(e_i) = e_j$ and $\rho_{ij}(e_l) = 0$ for all $l \neq i$. Given this k-basis, we have an $\widetilde{K}$-basis for $\widetilde{K} \otimes_k \mathrm{End}_k(K)$ given by

$$\{1_{\widetilde{K}} \otimes \rho_{ij} \mid i, j \in \{1, \ldots, n\}\}$$

as we did above. In particular, we have a map

$$\widetilde{K} \otimes_k \mathrm{End}_k(K) \to \mathrm{End}_{\widetilde{K}}(\widetilde{K} \otimes_k K)$$

$$\rho_{ij} \longmapsto 1_K \otimes \rho_{ij}$$

defined on a basis, giving us an isomorphism. In particular, the altered mapping $1 \otimes j$ above is actually simply the j map required in the definition of a Hopf-Galois extension, proving the claim. ∎

We are making great progress towards our goal. However, a question that might arise at this point is whether we can recover the original Hopf-Galois structure from the base changed version described above. The reason we are so interested in this is simply because in the proof of the Greither-Pareigis theorem we shall have to, in some sense, 'go up' and then 'go down' in order to prove the result.

The answer to the above question is in the positive. For the setup, take an H-Galois extension K/k base changed up via Theorem 4.16, so that we have the $(\widetilde{K} \otimes_k H)$-Galois extension $(\widetilde{K} \otimes_k K)/\widetilde{K}$. Note that the normal closure $\widetilde{K}$ of K is automatically Galois over k (separability carries up and we have normality from the normal closure) and so we may let $G = \mathrm{Gal}(\widetilde{K}/k)$. We have a clear action of G on $\widetilde{K} \otimes_k H$ given by the ordinary action on elements of $\widetilde{K}$ in the left factor, not touching H.

Now note that the fixed ring $(\widetilde{K} \otimes_k H)^G$ under this action of G on $\widetilde{K} \otimes_k H$ is a k-Hopf subalgebra of $\widetilde{K} \otimes_k H$, and

$$(\widetilde{K} \otimes_k H)^G = \widetilde{K}^G \otimes_k H = k \otimes_k H \cong H$$

and

$$(\widetilde{K} \otimes_k K)^G = \widetilde{K}^G \otimes_k K = k \otimes_k K \cong K$$

Thus we can accurately identify the fixed ring under the usual action of the Galois group G from $\widetilde{K}/k$ on $\widetilde{K} \otimes_k H$ by H, and from $\widetilde{K} \otimes_k K$ by K, in a sense returning to the original Hopf-Galois structure.

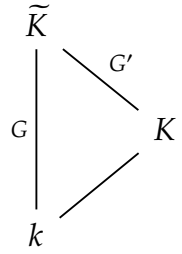
In this way, if we can classify all those base change Hopf-Galois structures, the $(\widetilde{K} \otimes_k H)$-Galois extensions $(\widetilde{K} \otimes_k)/\widetilde{K}$, then we can recover Hopf-Galois structures on the original H-Galois extension K/k.

4.4 The $\widetilde{K}$-algebras $\widetilde{K} \otimes_k H$ and Map$(G/G', \widetilde{K})$

We pick up where we left off in the previous section, our goal being to analyze in greater detail those $(\widetilde{K} \otimes_k H)$-Galois extensions $(\widetilde{K} \otimes_k K)/\widetilde{K}$, so that we might glean information from the H-Galois extensions K/k.

We begin by showing that $\widetilde{K} \otimes_k K$ is isomorphic as an $\widetilde{K}$-algebra to a strange object, which will prove indispensable in our eventual theory. To spoil the fun, we reveal this strange object.

Let K/k be a finite extension of fields and let $\widetilde{K}$ denote the normal closure of K. Then we have a diagram of fields



where $G = \text{Gal}(\widetilde{K}/k)$ and $G' = \text{Gal}(\widetilde{K}/K)$ are the Galois groups associated to the diagram. We consider the object

$$\text{Map}(G/G', \widetilde{K}) = \{f \mid f : G/G' \to \widetilde{K} \text{ a map of sets}\}$$

We are forced to work with set-maps since the set of cosets G/G' of G' in G is not necessarily a group, i.e., G' is not necessarily a normal subgroup of G, however $G' \subseteq G$ holds. Interestingly enough, $\text{Map}(G/G', \widetilde{K})$ can be made into a $\widetilde{K}$-algebra with multiplication

$$\nabla : \text{Map}(G/G', \widetilde{K}) \otimes \text{Map}(G/G', \widetilde{K}) \to \text{Map}(G/G', \widetilde{K})$$

$$\nabla(f \otimes g)(\alpha) = f(\alpha)g(\alpha)$$

and unit map

$$\eta : \widetilde{K} \to \text{Map}(G/G', \widetilde{K})$$

$$\eta(\beta)(\alpha) = \beta$$

for all $\beta \in \widetilde{K}$. These maps satisfy the associative and unit properties, and we can make $\text{Map}(G/G', \widetilde{K})$ into a $\widetilde{K}$-vector space using regular addition of set-maps and scalar multiplication given by usual multiplication in $\widetilde{K}$.

We also have a $\widetilde{K}$-basis

$$\{[e_{\overline{g}}] \mid \overline{g} \in G/G'\}$$

where $e_g : G/G' \to \widetilde{K}$ is defined by $e_g(\overline{g}) = \mathrm{id}_{\widetilde{K}}$ and $e_g(\overline{g'}) = 0$ for all $\overline{g'} \neq \overline{g}$. This fact is easily checked, and we leave it to the reader to verify the details.

In this new light, we have

$$\mathrm{Map}(G/G', \widetilde{K}) = \{ \sum_{\overline{g} \in G/G'} \alpha_g [e_g] \mid \alpha_g \in \widetilde{K} \}$$

with scalar multiplication by usual multiplication in the field $\widetilde{K}$.

With the above $\widetilde{K}$-algebra, we make a proposition.

Proposition 4.17. Let K/k be a separable extension of fields. Let $\widetilde{K}$ denote the normal closure of K. Write $G = \mathrm{Aut}(\widetilde{K}/k)$ and $G' = \mathrm{Aut}(\widetilde{K}/K)$. Then the map

$$\Phi : \widetilde{K} \otimes_k K \longrightarrow \mathrm{Map}(G/G', \widetilde{K})$$
$$\widetilde{\beta} \otimes \alpha \longmapsto \sum_{\overline{g} \in G/G'} \widetilde{\beta} g(\alpha) [e_{\overline{g}}]$$

defined for all $\widetilde{\beta} \in \widetilde{K}$ and $\alpha \in K$ is an isomorphism of $\widetilde{K}$-algebras.

Moreover, $\widetilde{K} \otimes_k K$ left G-module and $\mathrm{Map}(G/G', \widetilde{K})$ is a left G-module with action of G given by

$$\cdot : G \times \mathrm{Map}(G/G', \widetilde{K}) \to \mathrm{Map}(G/G', \widetilde{K})$$
$$h \cdot \sum_{\overline{g} \in G/G'} \alpha_g [e_g] = \sum_{\overline{g} \in G/G'} \alpha_g [e_{h^{-1}g}]$$

for all $h \in G$. We can also allow G to act by automorphisms and $\widetilde{K}$ to act by usual left multiplication on the first component of $\widetilde{K} \otimes_k K$, so that the map Φ above is also a G-module homomorphism, i.e., preserves the G-module structure.

Proof. By the primitive element theorem, we may write $K = k(\xi)$ for some element $\xi \in K$. Let $m_\xi(x) \in k[x]$ be the minimal polynomial of ξ over k. Since $\widetilde{K}/k$ is Galois, we have that $\{g(\xi) \mid \overline{g} \in G/G'\}$ is the set of roots of $m_\xi(x)$. Since $m_\xi(x)$ splits completely in the normal closure $\widetilde{K}$, we may employ the Chinese remainder theorem for rings; all in all, we get a sequence of isomorphisms

$$k(\xi) \cong k[x]/(m_\xi(x)) \cong k[x]/(\prod_{\overline{g} \in G/G'} (x - g(\xi))) \cong \prod_{\overline{g} \in G/G'} k[x]/(x - g(\xi))$$

Now we remark that by properties of the tensor product we have

$$\widetilde{K} \otimes_k K \cong \widetilde{K}[x]/(m_\xi(x)) \cong \prod_{\overline{g} \in G/G'} \widetilde{K}[x]/(x - g(\xi))$$

where the sequence of isomorphisms above takes elements as follows:

$$\beta \otimes p(x) \mapsto \beta p(x) \pmod{m_\xi(x)} \mapsto \beta \prod_{\overline{g} \in G} p(x) \pmod{(x - g(\xi))}$$

However, we can simplify what we have above. In particular, taking $x = g(\xi)$ for each $\overline{g} \in G/G'$ allows us to rewrite the above as follows:

$$\begin{aligned} \beta \prod_{\overline{g} \in G/G'} p(x) \pmod{(x - g(\xi))} &= \beta \prod_{\overline{g} \in G/G'} p(g(\xi)) \\ &= \beta \prod_{\overline{g} \in G/G'} g(p(\xi)) \\ &= \beta \prod_{\overline{g} \in G/G'} g(\alpha) \end{aligned}$$

Now we can define our final mapping Θ, which is given by

$$\Theta : \prod_{\overline{g} \in G/G'} \widetilde{K}[x]/(x - g(\xi)) \to \mathrm{Map}(G/G', \widetilde{K})$$

$$\beta \prod_{\overline{g} \in G/G'} g(\alpha) \mapsto \sum_{\overline{g} \in G/G'} \beta g(\alpha)[e_{\overline{g}}]$$

where of course the set $\{[e]_{\overline{g}} \mid \overline{g} \in G/G'\}$ is an $\widetilde{K}$-basis for $\mathrm{Map}(G/G', \widetilde{K})$ as an $\widetilde{K}$-vector space, and hence we take basis vectors of $\widetilde{K} \otimes_k K$ to those of $\mathrm{Map}(G/G', \widetilde{K})$, giving the $\widetilde{K}$-linear isomorphism.

Elements $\sigma \in G$ act by automorphisms on $\widetilde{K}$, and hence on the scalars in the $\widetilde{K}$-vector space $\mathrm{Map}(G/G', \widetilde{K})$. Furthermore, G acts on the left on $\widetilde{K} \otimes_k K$ by $\sigma(\widetilde{\beta} \otimes \alpha) = \sigma(\widetilde{\beta}) \otimes \alpha$ for all $\widetilde{\beta} \in \widetilde{K}$ and $\alpha \in K$; hence both $\widetilde{K} \otimes_k K$ and $\mathrm{Map}(G/G', \widetilde{K})$ are left G-modules. Note that for any $\sigma \in G$, we have

$$\begin{aligned} \Phi(\sigma(\widetilde{\beta} \otimes \alpha))) &= \Phi(\sigma(\widetilde{\beta}) \otimes \alpha) \\ &= \sum_{\overline{g} \in G/G'} \sigma(\widetilde{\beta}) g(\alpha)[e_{\overline{g}}] \\ &= \sum_{\overline{g} \in G/G'} \sigma(\widetilde{\beta}) \sigma(\sigma^{-1} g(\alpha))[e_{\overline{g}}] \\ &= \sigma\left(\sum_{\overline{g} \in G/G'} \widetilde{\beta}(\sigma^{-1} g)(\alpha)[e_{\overline{g}}] \right) \\ &= \sum_{\overline{g} \in G/G'} \widetilde{\beta} g(\alpha)[e_{\overline{\sigma g}}] \\ &= \sigma(\Phi(\widetilde{\beta} \otimes \alpha)) \end{aligned}$$

where we have used the left action of G on $\mathrm{Map}(G/G', \widetilde{K})$ to arrive at the final few inequalities, as defined in the statement of the proposition. ■

A lot happened there, but the heart of the matter is that we have successfully identified the $\widetilde{K}$-algebra $\widetilde{K} \otimes_k K$ with $\mathrm{Map}(G/G', \widetilde{K})$. Since, as we mentioned previously, a primary concern of ours is classifying those $(\widetilde{K} \otimes_k H)$-Galois extensions $(\widetilde{K} \otimes_k K)/\widetilde{K}$, we can now investigate the extension $\mathrm{Map}(G/G', \widetilde{K})/\widetilde{K}$ instead to acquire the same information.

While it might seem like $\mathrm{Map}(G/G', \widetilde{K})$ is a much harder object to work with than $\widetilde{K} \otimes_k K$, we have some very nice properties that will push us forward.

As a first step in this direction, we discuss the action of $G = \mathrm{Gal}(\widetilde{K}/k)$ on a $\widetilde{K}$-basis for $\mathrm{Map}(G/G', \widetilde{K})$. Note that from the proof above we have for all $\tau \in G$, an action

$$\tau \cdot [e_{\overline{\sigma}}] = [e_{\overline{\tau\sigma}}]$$

where $\{[e_{\overline{\sigma}} \mid \overline{\sigma} \in G/G'\}$ is the $\widetilde{K}$-basis. We can even define a map

$$\lambda : G \to \mathrm{Perm}(G/G')$$

$$\lambda(\tau)(\overline{\sigma}) = \overline{\tau\sigma}$$

and note that this is simply the left translation map of G on G/G'.

We cover a few lemmas.

Lemma 4.18. Let K/k be an H-Galois extension of fields and let $\widetilde{K}$ denote the normal closure of K. Let $G = \mathrm{Gal}(\widetilde{K}/k)$ and $G' = \mathrm{Gal}(\widetilde{K}/K)$. If $\mathrm{Map}(G/G', \widetilde{K})/\widetilde{K}$ is a $(\widetilde{K} \otimes_k H)$-Galois extension, then there is an isomorphism of $\widetilde{K}$-algebras

$$\bigoplus_{i=1}^{[\widetilde{K}:k]^2} \widetilde{K} \cong \bigoplus_{i=1}^{[\widetilde{K}:k]} (\widetilde{\otimes}_k H^*)$$

where $H^* = \mathrm{Hom}_{\widetilde{K}}(H, \widetilde{K})$ is the dual k-Hopf algebra.

Proof. We have immediately that

$$\mathrm{Map}(G/G', \widetilde{K}) \cong \bigoplus_{i=1}^{[\widetilde{K}:k]} \widetilde{K}$$

for instance by noting that multiplication in the $\widetilde{K}$-algebra $\mathrm{Map}(G/G', \widetilde{K})$ is componentwise, for instance via the mapping

$$\sum_{\overline{g}\in G/G'} \alpha_g[e_{\overline{g}}] \longmapsto (\alpha_g)_{\overline{g}\in G/G'}$$

which is an isomorphism of $\widetilde{K}$-algebras. Using exactly the same process we can deduce that

$$\mathrm{Map}(G/G' \times G/G', \widetilde{K}) \cong \bigoplus_{i=1}^{[\widetilde{K}:k]^2} \widetilde{K}$$

Now we note that, since $\widetilde{K} \otimes_{\widetilde{K}} \widetilde{K} \cong \widetilde{K}$, we may write

$$\begin{aligned}
\mathrm{Map}(G/G' \times G/G', \widetilde{K}) &\cong \bigoplus_{i=1}^{[\widetilde{K}:k]^2} (\widetilde{K} \otimes_{\widetilde{K}} \widetilde{K}) \\
&\cong \left(\bigoplus_{i=1}^{[\widetilde{K}:k]} \widetilde{K}\right) \otimes_{\widetilde{K}} \left(\bigoplus_{i=1}^{[\widetilde{K}:k]} \widetilde{K}\right) \\
&\cong \mathrm{Map}(G/G', \widetilde{K}) \otimes_{\widetilde{K}} \mathrm{Map}(G/G', \widetilde{K})
\end{aligned}$$

Now by assumption we have $\mathrm{Map}(G/G', \widetilde{K})/\widetilde{K}$ an $(\widetilde{K} \otimes_k H)$-Galois extension, and hence by definition we have an isomorphism of $\widetilde{K}$-algebras

$$j : \mathrm{Map}(G/G', \widetilde{K}) \otimes_{\widetilde{K}} (\widetilde{K} \otimes_k H) \to \mathrm{End}_{\widetilde{K}}(\mathrm{Map}(G/G', \widetilde{K}))$$

Which, by Proposition 3.17, gives us a $\widetilde{K}$-linear isomorphism

$$\gamma : \mathrm{Map}(G/G', \widetilde{K}) \otimes_{\widetilde{K}} \mathrm{Map}(G/G', \widetilde{K}) \to \mathrm{Map}(G/G', \widetilde{K}) \otimes_{\widetilde{K}} H^*$$

which by the same proposition is an isomorphism of $\widetilde{K}$-algebras.

Now we have the isomorphism from our initial observation above, where we use the fact that $\oplus$ distributes over $\otimes_{\widetilde{K}}$ as follows:

$$\begin{aligned}
\mathrm{Map}(G/G', \widetilde{K}) \otimes_{\widetilde{K}} (\widetilde{K} \otimes_k H)^* &\cong \left(\bigoplus_{i=1}^{[\widetilde{K}:k]} \widetilde{K}\right) \otimes_{\widetilde{K}} H^* \\
&\cong \bigoplus_{i=1}^{[\widetilde{K}:k]} (\widetilde{K} \otimes_{\widetilde{K}} H^*) \\
&\cong \bigoplus_{i=1}^{[\widetilde{K}:k]} H^*
\end{aligned}$$

Putting together all the pieces above, we recover the desired isomorphism in the lemma. ∎

We now can say more using the above lemma.

Corollary 4.19. With the notation as in Lemma 4.18, there is an isomorphism of $\widetilde{K}$-algebras

$$(\widetilde{K} \otimes_k H)^* \cong \bigoplus_{i=1}^{[\widetilde{K}:k]} \widetilde{K}$$

where as usual $(\widetilde{K} \otimes_k H)^*$ denotes the dual $\widetilde{K}$-algebra of $\widetilde{K} \otimes_k H$.

Proof. The proof of the corollary follows immediately from the general theory of semisimple rings combined with the results of Lemma 4.18 above. All that needs to be said is that the field $\widetilde{K}$ is a simple $\widetilde{K}$-module, and hence $(\widetilde{K} \otimes_k H)^*$ is a semisimple module. The rest follows. ∎

We finally have all the tools we need to dig into the Hopf-Galois structure of this mystical $(\widetilde{K} \otimes_k H)$-Galois extension of fields $\mathrm{Map}(G/G', \widetilde{K})/\widetilde{K}$. We do so with vigor and gusto, as we are fast approaching our goal of classifying the Hopf-Galois structure on the H-Galois extension K/k.

Theorem 4.20. Let K/k be an H-Galois extension of fields and let $\widetilde{K}$ denote the normal closure of K. Let $G = \mathrm{Gal}(\widetilde{K}/k)$ and $G' = \mathrm{Gal}(\widetilde{K}/K)$. If $\mathrm{Map}(G/G', \widetilde{K})/\widetilde{K}$ is a $(\widetilde{K} \otimes_k H)$-Galois extension, then

$$\widetilde{K} \otimes_k H \cong \widetilde{K}[N]$$

for some group N which may be identified as a regular (that is, transitive and fixed-point free) subgroup of $\mathrm{Perm}(G/G')$.

Conversely, if N is a regular subgroup of $\mathrm{Perm}(G/G')$, then the extension of fields $\mathrm{Map}(G/G', \widetilde{K})/\widetilde{K}$ is a $\widetilde{K}[N]$-Galois extension.

Proof. Suppose $\mathrm{Map}(G/G', \widetilde{K})$ is $(\widetilde{K} \otimes_k H)$-Galois. By Corollary 4.19 we have an isomorphism of $\widetilde{K}$-algebras, where for convenience we let $[\widetilde{K} : k] = n$.

$$(\widetilde{K} \otimes_k H)^* \cong \bigoplus_{i=1}^{n} \widetilde{K}$$

Define a collection of functions

$$n_i : (\widetilde{K} \otimes_k H)^* \to \widetilde{K}$$

$$(x_1, \ldots, x_n) \longmapsto x_i$$

for each $i \in \{1, \ldots, n\}$, and let $N = \{n_i \mid i \in \{1, \ldots, n\}\}$. These are simply projection maps, and we leave the verification that N forms a $\widetilde{K}$-basis for $\mathrm{Hom}_{(\widetilde{K}}((\widetilde{K} \otimes_k H)^*, \widetilde{K})$ as a $\widetilde{K}$-vector space to the reader. One notes that

$$\mathrm{Hom}_{\widetilde{K}}((\widetilde{K} \otimes_k H)^*, \widetilde{K}) = ((\widetilde{K} \otimes_k H)^*)^* \cong \widetilde{K} \otimes_k H$$

where the last isomorphism above follows since $\widetilde{K} \otimes_k H$ is a finite dimensional $\widetilde{K}$-vector space. Since each of the n_i are easily seen to be $\widetilde{K}$-algebra isomorphisms, and hence by Proposition 2.25, each n_i is a grouplike element of $\widetilde{K} \otimes_k H$. Since the grouplikes of a Hopf algebra form linearly independent subsets, see Proposition 2.23, and N is a $\widetilde{K}$-basis, N is a maximal linearly independent subset, hence $G(\widetilde{K} \otimes_k H) = N$, the grouplikes are exactly N. Now, since the grouplikes form a group, N is a group; hence

$$\widetilde{K} \otimes_k H = \widetilde{K}[N] = \{\sum_{i=1}^{m} \alpha_i [n_i] \mid \alpha_i \in \widetilde{K}\}$$

But how do we make N act on G/G' as we desire?

Since $\mathrm{Map}(G/G', \widetilde{K})/\widetilde{K}$ is $(\widetilde{K} \otimes_k H)$-Galois by assumption, we know immediately that $\mathrm{Map}(G/G', \widetilde{K})/\widetilde{K})$ is $\widetilde{K}[N]$-Galois. Thus there is a Hopf action

$$\widetilde{K}[N] \times \mathrm{Map}(G/G', \widetilde{K}) \to \mathrm{Map}(G/G', \widetilde{K})$$

which we may restrict to $N \subseteq \widetilde{K}[N]$ and to the $\widetilde{K}$-basis $\{[e_{\overline{g}}] \mid \overline{g} \in G/G'\}$ to get

$$N \times G/G' \to G/G'$$

$$(n_i, [e_{\overline{g}}]) \longmapsto [e_{\overline{h}}]$$

for some $\overline{h} \in G/G'$. In fact, we can view the above scenario as an action of n_i on the coordinate, i.e.,

$$(n_i, [e_{\overline{g}}]) \longmapsto [e_{n_i(\overline{g})}]$$

where $n_i(\overline{g}) = \overline{h}$. In particular, N acts by permuting the elements of G/G', hence N is a subgroup of $\mathrm{Perm}(G/G')$.

Before we get too carried away with our progress, we must prove that such a restriction to $N \times G/G' \to X$ is possible. Since $\mathrm{Map}(G/G', \widetilde{K})/\widetilde{K}$ is a $\widetilde{K}[N]$-Galois extension, in particular we have that $\mathrm{Map}(G/G', \widetilde{K})$ is a left $\widetilde{K}[N]$-module $\widetilde{K}$-algebra, and hence that

$$n([e_{\overline{g}}]) = n([e_{\overline{g}} e_{\overline{g}}]) = n \cdot [e_{\overline{g}} e_{\overline{g}}] = \Delta(n)([e_{\overline{g}}] \otimes [e_{\overline{g}}]) = n([e_{\overline{g}}]) n([e_{\overline{g}}])$$

since $\Delta(n) = n \otimes n$, as n is a grouplike element. We also clearly have

$$n([e_{\overline{g}}e_{\overline{h}}]) = n([e_{\overline{g}}])n([e_{\overline{h}}]) = 0$$

for all $\overline{g} \neq \overline{h}$ in G/G' by construction of these basis elements. Lastly, we have

$$1 \cdot [e_{\overline{g}}] = n^{-1}n \cdot [e_{\overline{g}}] = n^{-1} \cdot n([e_{\overline{g}}]) = [e_{\overline{g}}]$$

and hence $n([e_{\overline{g}}]) \neq 0$ for all $n \in N$ and $\overline{g} \in G/G'$. Further, since n is a grouplike,

$$\eta([e_{\overline{1_G}}]) = \varepsilon(n) = [e_{\overline{1_G}}]$$

We may make the observation that

$$\sum_{\overline{g} \in G/G'} [e_{\overline{g}}] = [e_{\overline{1_G}}]$$

in $\mathrm{Map}(G/G', \widetilde{K})$, and hence that

$$[e_{\overline{1_G}}] = n([e_{\overline{1_G}}]) = n\left(\sum_{\overline{g} \in G/G'} [e_{\overline{g}}]\right) = \sum_{\overline{g} \in G/G'} n([e_{\overline{g}}])$$

In this way, each map $n([e_{\overline{g}}])$ is the sum of primitive idempotents in $\mathrm{Map}(G/G', \widetilde{K})$, and by the facts mentioned above, each primitive idempotent can occur exactly once in this sum, and so $n([e_{\overline{g}}])$ is the sum of $|G/G'|$ distinct terms. In particular, this suffices to show that $n([e_{\overline{g}}]) = [e_{\overline{h}}]$ implies $[e_{n(\overline{g})}] = [e_{\overline{h}}]$, so that $n(\overline{g}) = \overline{h}$. This gives us that restriction mentioned earlier, and hence we have an embeddding $N \to \mathrm{Perm}(G/G')$ as a subgroup.

What remains is to show that N is a regular subgroup of $\mathrm{Perm}(G/G')$. Note that $|N| = |G/G'|$. Assume, for contradiction, that N is not transitive as a subgroup. Define

$$N[e_{\overline{g}}] = \{[e_{\overline{h}}] \mid \overline{h} \in X \subset G/G'\}$$

Choose $\overline{w} \in (G/G') \setminus X$, and define a mapping

$$f_{\overline{gw}} : \mathrm{Map}(G/G', \widetilde{K}) \to \mathrm{Map}(G/G', \widetilde{K})$$

$$f_{\overline{gw}}([e_{\overline{g}}]) = [e_{\overline{g}}]$$

$$f_{\overline{gw}}([e_{\overline{h}}]) = 0$$

for all $\overline{h} \neq \overline{g}$. One immediately observes that $f_{\overline{gw}}$ is $\widetilde{K}$-linear.

We have $\mathrm{Map}(G/G', \widetilde{K})$ is $\widetilde{K}[N]$-Galois over $\widetilde{K}$. Thus

$$j : \mathrm{Map}(G/G', \widetilde{K}) \otimes_{\widetilde{K}} \widetilde{K}[N] \to \mathrm{End}_{\widetilde{K}}(\mathrm{Map}(G/G', \widetilde{K}))$$

is a $\widetilde{K}$-linear isomorphism. We claim that the map $f_{\overline{gw}}$ constructed above is not in the image of j, so that j would not be surjective. Indeed, we have a $\widetilde{K}$-basis

$$\{n_i \otimes [e_{\overline{g}}] \mid \overline{g} \in G/G',\ i \in \{1, \ldots, n\}\}$$

for $\mathrm{Map}(G/G', \widetilde{K}) \otimes_{\widetilde{K}} \widetilde{K}[N]$, so that any $\xi \in \mathrm{Map}(G/G', \widetilde{K}) \otimes_{\widetilde{K}} \widetilde{K}[N]$ has

$$\xi = \sum_{n_i \in N} \sum_{\overline{g} \in G/G'} \alpha_{\overline{g},i}([e_{\overline{g}}] \otimes n_i)$$

Therefore we may write that

$$\begin{aligned} j\left(\sum_{n_i \in N} \sum_{\overline{g} \in G/G'} \alpha_{\overline{g},i}([e_{\overline{g}}] \otimes n_i)\right)([e_{\overline{h}}]) &= \sum_{n_i \in N} \sum_{\overline{g} \in G/G'} \alpha_{\overline{g},i} j([e_{\overline{g}}] \otimes n_i)([e_{\overline{h}}]) \\ &= \sum_{n_i \in N} \sum_{\overline{g} \in G/G'} \alpha_{\overline{g},i}[e_{\overline{g}}] n_i([e_{\overline{h}}]) \\ &= \sum_{n_i \in N} \alpha_{\overline{w},i}[e_{\overline{w}}] \end{aligned}$$

Where the final equality follows since for fixed $\overline{h} \in G/G'$, there exists $\overline{w} \in G/G'$ such that $n([e_{\overline{g}}]) = [e_{\overline{w}}]$, and since the elements are pairwise orthogonal, we have $[e_{\overline{g}}]n_i([e_{\overline{h}}] = 0$ if $\overline{g} \neq \overline{h}$ and $[e_{\overline{h}}]$ otherwise. Note that the element

$$\sum_{n_i \in N} \alpha_{\overline{w},i}[e_{\overline{w}}] \in N[e_{\overline{g}}]$$

however $[e_{\overline{g}}]$ is not contained in $N[e_{\overline{g}}]$, hence a contradiction, so that we require N to be transitive. The transitivity condition and the fact that $|N| = |G/G'|$ give us that N is a regular subgroup of $\mathrm{Perm}(G/G')$, as desired.

Now we prove the converse to the theorem. So suppose N is a regular subgroup of $\mathrm{Perm}(G/G')$. We prove that $\mathrm{Map}(G/G', \widetilde{K})/\widetilde{K}$ is $\widetilde{K}[N]$-Galois. We begin with a Hopf action. We know that N acts on G/G' and on $[e_{\overline{g}}]$ via indices. Define

$$\mu : \widetilde{K}[N] \times \mathrm{Map}(G/G', \widetilde{K}) \to \mathrm{Map}(G/G', \widetilde{K})$$

$$(n, [e_{\overline{g}}]) \longmapsto n([e_{\overline{g}}]) = [e_{n(\overline{g})}]$$

on a $\widetilde{K}$-basis, which extends by linearity to the whole algebra. Now we check that the j map is an isomorphism. We have

$$\dim_{\widetilde{K}}(\mathrm{Map}(G/G', \widetilde{K})) = \dim_{\widetilde{K}}(\widetilde{K}^{|G/G'|}) = |G/G'|$$

Now since N is regular, $|N| = |G/G'|$, and hence

$$\dim_{\widetilde{K}}(\widetilde{K}[N]) = |N| = |G/G'|$$

and thus we have

$$\dim_{\widetilde{K}}(\mathrm{Map}(G/G', \widetilde{K}) \otimes_{\widetilde{K}} \widetilde{K}[N]) = |G/G'|^2$$

which we recall is precisely the dimension of $\mathrm{End}_{\widetilde{K}}(\mathrm{Map}(G/G', \widetilde{K}))$ as a $\widetilde{K}$-vector space. Surjectivity is easy enough to check, which gives the isomorphism.

Lastly, it is easy to check that the Hopf action μ defined above gives $\mathrm{Map}(G/G', \widetilde{K})$ the structure of a left $\widetilde{K}[N]$-module $\widetilde{K}$-algebra, sufficing to prove that $\mathrm{Map}(G/G', \widetilde{K})/\widetilde{K}$ is a $\widetilde{K}[N]$-Galois extension, which was the desired result. ■

The road was long and hard, but we have finally done it. We have successfully investigated the Hopf-Galois structure of those extensions of the form $\mathrm{Map}(G/G', \widetilde{K})/\widetilde{K}$, and showed that the Hopf-Galois structures $\widetilde{K}[N], \cdot)$ are in bijective correspondence with regular subgroups N of the group $\mathrm{Perm}(G/G')$.

The question now becomes: how do we translate these results 'down' into the original extension K/k? In particular, how can we adapt what we have gleaned from these base changed Hopf-Galois extensions to the original Hopf-Galois extensions.

4.5 K-Forms and Galois Descent

As hinted at in the preivous section, we concern ourselves with the reverse process associated to base change. We have shown how a finite separable extension of fields K/k with a Hopf-Galois structure given by a k-Hopf algebra H gives rise (via base change) to a $(\widetilde{K} \otimes_k H)$-Galois extension $(\widetilde{K} \otimes_k K)/\widetilde{K}$, which by Proposition 4.16 is isomorphic to $\mathrm{Map}(G/G', \widetilde{K})/\widetilde{K}$. In the last section we proved an extremely useful bijection which, in some sense, completely identifies the Hopf-Galois structures which can be placed on $\mathrm{Map}(G/G', \widetilde{K})/\widetilde{K}$, and so also on the isomorphic $(\widetilde{K} \otimes_k K)/\widetilde{K}$. Now we would like to go down, bringing these nice results back to K/k. The technique we shall employ to do this is that of Galois descent, which we now develop.

Galois descent can roughly be understood as when (and how) an $\widetilde{K}$-isomorphism descends to K. We shall make this precise after introducing some preliminary terminology and machinery.

Recall the following definition, which we include here for completeness, despite having used the concept in previous sections.

Definition 4.21. Let G be a group. A *left G-module* is an abelian group M together with an action $G \times M \to M$ defined by $(g, m) \mapsto g \cdot m$ for all $g \in G$ and $m \in M$, which satisfies

$$g \cdot (m + n) = g \cdot m + g \cdot n$$

for all $g \in G$ and $m, n \in M$. Equivalently, we may think of M as a left $\mathbb{Z}[G]$-module in the usual sense.

Definition 4.22. Let G be a group and M a left G-module. A 1-*cocycle of G into M* is a map $\rho : G \to A$ defined by $\rho(g) = \rho_g$ for all $g \in G$, which satisfies

$$\rho_{gh} = \rho_g(g \cdot \rho_h)$$

for all $g, h \in G$. By convention, we let $Z^1(G, M)$ denote the set of all 1-cocycles of G into M.

Definition 4.23. Let G be a group and M a left G-module. On the set $Z^1(G, M)$, consider the equivalence relation $\sim$ defined by $\rho \sim \mu$ if and only if there exists $m \in M$ such that

$$\mu_m = m^{-1}\rho_g(g \cdot m)$$

We define the *first cohomology set of G in A* as the quotient

$$H^1(G, M) = Z^1(G, M)/\sim$$

We explore a particular scenario of the above which applies directly to our development.

Let K/k be a finite Galois extension of fields with Galois group $G = \mathrm{Gal}(K/k)$. In this way, elements of G naturally act on elements of the field K. Now let A be a k-algebra. We have a natural action

$$G \times K \otimes A \to K \otimes A$$

$$(g, \beta \otimes a) \mapsto g \cdot \beta \otimes a$$

for all $g \in G$, $\beta \in K$, and $a \in A$.

More generally, let A and B be k-algebras, and suppose $\psi : A \to B$ is a k-algebra homomorphism. For convenience, denote the action of $g \in G$ on $K \otimes A$ and $K \otimes B$ by simply g. Then we have a diagram

$$\begin{array}{ccc} K \otimes A & \xrightarrow{\psi} & K \otimes B \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g} \\ K \otimes A & \xrightarrow{g \circ \psi \circ g^{-1}} & K \otimes B \end{array}$$

which commutes.

Definition 4.24. Let K/k be a finite Galois extension of fields, and let A be a k-algebra. We say that a k-algebra B is a *K-form* of A if there exists a K-linear isomorphism $K \otimes A \cong K \otimes B$.

Theorem 4.25. Let K/k be a finite Galois extension, and let A be an K-form. The set of K-$\mathrm{Form}(A)$ of K-forms of A is in bijective correspondence with the first cohomology set of G in $\mathrm{Aut}_K(K \otimes A)$; K-$\mathrm{Form}(A) \cong H^1(G, \mathrm{Aut}_K(K \otimes A))$.

Proof. Let B be a K-form of A. Then there exists an K-linear isomorphism $\varphi : K \otimes A \to K \otimes B$. While we do not explain all the details, for sake of brevity, we exhibit the actual bijection (the details can be checked). The bijection is given by

$$B \longleftrightarrow (g \mapsto \rho_g = \varphi \circ g \circ \varphi \circ g^{-1})$$

for all $g \in G$. ∎

Now we cover more generally the theory of Galois descent as it applies to our specific use-case.

Definition 4.26. Let K/k be a finite Galois extension and let A_1, A_2, B_1, B_2 be k-algebras. Suppose B_1 is a K-form of A_1 and that B_2 is a K-form of A_2, with K-linear isomorphisms $\varphi_1 : K \otimes B_1 \to K \otimes A_1$ and $\varphi_2 : K \otimes B_2 \to K \otimes A_2$, respectively. If $f : K \otimes A_1 \to K \otimes A_2$ is an K-linear map, then we call f *descendable* if there exist an K-linear map g such that the diagram

$$\begin{array}{ccc} K \otimes A_1 & \xrightarrow{\quad f \quad} & K \otimes A_2 \\ \uparrow{\scriptstyle \varphi_1} & & \uparrow{\scriptstyle \varphi_2} \\ K \otimes B_1 & \xrightarrow{\quad \mathrm{id}_K \otimes g \quad} & K \otimes B_2 \end{array}$$

commutes. In other words, we have

$$(f \circ \varphi_1)(\beta \otimes b) = (\varphi_2 \circ (\mathrm{id}_K \otimes g))(\beta \otimes b)$$

for all $b \in B_1$ and $\beta \in K$.

Armed with the above definition, we tackle the lemma.

Lemma 4.27. Let $p^{(1)}$ be the 1-cocycle associated to B_1, and let $p^{(2)}$ be the 1-cocycle associated to B_2. Then a morphism $f : K \otimes A_1 \to K \otimes A_2$ is descendable if and only if

$$f \circ p^{(1)}_\sigma = p^{(2)}_\sigma \circ \sigma \circ f \circ \sigma^{-1}$$

for all $\sigma \in G$.

Proof. Assume that f is descendable. Then there exists a morphism $g : K \otimes B_1 \to K \otimes B_2$ such that

$$f \circ \varphi_1 = \varphi_2 \circ g = \varphi_2 \circ (\mathrm{id}_K \otimes g)$$

for all $\beta \in K$ and $b \in B_1$; hence applying the inverse of the K-linear isomorphism φ_2 to the left of both sides of the above yields

$$\varphi_2^{-1} \circ f \circ \varphi_1 = \varphi_2^{-1} \circ \varphi_2 \circ (\mathrm{id}_K \otimes g) = \mathrm{id}_K \otimes g$$

Now let $\sigma \in G$ be arbitrary. We know that, since G is the Galois group of K/k, that σ acts on elements of K. Thus we have

$$\begin{aligned} (\sigma \circ (\mathrm{id}_K \otimes g))(\beta \otimes b) &= \sigma(\beta \otimes g \cdot b) \\ &= \sigma(\beta) \otimes g \cdot b \\ &= (\mathrm{id}_L \otimes g)(\sigma(\beta) \otimes b) \\ &= ((\mathrm{id}_L \otimes g) \circ \sigma)(\beta \otimes b) \end{aligned}$$

for all $b \in B_1$ and $\beta \in K$. With this fact in mind, and since above we showed

$$\varphi_2^{-1} \circ f \circ \varphi_1 = \mathrm{id}_K \otimes g$$

we may note that for all $\sigma \in G$ we have

$$\sigma \circ \varphi_2^{-1} \circ f \circ \varphi_1 = \varphi_2^{-1} \circ f \circ \varphi_1 \circ \sigma$$

We are nearly there. Applying the K-linear map φ_2 to the left of both sides of the above equation yields

$$\varphi_2 \circ \sigma \circ \varphi_2^{-1} \circ f \circ \varphi_1 = f \circ \varphi_1 \circ \sigma$$

Once more, apply the inverse of φ_1 (which exists since φ_1 is an K-linear isomorphism) to the above eqaution on the right yields

$$\varphi_2 \circ \sigma \circ \varphi_2^{-1} \circ f = f \circ \varphi_1 \circ \sigma \circ \varphi_1^{-1}$$

Finally, apply the inverse of σ to the right of both sides above, and so obtain

$$\varphi_2 \circ \sigma \circ \varphi_2^{-1} \circ f \circ \sigma^{-1} = f \circ \varphi_1 \circ \sigma \circ \varphi_1^{-1} \circ \sigma^{-1}$$

which is equivalent to

$$(\varphi_2 \circ \sigma \circ \varphi_2^{-1} \circ \sigma^{-1}) \circ \sigma \circ f \circ \sigma^{-1} = f \circ (\varphi_1 \circ \sigma \circ \varphi_1^{-1} \circ \sigma^{-1})$$

Now note that $\varphi_2 \circ \sigma \circ \varphi_2^{-1} \circ \sigma^{-1} = p_\sigma^{(2)}$ and $\varphi_1 \circ \sigma \circ \varphi^{-1} \circ \sigma^{-1} = p_\sigma^{(1)}$, and hence we retrieve the equality

$$p_\sigma^{(2)} \circ \sigma \circ f \circ \sigma^{-1} = f \circ p_\sigma^{(1)}$$

which proves the first implication. For the converse, assume $f \circ p_\sigma^{(1)} = p_\sigma^{(2)} \circ \sigma \circ f \circ \sigma^{-1}$ holds for all $\sigma \in G$. Define a map

$$\mathcal{G} = \varphi_2^{-1} \circ f \circ \varphi_1 : K \otimes B_1 \to K \otimes B_2$$

$$\beta \otimes b \mapsto (\varphi_2^{-1} \circ f \circ \varphi_1)(\beta \otimes b)$$

for all $\beta \otimes b \in L \otimes B_1$. In the proof of the first direction above, we showed that the element σ commutes with $\mathcal{G}$ as defined above, so that $\sigma \circ \mathcal{G} = \mathcal{G} \circ \sigma$. In particular, if $\beta \in K$ is invariant under σ, then we have $\sigma(\beta) = \beta$, and hence require

$$\sigma(\mathcal{G})(\beta \otimes b)) = (\mathcal{G} \circ \sigma)(\beta \otimes b) = \mathcal{G}(\sigma(\beta) \otimes b) = \mathcal{G}(\beta \otimes b)$$

In particular, $\mathcal{G}(\beta \otimes b)$ is also invariant under σ for all $\sigma \in G$. However, since G is the Galois group of K/k, we know that the only elements invariant under all $\sigma \in G$ is precisely the base field k. In particular, we may restrict $\mathcal{G}$ as follows:

$$\mathcal{G}|_{k\otimes B_1} : k \otimes B_1 \to k \otimes B_2$$

and since we have the canonical isomorphisms $k \otimes B_1 \cong B_1$ and $k \otimes B_2 \cong B_2$, we may let $g = \mathcal{G}|_{k\otimes B_1}$ be the desired map in the definition of a descendable morphism. ■

We apply this work to the next section; it will have tremendous benefits for our theory.

4.6 Greither and Pareigis' Theorem

We are finally in a position to prove Greither and Pareigis' theorem for completely characterizing Hopf-Galois structures on separable field extensions.

We build up the theorem slowly, breaking it into two parts so as to better understand and appreciate precisely what is going on beneath the hood. The first direction is the theorem below.

Theorem 4.28. Let K/k be an H-Galois extension with Hopf action $h \cdot \alpha$ for $\alpha \in K$ and $h \in H$, and let $\widetilde{K}$ denote the normal closure of K. Let $G = \mathrm{Gal}(\widetilde{K}/k)$ and $G' = \mathrm{Gal}(\widetilde{K}/K)$. Then the Hopf action of $\widetilde{K} \otimes_k H$ on $\widetilde{K} \otimes_k K$ obtained by base change

$$\Phi : (\widetilde{K} \otimes_k H) \otimes_{\widetilde{K}} (\widetilde{K} \otimes_k K) \to \widetilde{K} \otimes_k K$$
$$(\widetilde{\beta} \otimes h) \otimes (\widetilde{\gamma} \otimes \alpha) \longmapsto (\widetilde{\beta}\widetilde{\gamma}) \otimes (h \cdot \alpha)$$

is equivalent to a Hopf action

$$\Psi : \widetilde{K}[N] \otimes_{\widetilde{K}} \mathrm{Map}(G/G', \widetilde{K}) \to \mathrm{Map}(G/G', \widetilde{K})$$

making $\mathrm{Map}(G/G', \widetilde{K})/\widetilde{K}$ a $\widetilde{K}[N]$-Galois extension, which corresponds to a regular subgroup N of order $|G/G'|$ in $\mathrm{Perm}(G/G')$ such that if $\lambda : G \to \mathrm{Perm}(G/G')$ is the left translation map, then $\lambda(G)$ normalizes the image of N in $\mathrm{Perm}(G/G')$.

Proof. Given our assumption that K/k is a finite extension, from Proposition 4.16 we have that $\mathrm{Map}(G/G', \widetilde{K})/\widetilde{K}$ is a $(\widetilde{K} \otimes_k H)$-Galois extension. Take a $\widetilde{K}$-basis $X = \{[e_{\overline{g}}] \mid \overline{g} \in G/G'\}$ for $\mathrm{Map}(G/G', \widetilde{K})$. From Proposition 4.17 we have a G-module isomorphism

$$\Phi : \widetilde{K} \otimes_k K \longrightarrow \mathrm{Map}(G/G', \widetilde{K})$$
$$\widetilde{\beta} \otimes \alpha \longmapsto \sum_{\overline{g} \in G/G'} \widetilde{\beta} g(\alpha)[e_{\overline{g}}]$$

In particular, G acts on X by

$$G \times X \to X$$
$$(\sigma, [e_{\overline{g}}]) \longmapsto [e_{\overline{\sigma g}}]$$

as we saw in the discussion preceding Lemma 4.18. Note that

$$(\sigma, [e_{\overline{g}}]) \longmapsto [e_{\overline{\sigma g}}] = [e_{\lambda(\sigma)(\overline{g})}]$$

where $\lambda : G \to \mathrm{Perm}(G/G')$ is the left translation map. Put this aside for now. From Theorem 4.20, we are given that

$$\widetilde{K} \otimes_k H \cong \widetilde{K}[N]$$

for some regular subgroup N of $\mathrm{Perm}(G/G')$. As we saw in the proof of the same theorem, N acts on X by

$$N \times X \to X$$

$$(n, [e_{\overline{g}}]) \longmapsto n([e_{\overline{g}}]) = [e_{n(\overline{g})}]$$

We have the following picture:

$$\begin{array}{ccc} (\widetilde{K} \otimes_k H) \otimes_{\widetilde{K}} (\widetilde{K} \otimes_k K) & \xrightarrow{\Phi} & \widetilde{K} \otimes_k K \\ \downarrow \cong & & \downarrow \cong \\ \widetilde{K}[N] \otimes_{\widetilde{K}} \mathrm{Map}(G/G', \widetilde{K}) & \xrightarrow{\Psi} & \mathrm{Map}(G/G', \widetilde{K}) \end{array}$$

In this way, the action Φ becomes equivalent to an action

$$\Psi : \widetilde{K}[N] \otimes_{\widetilde{K}} \mathrm{Map}(G/G', \widetilde{K}) \to \mathrm{Map}(G/G', \widetilde{K})$$

$$n \otimes [e_{\overline{g}}] \longmapsto n([e_{\overline{g}}]) = [e_{n(\overline{g})}]$$

What remains is to check that $\lambda(G)$ normalizes the image of N in $\mathrm{Perm}(G/G')$. First we check that G actually acts on N. We have the obvious action of $G = \mathrm{Gal}(\widetilde{K}/k)$ on $\widetilde{K}$ given by $g \cdot \alpha = g(\alpha)$. This action, moreover, preserves the $\widetilde{K}$-Hopf algebra structure of $\widetilde{K} \otimes_k H$ obtained by base changing as in Proposition 4.16. Since $\widetilde{K} \otimes_k H \cong \widetilde{K}[N]$, G must too act on $\widetilde{K}[N]$, also preserving the $\widetilde{K}$-Hopf algebra structure.

Note that the set of grouplikes of $\widetilde{K}[N]$ coincides with N. Now observe that for any $n \in N$, and any $\sigma \in G$, we have

$$\Delta(\sigma(n)) = \sigma\Delta(n) = \sigma(n \otimes n) = \sigma(n) \otimes \sigma(n)$$

where the second equality follows since, as mentioned above, G preserves the $\widetilde{K}$-Hopf algebra structure of $\widetilde{K}[N]$, the third since n is a grouplike of $\widetilde{K}[N]$, and the final since the action of G on $\widetilde{K}[N]$ can be extended to an action of G on $\widetilde{K}[N] \otimes \widetilde{K}[N]$ in the usual way (by acting on both components). In particular, the above shows that G takes grouplikes of $\widetilde{K}[N]$ to grouplies of $\widetilde{K}[N]$, so takes N to N, giving us an actual action of G on N.

We would like to show that this action is via conjugation under λ the left translation. We claim first that $\sigma(\Phi(x)) = \Phi(\sigma(x))$ for all $\sigma \in G$ and $x \in (\widetilde{K} \otimes_k H) \otimes_{\widetilde{K}} (\widetilde{K} \otimes_k K)$, i.e., that Φ is G-equivariant. We have

$$\begin{aligned}\sigma(\Phi((\widetilde{\beta} \otimes h) \otimes (\widetilde{\gamma} \otimes \alpha))) &= \sigma(\widetilde{\beta}\widetilde{\gamma} \otimes (h \cdot \alpha)) \\ &= \sigma(\widetilde{\beta}\widetilde{\gamma}) \otimes (h \cdot \alpha) \\ &= \sigma(\widetilde{\beta})\sigma(\widetilde{\gamma}) \otimes (h \cdot \alpha) \\ &= \Phi((\sigma(\widetilde{\beta}) \otimes h) \otimes (\sigma(\widetilde{\gamma}) \otimes \alpha)) \\ &= \Phi(\sigma((\widetilde{\beta} \otimes h) \otimes (\widetilde{\gamma} \otimes \alpha)))\end{aligned}$$

which proves the statement. In particular, the equivalence of the actions Φ and Ψ gives Ψ is G-equivariant as well, and hence it follows that for all $\sigma \in G$, $n \in N$, and $[e_{\overline{g}}] \in X$ we have

$$\begin{aligned}\sigma(n)(\sigma([e_{\overline{g}}])) &= \Psi(\sigma(n) \otimes \sigma([e_{\overline{g}}])) \\ &= \Psi(\sigma(n \otimes [e_{\overline{g}}])) \\ &= \sigma(\Psi(n \otimes [e_{\overline{g}}])) \\ &= \sigma(n([e_{\overline{g}}]))\end{aligned}$$

In particular, we can find

$$\begin{aligned}&= \sigma([e_{n(\overline{g})}]) \\ &= \sigma(n([e_{\overline{g}}])) \\ &= \sigma(n)([e_{\overline{g}}]) \\ &= \sigma(n)(\sigma([e_{\overline{g}}])) \\ &= \sigma(n)([e_{\sigma(\overline{g})}]) \\ &= [e_{\sigma(n)(\lambda(\sigma)(\overline{g})}]\end{aligned}$$

using what we found above. Since each of the elements above were arbitrary, we have in fact showed that

$$\sigma(n)(\lambda(\sigma)(\overline{g})) = \lambda(\sigma)\left(n(\overline{g})\right)\big) = (\lambda(\sigma) \circ n)(\overline{g})$$

Now we are at liberty to define $\overline{h} = \lambda(\sigma)(\overline{g})$, which gives $\overline{g} = \lambda(\sigma^{-1})(\overline{h})$ if we apply inverses in G. In summary, we have

$$\sigma(n)(\overline{h}) = \left(\lambda(\sigma) \circ n \circ \lambda(\sigma^{-1})\right)(\overline{h})$$

for all $\sigma \in G$, $n \in N$, and $\overline{h} \in G/G'$. In particular, we have shown that elements $\sigma \in G$ act on elements $n \in N$ via conjugation by $\lambda(\sigma) \in \mathrm{Perm}(G/G')$, i.e., that $\sigma(n) = \lambda(\sigma) \circ n \circ \lambda(\sigma^{-1})$. Hence $\lambda(G)$ normalizes the image of N in $\mathrm{Perm}(G/G')$, proving the theorem. ∎

While that was somewhat arduous, we are that much closer to our goal. We now attempt to treat the converse statement. That is, given a regular subgroup N of $\mathrm{Perm}(G/G')$ normalized by $\lambda(G)$, do we get a unique H-Hopf algebra making K/k into an H-Galois extension, which is associated to that specific N?

Theorem 4.29. Let K/k be a finite separable extension of fields, and let $\widetilde{K}$ denote the normal closure of K. Let $G = \mathrm{Gal}(\widetilde{K}/k)$ and $G' = \mathrm{Gal}(\widetilde{K}/K)$. If N is a regular subgroup of $\mathrm{Perm}(G/G')$ normalized by $\lambda(G)$, then K/k is H-Galois, where H is a $\widetilde{K}$-form of $\widetilde{K}[N]$.

Proof. Suppose N is such a regular subgroup of $\mathrm{Perm}(G/G')$ nornalized by $\lambda(G)$. Once again, let $X = \{[e_{\overline{g}}] \mid \overline{g} \in G/G'\}$ denote a $\widetilde{K}$-basis for $\mathrm{Map}(G/G', \widetilde{K})$ over $\widetilde{K}$. From Theorem 4.20, we have that $\mathrm{Map}(G/G', \widetilde{K})/\widetilde{K}$ is a $\widetilde{K}[N]$-Galois extension, with the associated Hopf action of $\widetilde{K}[N]$ on $\mathrm{Map}(G/G', \widetilde{K})$ given by

$$\mu : \widetilde{K}[N] \otimes_{\widetilde{K}} \mathrm{Map}(G/G', \widetilde{K}) \to \mathrm{Map}(G/G', \widetilde{K})$$

$$n \otimes [e_{\overline{g}}] \longmapsto n([e_{\overline{g}}]) = [e_{n(\overline{g})}]$$

defined above on X, and easily extended by linearity. Now, by assumption N is normalized by $\lambda(G)$, that is, there is a bijection for every $\sigma \in G$ given by

$$p_\sigma : N \to N$$

$$n \longmapsto \lambda(\sigma) n \lambda(\sigma^{-1})$$

With this collection of maps, we claim that $\Gamma : G \to \mathrm{Aut}(N)$ defined by $\Gamma(\sigma) = p_\sigma$ is a group homomorphism. To show this, let $\sigma, \tau \in G$. Then for all $n \in N$ we have

$$\begin{aligned} p_{\sigma\tau}(n) &= \lambda(\sigma\tau) n \lambda((\sigma\tau)^{-1}) \\ &= \lambda(\sigma\tau) n \lambda(\tau^{-1}\sigma^{-1}) \\ &= \lambda(\sigma)\lambda(\tau) n \lambda(\tau^{-1})\lambda(\sigma^{-1}) \\ &= p_\sigma(\lambda(\tau)(n)\lambda(\tau^{-1})) \\ &= (p_\sigma \circ p_\tau)(n) \end{aligned}$$

and hence Γ is indeed a group homomorphism. Now note that $\mathrm{Aut}(N) \cong \mathrm{Aut}_{\widetilde{K}}(\widetilde{K}[N])$ where $\widetilde{K}[N]$ is considered as a $\widetilde{K}$-Hopf algebra (this should not be too bad, just extend automorphisms of N in a $\widetilde{K}$-linear fashion). Thus for each $\sigma \in G$ we have an associated p_σ which (under the isomorphism)

acts as a $\widetilde{K}$-linear automorphism of $\widetilde{K}[N]$. In particular, $\{p_\sigma \mid \sigma \in G\}$ is a set of 1-cocycles in the first cohomology set $H^1(G, \mathrm{Aut}_{\widetilde{K}}(\widetilde{K}[N]))$.

We next check that the following diagram commutes:

$$\begin{array}{ccc} \widetilde{K}[N] \otimes_{\widetilde{K}} \mathrm{Map}(G/G', \widetilde{K}) & \xrightarrow{\sigma\circ\mu\circ\sigma^{-1}} & \mathrm{Map}(G/G', \widetilde{K}) \\ \Big\downarrow{\scriptstyle p_\sigma\otimes\mathrm{id}} & & \Big\| \\ \widetilde{K}[N] \otimes_{\widetilde{K}} \mathrm{Map}(G/G', \widetilde{K}) & \xrightarrow{\mu} & \mathrm{Map}(G/G', \widetilde{K}) \end{array}$$

For convenience, set $\mu^\sigma = \sigma \circ \mu \circ \sigma^{-1}$. Allow G to act trivially on N, $\sigma \cdot n = n$ for all $\sigma \in G$ and $n \in N$, and recall that G acts on $\mathrm{Map}(G/G', \widetilde{K})$ via the action

$$G \times \mathrm{Map}(G/G', \widetilde{K}) \to \mathrm{Map}(G/G', \widetilde{K})$$

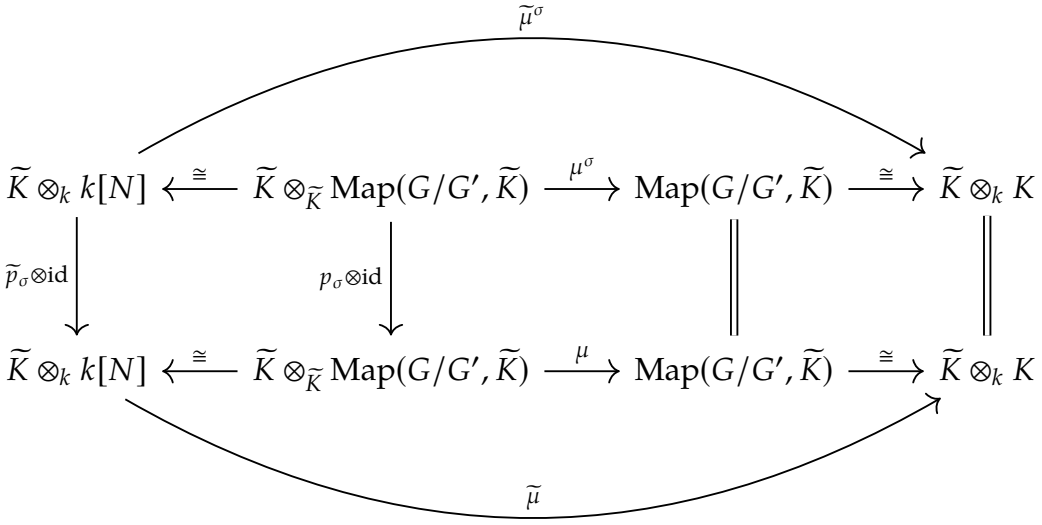
$$(\sigma, [e_{\overline{g}}]) \longmapsto \sigma([e_{\overline{g}}]) = [e_{\overline{\sigma g}}] = [e_{\lambda(\sigma)(\overline{g})}]$$

To show commutativity of the diagram above, we must prove that $\mu^\sigma = \mu \circ (p_\sigma \otimes \mathrm{id})$. To this end, note that for all $n \otimes [e_{\overline{g}}] \in \widetilde{K}[N] \otimes_{\widetilde{K}} \mathrm{Map}(G/G', \widetilde{K})$ we have

$$\begin{aligned} \mu^\sigma(n \otimes [e_{\overline{g}}]) &= (\sigma \circ \mu \circ \sigma^{-1})(n \otimes [e_{\overline{g}}]) \\ &= (\sigma \circ \mu)(n \otimes [e_{\overline{\sigma^{-1}g}}])) \\ &= \sigma([e_{n(\overline{\sigma^{-1}g})}]) \\ &= [e_{\overline{\sigma} n(\overline{\sigma^{-1}g})}] \\ &= [e_{\lambda(\sigma)(n(\lambda(\sigma^{-1})(\overline{g}))}] \\ &= [e_{(\lambda(\sigma)\circ n\circ\lambda(\sigma^{-1}))(\overline{g})}] \\ &= \mu\left(\lambda(\sigma) n \lambda(\sigma^{-1}) \otimes [e_{\overline{g}}]\right) \\ &= \mu(p_\sigma \otimes \mathrm{id})(n \otimes [e_{\overline{g}}]) \end{aligned}$$

which proves commutativity of the diagram, as claimed. Now we can use previous lemmas (some choice isomorphisms) to modify the diagram to suit our needs. Recall from Proposition 4.17 that $\mathrm{Map}(G/G', \widetilde{K}) \cong \widetilde{K} \otimes_k K$ as $\widetilde{K}$-algebras. We also have $\widetilde{K}[N] \cong \widetilde{K} \otimes_k k[N]$ as $\widetilde{K}$-algebras. Hence we

have a diagram



where $\widetilde{\mu}^\sigma$, $\widetilde{\mu}$, and $\widetilde{p}_\sigma \otimes \mathrm{id}$ are the maps induced by the commutativity of the first diagram and the isomorphisms of $\widetilde{K}$-algebras mentioned above. In particular, the above diagram commutes, and so $\widetilde{\mu}$ is the new Hopf action of $\widetilde{K} \otimes_k k[N]$ on $\widetilde{K} \otimes_k K$.

We have all the requisite ingredients to apply the techniques of Galois descent covered in the previous section. Note that $\widetilde{p}_\sigma$ is a 1-cocycle inside of the first cohomology set $H^1(G, \mathrm{Aut}_{\widetilde{K}}(\widetilde{K} \otimes_k k[N]))$. As such, since $\widetilde{K}/K$ is a finite Galois extension of fields, Theorem 4.25 asserts that $\widetilde{p}_\sigma$ corresponds to a K-form of $K[N]$. Let H be this $\widetilde{K}$-form. We also trivially have that K is a $\widetilde{K}$-form, corresponding to the identity 1-cocycle. Note that the map

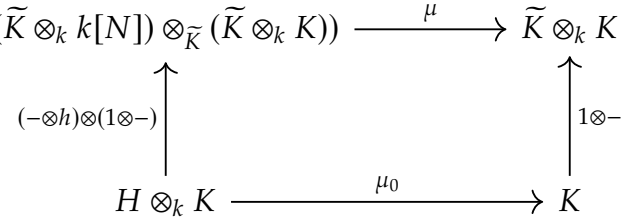
$$\widetilde{\mu} : (\widetilde{K} \otimes_k k[N]) \otimes_{\widetilde{K}} (\widetilde{K} \otimes_k K) \to \widetilde{K} \otimes_k K$$

satisfies

$$\widetilde{\mu} \circ \widetilde{p}_\sigma = \widetilde{\mu}^\sigma = \sigma \circ \widetilde{\mu} \circ \sigma^{-1}$$

and hence in the notation of Lemma 4.27 we have that $\widetilde{\mu}$ is descendable (this works because we have the above for all $\sigma \in G$).

By definition of descendability, this means that there exists a (necessarily unique) k-linear map μ_0 such that the diagram



commutes. This map μ_0 is a Hopf action of H on K. Now we claim that H identifies with the k-Hopf subalgebra $(\widetilde{K} \otimes_k H)^G$ of $\widetilde{K} \otimes_k H$, where the superscript G denotes the fixed ring defined previously. We have

$$(\widetilde{K} \otimes_k H)^G = \widetilde{K}^G \otimes_k H = k \otimes_k H \cong H$$

since G is acting here only on the $\widetilde{K}$ component of the tensor. Similarly, we may identify K with the k-subalgebra $(\widetilde{K} \otimes_k K)^G$ of $\widetilde{K} \otimes_k K$ via

$$(\widetilde{K} \otimes_k K)^G = \widetilde{K}^G \otimes_k K = k \otimes_k K \cong K$$

Hence (H, μ_0) is a Hopf-Galois structure for K/k, sufficing to make K/k into a H-Galois extension; note also that since $\widetilde{K} \otimes_k H \cong \widetilde{K}[N]$, we have that

$$(\widetilde{K} \otimes_k H)^G \cong (\widetilde{K}[N])^G$$

from the above discussion, which now shows that K/k is a $(\widetilde{K}[N])^G$-Galois extension. ■

And finally, at last, we have reached our destination. After all of the heavy-lifting above, we may present the Greither-Pareigis theorem for separable extensions of fields. The proof will be short and sweet, we merely cite the two theorems above.

Theorem 4.30 (Greither-Pareigis)**.** Let K/k be a finite separable extension of fields. Let $\widetilde{K}$ denote the normal closure of K. Write $G = \mathrm{Aut}(\widetilde{K}/k)$ and $G' = \mathrm{Aut}(\widetilde{K}/K)$.

Let N be a subgroup of $\mathrm{Perm}(G/G')$. Then the following are equivalent

1. There exists a k-Hopf algebra H making the extension K/k into an H-Galois extension.
2. N is a regular subgroup of $\mathrm{Perm}(G/G')$, and $\lambda(G)$, the image of G the left translation map $\lambda : G \to \mathrm{Perm}(G/G')$, normalizes N.

In other words, there is a bijection between the distinct isomorphism classes of Hopf-Galois structures on K/k to the regular subgroups of $\mathrm{Perm}(G/G')$ which are normalized by the image of G under the left translation mapping in $\mathrm{Perm}(G/G')$.

Moreover, the k-Hopf algebra H corresponding to the regular subgroup N normalized by $\lambda(G)$ in (1) above is precisely the k-Hopf subalgebra $(\widetilde{K}[N])^G$ of $\widetilde{K}[N]$ consisting of those elements fixed by the usual Galois action of G on elements of $\widetilde{K}$.

Proof. A simple three line proof. The implication (1) $\implies$ (2) is given by Theorem 4.28. The implication (2) $\implies$ (1) is given by Theorem 4.29, completing the proof. ∎

We now make several remarks about the Hopf-Galois structure given from the existence of a regular subgroup of $\mathrm{Perm}(G/G')$ normalized by $\lambda(G)$ in (1) of Theorem 4.30.

As is mentioned in the theorem, the k-Hopf algebra H corresponding to this N is precisely the fixed ring k-Hopf subalgebra $(\widetilde{K}[N])^G$ of $\widetilde{K}[N]$. We make note of the fact that G acts on $\widetilde{K}[N]$ by acting as automorphisms of $\widetilde{K}$ fixing k and by acting by conjugation via λ on N. That is, for every $\sigma \in G$ and $n \in N$, we have

$$\sigma\left(\sum_{n\in N} \beta_n[n]\right) = \sum_{n\in N} \sigma(\beta_n)[\lambda(\sigma)n\lambda(\sigma^{-1}]$$

where we note that $\lambda(\sigma)n\lambda(\sigma^{-1}) \in N$ since N is normalized by $\lambda(G)$. A next question might be, what is the Hopf action of $(\widetilde{K}[N])^G$ on K/k. We have that

$$\Theta : \widetilde{K}[N] \to \mathrm{End}_k(\widetilde{K})$$

taking elements $n \in N$ to σ where $n^{-1}(\overline{1_G})) = \overline{\sigma}$, and taking $\beta \in \widetilde{K}$ to the k-linear endomorphism induced by left multiplication by β. Restricting this map Θ to the k-Hopf subalgebra $(\widetilde{K}[N])^G$ gives us the Hopf action.

References

[CGK+21] Lindsay N Childs, Cornelius Greither, Kevin P Keating, Alan Koch, Timothy Kohl, Paul J Truman, and Robert G Underwood. *Hopf algebras and Galois module theory*, volume 260. American Mathematical Soc., 2021.

[Chi89] Lindsay N Childs. On the hopf galois theory for separable field extensions. *Communications in Algebra*, 17(4):809–825, 1989.

[Chi00] Lindsay Childs. *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory: Hopf Algebras and Local Galois Module Theory*. Number 80. American Mathematical Soc., 2000.

[DNR00] Sorin Dascalescu, Constantin Nastasescu, and Serban Raianu. *Hopf algebra: An introduction*. CRC Press, 2000.

[PG87] Bodo Pareigis and Cornelius Greither. Hopf galois theory for separable field extensions. *Journal of Algebra*, (1):239–258, 1987.

[Und11] Robert G Underwood. *An introduction to Hopf algebras*. Springer Science & Business Media, 2011.

[Und15] Robert G Underwood. *Fundamentals of Hopf algebras*. Springer, 2015.