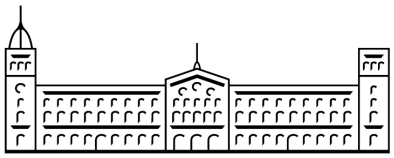


Treball final de grau

GRAU DE MATEMÀTIQUES

Facultat de Matemàtiques
Universitat de Barcelona

HOPF GALOIS THEORY OF SEPARABLE FIELD EXTENSIONS

Marta Salguero García

Directora: Dra. Teresa Crespo
Realitzat a: Departament d'Àlgebra i Geometria

Barcelona, June 27, 2016

Abstract

Hopf Galois theory is a generalization of Galois theory. Galois theory gives a bijective correspondence between intermediate fields of a Galois field extension (normal and separable) and subgroups of the Galois group. Hopf Galois theory substitutes the Galois group by a Hopf algebra. In the case of separable extensions it has a characterization of the Hopf Galois character in terms of groups. Thus, we use Magma in order to obtain all Hopf Galois structures of extensions of degree 8.

Acknowledgements

I want to thank Professor Teresa Crespo for all the help and time she has spent with me these last five months. I would also like to thank Teresa as well as Joan Nualart, who were my teachers of Algebraic Equations for the past year, for their patience, enthusiasm and time when I most needed it. That subject was very difficult for me but actually led me to this dissertation.

I want to thank my teachers of the University of Extremadura too, where I started my degree, for they laid the foundations. I am especially grateful to Juan A. Navarro, José Navarro, Juan Sancho, Pedro Sancho and Fernando Sánchez for having been such wonderful teachers and, furthermore, models and friends.

I want to thank my family, especially my parents, my friends and my local churches in Barcelona and in Badajoz for their support during my undergraduate studies.

And finally, but not least, I want to thank God, the Great Mathematician and Creator of the Universe. Thank you, Jesus, for giving me a new life and for giving real meaning to what I am and do.

"This most beautiful system of the sun, planets, and comets, could only proceed from the counsel and dominion of an intelligent and powerful Being... This Being governs all things, not as the soul of the world, but as Lord over all"

Principia Mathematica - Sir Isaac Newton

Contents

1 Introduction

Project

Galois theory, named after Évariste Galois, provides a connection between field theory and group theory. Using Galois theory, certain problems in field theory can be reduced to group theory, which is, in some sense, simpler and better understood. Galois theory classifies intermediate fields of a Galois field extension $L|K$ by means of the subgroups of $G = \mathrm{Gal}(L|K)$ of K-automorphisms of L.

The Galois action of the Galois group G on L induces an action of the group algebra $K[G]$ on L. Replacing $K[G]$ with an appropriate algebra we can generalize Galois theory. Chase and Sweedler introduced in the sixties the Hopf Galois theory in which the action of G is replaced by the action of a Hopf algebra, and they applied it to inseparable extensions. Later on, Greither and Pareigis studied the Hopf Galois theory of separable field extensions and stated the Hopf Galois character of a field extension in terms of groups. Hopf Galois theory has applications in number theory in the study of integral normal basis and ramification.

In this dissertation, we introduce the notions of Hopf algebra and Hopf Galois extension, and discuss some results of Hopf Galois theory in the case of separable extensions. The characterization of the Hopf Galois character in terms of groups allows us to use the computational algebra system Magma to obtain explicit calculations. We focus on separable extensions of degree 8.

Memory structure

In order to reach to the concept of Hopf algebra, we need some previous knowledge. We start defining tensor product of modules over a ring. It leads us to construct the first important structure, called algebra, as a vector space endowed with two linear maps satisfying certain properties which may be presented via commutative diagrams. We define coalgebras as co-objects to algebras formed by reversing the arrows in the diagrams for algebras. Afterwards, we define bialgebras as vector spaces which are both algebras and coalgebras. Finally, we construct Hopf algebras as bialgebras with an additional map.

We consider the action of a bialgebra over an algebra and define Hopf Galois extensions by means of the action of a Hopf algebra on the extension field. Moreover, in the case of separable field extensions, there is a characterization of Hopf Galois extensions in terms of groups which allows us to obtain explicit results using Magma. We focus on separable extensions of degree 8 and discuss an example in detail.

2 Algebras and coalgebras

In this first chapter, we introduce algebras and coalgebras. We begin by constructing the tensor product of a finite collection of R-modules, where R is a commutative ring with unity. We specialize to tensor products over a field K and give the diagram-theoretic definition of a K-algebra. We then define coalgebras as coobjects to algebras formed by reversing the arrows in the diagrams for algebras.

We next consider the linear dual. We show that if C is a coalgebra, then C^* is an algebra. But the converse of this statement is not true in general. In order to have the reciprocal result, we need to replace the dual space A^* with a certain subspace A° called the finite dual. Now, if A is an algebra, then A° is a coalgebra. As an application, we show that the finite dual $K[x]^\circ$ can be identified with the collection of linearly recursive sequences of all orders over K.

2.1 Multilinear maps and tensor products

In this section, we define R-n-linear maps in order to construct the tensor product of a set of R-modules $M_1, \ldots, M_n$ as the solution to a universal mapping problem.

Let R be a commutative ring with unity. Let $n \geq 2$ be an integer. Let $M_1, \ldots, M_n$ be a collection of R-modules, and let A be an R-module.

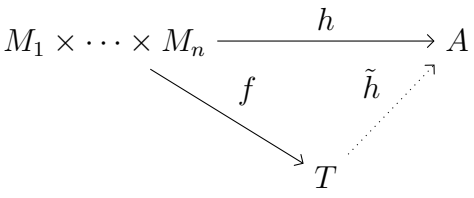
Definition 2.1.1. A map $f : M_1 \times \cdots \times M_n \to A$ is **R-n-linear** if for all $r \in R$, $a_i, a_i' \in M_i$, where $i \in \{1, \ldots, n\}$, it satisfies

1. $f(a_1, \ldots, a_i + a_i', \ldots, a_n) = f(a_1, \ldots, a_i, \ldots, a_n) + f(a_1, \ldots, a_i', \ldots, a_n)$,
2. $f(a_1, \ldots, ra_i, \ldots, a_n) = rf(a_1, \ldots, a_i, \ldots, a_n)$.

For instance, an R-bilinear map is an R-2-linear map.

Definition 2.1.2. A **tensor product** of $M_1, \ldots, M_n$ over R is an R-module T together with an R-n-linear map $f : M_1 \times \cdots \times M_n \to T$ so that for every R-module A and R-n-linear map $h : M_1 \times \cdots \times M_n \to A$ there exists a unique R-module map $\tilde{h} : T \to A$ for which $\tilde{h}f = h$.

Equivalently, the following diagram commutes:



Remark 2.1.3. From the definition, we deduce the uniqueness of the tensor product up to isomorphism. Let T_1, T_2 be tensor products of $M_1, \ldots, M_n$ over R, that is, T_1, T_2 are respectively endowed with R-n-linear maps $f_1 : M_1 \times \cdots \times M_n \to T_1$, $f_2 : M_1 \times \cdots \times M_n \to T_2$ which satisfy the tensor product property. Since T_1 is a tensor product and we have f_2, there exists a unique $\tilde{h}_1 : T_1 \to T_2$ for which $\tilde{h}_1 \circ f_1 = f_2$. Similarly, since T_2 is a tensor product and we have f_1, there exists a unique $\tilde{h}_2 : T_2 \to T_1$ for which $\tilde{h}_2 \circ f_2 = f_1$.

We need to prove that $\tilde{h}_2 \circ \tilde{h}_1 = I_{T_1}$. Note that $\tilde{h}_2 \circ (\tilde{h}_1 \circ f_1) = \tilde{h}_2 \circ f_2 = f_1$, that is, $(\tilde{h}_2 \circ \tilde{h}_1) \circ f_1 = f_1$. Since T_1 is a tensor product and we have f_1, there exists a unique $\tilde{h} : T_1 \to T_1$ for which $\tilde{h} \circ f_1 = f_1$. Thus, since both $\tilde{h}_2 \circ \tilde{h}_1$ and I_{T_1} satisfy the property of $\tilde{h}$ and it is unique, we conclude $\tilde{h}_2 \circ \tilde{h}_1 = I_{T_1}$. Analogously, one has $\tilde{h}_1 \circ \tilde{h}_2 = I_{T_2}$.

Therefore, from now on, we will note $M_1 \otimes_R \cdots \otimes_R M_n$ the tensor product of $M_1, \ldots, M_n$ over R, or just $M_1 \otimes \cdots \otimes M_n$.

We construct a tensor product as follows. Let $F\langle M_1 \times \cdots \times M_n \rangle$ be the free R-module on $M_1 \times \cdots \times M_n$: $\{f : M_1 \times \cdots \times M_n \to R$ such that $f(m_1, \ldots, m_n) = 0$, up to a finite number of elements$\}$, with operations given pointwise

$$\begin{cases} (f+g)(m_1, \ldots, m_n) = f(m_1, \ldots, m_n) + g(m_1, \ldots, m_n), \\ (\lambda f)(m_1, \ldots, m_n) = \lambda f(m_1, \ldots, m_n), \end{cases}$$

for all $(m_1, \ldots, m_n) \in M_1 \times \cdots \times M_n$ and $\lambda \in R$. Its basis is $\{f_m\}_{m \in M_1 \times \cdots \times M_n}$, where

$$f_m : M_1 \times \cdots \times M_n \longrightarrow R, \ f_m(m') = \begin{cases} 1_R & \text{if } m' = m \\ 0 & \text{if } m' \neq m \end{cases}$$

so every $f \in F\langle M_1 \times \cdots \times M_n \rangle$ can be written as $f = \sum_{m \in M_1 \times \cdots \times M_n} f(m) f_m$. From now on, we will note f_m simply as m.

Let J be the submodule of $F\langle M_1 \times \cdots \times M_n \rangle$ generated by quantities of the form

$$\begin{gathered} (a_1, \ldots, a_j + a'_j, \ldots, a_n) - (a_1, \ldots, a_j, \ldots, a_n) - (a_1, \ldots, a'_j, \ldots, a_n), \\ (a_1, \ldots, ra_j, \ldots, a_n) - r(a_1, \ldots, a_j, \ldots, a_n), \end{gathered}$$

for $a_j, a'_j \in M_j, \ r \in R, j \in \{1, \ldots, n\}$. Let $i : M_1 \times \cdots \times M_n \hookrightarrow F\langle M_1 \times \cdots \times M_n \rangle$ be the natural inclusion map and let $\pi : F\langle M_1 \times \cdots \times M_n \rangle \to F\langle M_1 \times \cdots \times M_n \rangle / J$ be the canonical surjection. Set $f := \pi \circ i$. Then, the following diagram commutes:

$$\begin{array}{ccc} M_1 \times \cdots \times M_n & \xhookrightarrow{\ i\ } & F\langle M_1 \times \cdots \times M_n \rangle \\ & \searrow^{f} & \downarrow \pi \\ & & F\langle M_1 \times \cdots \times M_n \rangle / J \end{array}$$

Then the quotient space $F\langle M_1 \times \cdots \times M_n\rangle/J$ together with the map f (which is clearly R-n-linear due to the definition of J) is a tensor product. It solves the universal mapping problem described in Definition 2.1.2.

Proposition 2.1.4. *The quotient space $F\langle M_1 \times \cdots \times M_n\rangle/J$ together with the map f is a tensor product of $M_1, \ldots, M_n$ over R.*

Proof. We need to show that the conditions of Definition 2.1.2 are satisfied. Let A be an R-module and let $h : M_1 \times \cdots \times M_n \to A$ be an R-n-linear map. The following diagram illustrates the idea of the proof:

$$\begin{array}{ccc} M_1 \times \cdots \times M_n & \xrightarrow{\quad h \quad} & A \\ {\scriptstyle i}\big\downarrow & \nearrow_{\phi} & \big\uparrow{\scriptstyle \tilde{h}} \\ F\langle M_1 \times \cdots \times M_n\rangle & \xrightarrow{\quad \pi \quad} & F\langle M_1 \times \cdots \times M_n\rangle/J \end{array}$$

Indeed, there exists an R-module map $\phi : F\langle M_1 \times \cdots \times M_n\rangle \to A$ determined by $\phi(m_1, \ldots, m_n) = h(m_1, \ldots, m_n)$. Since h is R-n-linear, by the definition of J and ϕ, one has $J \subseteq \mathrm{Ker}(\phi)$. Thus, by the universal property of the quotient module, there exists a unique R-module map $\tilde{h} : F\langle M_1 \times \cdots \times M_n\rangle/J \to A$ defined as $\tilde{h}([m_1, \ldots, m_n]_J) = \phi(m_1, \ldots, m_n)$. Finally, $\tilde{h} \circ \pi \circ i = \tilde{h} \circ f = h$. □

Consequently, we write

$$F\langle M_1 \times \cdots \times M_n\rangle/J = M_1 \otimes \cdots \otimes M_n.$$

with the class $[(m_1, \ldots, m_n)]_J$ now written as the **tensor** $m_1 \otimes \cdots \otimes m_n$.

Proposition 2.1.5. *Let M_1, M_2 be R-modules and let N_1, N_2 be R-submodules of M_1, M_2, respectively. Then there is an isomorphism of R-modules*

$$M_1/N_1 \otimes M_2/N_2 \cong (M_1 \otimes M_2)/(N_1 \otimes M_2 + M_1 \otimes N_2).$$

Proof. The following diagrams illustrate the idea of the proof:

$$\begin{array}{ccc} M_1 \times M_2 & \xrightarrow{\quad \text{bilin} \quad} & M_1 \otimes M_2 \\ {\scriptstyle h}\big\downarrow & \swarrow_{\tilde{h}} & \big\downarrow{\scriptstyle \pi} \\ M_1/N_1 \otimes M_2/N_2 & \xleftarrow[\cong\, \alpha]{} & (M_1 \otimes M_2)/(N_1 \otimes M_2 + M_1 \otimes N_2) \end{array}$$

$$\begin{array}{ccc} M_1/N_1 \times M_2/N_2 & \xrightarrow{\quad \text{bilin} \quad} & M_1/N_1 \otimes M_2/N_2 \\ {\scriptstyle l}\big\downarrow & \swarrow_{\cong\, \tilde{l} = \alpha^{-1}} & \\ (M_1 \otimes M_2)/(N_1 \otimes M_2 + M_1 \otimes N_2) & & \end{array}$$

First note that there is an R-bilinear map $h : M_1 \times M_2 \to M_1/N_1 \otimes M_2/N_2$ defined by $h(m_1, m_2) = [m_1]_{N_1} \otimes [m_2]_{N_2}$. Since $M_1 \otimes M_2$ is a tensor product, there exists a unique R-module map $\tilde{h} : M_1 \otimes M_2 \to M_1/N_1 \otimes M_2/N_2$ defined by $\tilde{h}(m_1 \otimes m_2) = [m_1]_{N_1} \otimes [m_2]_{N_2}$.

Then, note that $N_1 \otimes M_2 + M_1 \otimes N_2 \subseteq \ker(\tilde{h})$. Now, we consider the canonical surjection $\pi : M_1 \otimes M_2 \to (M_1 \otimes M_2)/N_1 \otimes M_2 + M_1 \otimes N_2)$. Thus, by the universal property of the quotient module, there exists a unique R-module map

$$\begin{array}{rccc} \alpha: & (M_1 \otimes M_2)/(N_1 \otimes M_2 + M_1 \otimes N_2) & \to & M_1/N_1 \otimes M_2/N_2 \\ & [m_1 \otimes m_2]_{(N_1 \otimes M_2 + M_1 \otimes N_2)} & \mapsto & [m_1]_{N_1} \otimes [m_2]_{N_2} \end{array}$$

Next, we define the following map

$$\begin{array}{rccc} l: & (M_1/N_1 \times M_2/N_2) & \to & (M_1 \otimes M_2)/(N_1 \otimes M_2 + M_1 \otimes N_2) \\ & ([m_1]_{N_1}, [m_2]_{N_2}) & \mapsto & [m_1 \otimes m_2]_{(N_1 \otimes M_2 + M_1 \otimes N_2)} \end{array}$$

We see that l is a well-defined map. Let $[m_1]_{N_1} = [m_1']_{N_1}$ and $[m_2]_{N_2} = [m_2']_{N_2}$. There exist $n_1 \in N_1, n_2 \in N_2$ such that $m_1' = m_1 + n_1, m_2' = m_2 + n_2$. Therefore,

$$m_1' \otimes m_2' = (m_1 + n_1) \otimes (m_2 + n_2) = m_1 \otimes m_2 + m_1 \otimes n_2 + n_1 \otimes m_2 + n_1 \otimes n_2 =$$
$$= m_1 \otimes m_2 + n_1 \otimes m_2 + (m_1 + n_1) \otimes n_2 \in m_1 \otimes m_2 + N_1 \otimes M_2 + M_1 \otimes N_2 =$$
$$= [m_1 \otimes m_2]_{N_1 \otimes M_2 + M_1 \otimes N_2} \Rightarrow [m_1 \otimes m_2]_{N_1 \otimes M_2 + M_1 \otimes N_2} = [m_1' \otimes m_2']_{N_1 \otimes M_2 + M_1 \otimes N_2}.$$

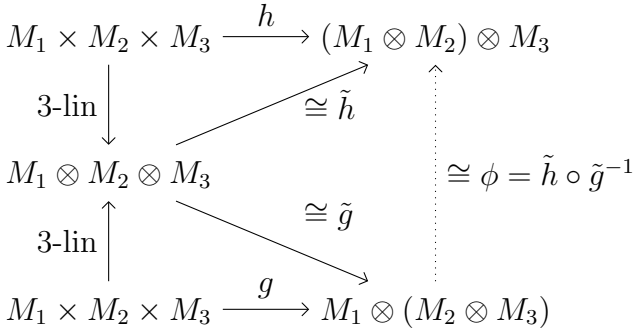
Hence, l is well-defined. It is easy to show that l is R-bilinear and so, since $M_1/N_1 \otimes M_2/N_2$ is a tensor product, there exists a unique R-module map

$$\begin{array}{rccc} \tilde{l}: & (M_1/N_1 \otimes M_2/N_2) & \to & (M_1 \otimes M_2)/(N_1 \otimes M_2 + M_1 \otimes N_2) \\ & [m_1]_{N_1} \otimes [m_2]_{N_2} & \mapsto & [m_1 \otimes m_2]_{(N_1 \otimes M_2 + M_1 \otimes N_2)} \end{array}$$

Clearly, $\alpha^{-1} = \tilde{l}$, and thus $\tilde{l}$ is an isomorphism. □

Proposition 2.1.6. *Let M_1, M_2, M_3 be R-modules. Then there is an R-module isomorphism $M_1 \otimes (M_2 \otimes M_3) \cong (M_1 \otimes M_2) \otimes M_3$ (that is, the associative property for tensor products holds).*

Proof. The following diagram illustrates the idea of the proof:



Let $h : M_1 \times M_2 \times M_3 \to (M_1 \otimes M_2) \otimes M_3$ be the map defined by $h(m_1, m_2, m_3) = (m_1 \otimes m_2) \otimes m_3$. We see that h is R-3-linear: for $r, r' \in R, m_1, m_1' \in M_1, m_2 \in M_2$, $m_3 \in M_3$,

$$\begin{aligned} h(rm_1 + r'm_1', m_2, m_3) &= ((rm_1 + r'm_1') \otimes m_2) \otimes m_3 = \\ &= (r(m_1 \otimes m_2) + r'(m_1' \times m_2)) \otimes m_3 = \\ &= r((m_1 \otimes m_2) \otimes m_3) + r'((m_1' \otimes m_2) \otimes m_3) = \\ &= rh(m_1, m_2, m_3) + r'h(m_1', m_2, m_3). \end{aligned}$$

So, h is R-linear in the first component. Similar calculations show that h is R-linear in the other components. Thus, h is an R-3-linear map, and since $M_1 \otimes M_2 \otimes M_3$ is a tensor product, there exists a unique map of R-modules $\tilde{h} : M_1 \otimes M_2 \otimes M_3 \to (M_1 \otimes M_2) \otimes M_3$ defined by $\tilde{h}(m_1 \otimes m_2 \otimes m_3) = (m_1 \otimes m_2) \otimes m_3$. Clearly, $\tilde{h}$ is an isomorphism.

In a similar manner, one constructs another isomorphism $\tilde{g} : M_1 \otimes M_2 \otimes M_3 \to M_1 \otimes (M_2 \otimes M_3)$ defined by $\tilde{g}(m_1 \otimes m_2 \otimes m_3) = m_1 \otimes (m_2 \otimes m_3)$. Finally, we define $\phi : M_1 \otimes (M_2 \otimes M_3) \to (M_1 \otimes M_2) \otimes M_3$ as the composition $\phi = \tilde{h} \circ \tilde{g}^{-1}$. Then ϕ is an isomorphism of R-modules. □

By an **"iterated tensor product in some association"** we mean a tensor product whose factors themselves may be tensor products or tensor products of tensor products, and so on. As we have seen in the previous proposition, there is a natural isomorphism between tensor products and iterated tensor products in some association.

Proposition 2.1.7. *Let $M_1, \ldots, M_n$ be R-modules and let S be an iterated tensor product of $M_1, \ldots, M_n$ in some association. Then there is a natural isomorphism $M_1 \otimes \cdots \otimes M_n \cong S$.*

Proof. We proceed by induction on n. The trivial case $n = 2$ clearly holds. Assume the result holds for any collection of less than n R-modules, and we are going to see that it holds for $M_1, \ldots, M_n$. There exists an integer $r \in \{1, \ldots, n-1\}$ for which $S = T \otimes U$, where T is an iterated tensor product of $M_1, \ldots, M_r$ in some association and U is an iterated tensor product of $M_{r+1}, \ldots, M_n$ in some association. By the induction hypothesis, $T \cong M_1 \otimes \cdots \otimes M_r$ and $U \cong M_{r+1} \otimes \cdots \otimes M_n$, and so, $S \cong (M_1 \otimes \cdots \otimes M_r) \otimes (M_{r+1} \otimes \cdots \otimes M_n)$.

Let $h : M_1 \times \cdots \times M_n \to (M_1 \otimes \cdots \otimes M_r) \otimes (M_{r+1} \otimes \cdots \otimes M_n)$ be the map defined as $h(m_1, \ldots, m_r, m_{r+1}, \ldots, m_n) = (m_1 \otimes \cdots \otimes m_r) \otimes (m_{r+1} \otimes \cdots \otimes m_n)$, which is n-linear. Since $M_1 \otimes \cdots \otimes M_n$ is a tensor product, there exists a unique map of R-modules $\tilde{h} : M_1 \otimes \cdots \otimes M_n \to (M_1 \otimes \cdots \otimes M_r) \otimes (M_{r+1} \otimes \cdots \otimes M_n)$ given by $\tilde{h}(m_1 \otimes \cdots \otimes m_r \otimes m_{r+1} \otimes \cdots \otimes m_n) = (m_1 \otimes \cdots \otimes m_r) \otimes (m_{r+1} \otimes \cdots \otimes m_n)$. Clearly, $\tilde{h}$ is an isomorphism. Therefore we conclude $S \cong M_1 \otimes \cdots \otimes M_n$. □

In view of this proposition, we will ignore the parentheses from now on and consider tensor products and iterated tensor products in some association as the same objects through the natural isomorphism.

We close this section with two remarks about maps.

Proposition 2.1.8. *Let $M_1, \ldots, M_n, M'_1, \ldots, M'_n$ be R-modules and for $i \in \{1, \ldots, n\}$, let $f_i : M_i \to M'_i$ be R-module maps. Then there exists a unique map of R-modules*

$$\begin{array}{rccc} f_1 \otimes \cdots \otimes f_n : & M_1 \otimes \cdots \otimes M_n & \to & M'_1 \otimes \cdots \otimes M'_n \\ & m_1 \otimes \cdots \otimes m_n & \mapsto & f_1(m_1) \otimes \cdots \otimes f_n(m_n) \end{array}$$

Proof. There exists an R-n-linear map $h = f_1 \times \cdots \times f_n : M_1 \times \cdots \times M_n \to M'_1 \otimes \cdots \otimes M'_n$ defined as $(f_1 \times \cdots \times f_n)(m_1, \ldots, m_n) = f_1(m_1) \otimes \cdots \otimes f_n(m_n)$. Since $M_1 \otimes \cdots \otimes M_n$ is a tensor product, there exists a unique R-module map $\tilde{h} = f_1 \times \cdots \times f_n : M_1 \otimes \cdots \otimes M_n \to M'_1 \otimes \cdots \otimes M'_n$ defined as $\tilde{h}(m_1 \otimes \cdots \otimes m_n) = f_1(m_1) \otimes \cdots \otimes f_n(m_n)$. □

Corollary 2.1.9. *Let K be a field and let $V_1, \ldots, V_n$ be a finite set of vector spaces over K. Then $V_1^* \otimes \cdots \otimes V_n^* \subseteq (V_1 \otimes \cdots \otimes V_n)^*$.*

Proof. Let $f_i \in V_i^*$, where $i \in \{1, \ldots, n\}$, be a set of K-linear forms, that is to say, $f_i : V_i \to K, \forall i \in \{1, \ldots, n\}$. By the previous proposition, there exists a unique K-linear map $f_1 \otimes \cdots \otimes f_n \in V_1^* \otimes \cdots \otimes V_n^*$ defined as:

$$\begin{array}{rccc} f_1 \otimes \cdots \otimes f_n : & V_1 \otimes \cdots \otimes V_n & \to & K \otimes \cdots \otimes K \\ & v_1 \otimes \cdots \otimes v_n & \mapsto & f_1(v_1) \otimes \cdots \otimes f_n(v_n) \end{array}$$

Since $K \otimes K \cong K$ through the map $r \otimes s \mapsto rs$, then $f_1(v_1) \otimes \cdots \otimes f_n(v_n) = f_1(v_1) \ldots f_n(v_n) \in K$, and so $f_1 \otimes \cdots \otimes f_n \in (V_1 \otimes \cdots \otimes V_n)^*$. Consequently, $V_1^* \otimes \cdots \otimes V_n^* \subseteq (V_1 \otimes \cdots \otimes V_n)^*$. □

We remark that we have the equality in the previous corollary if, and only if, each V_i is finite dimensional.

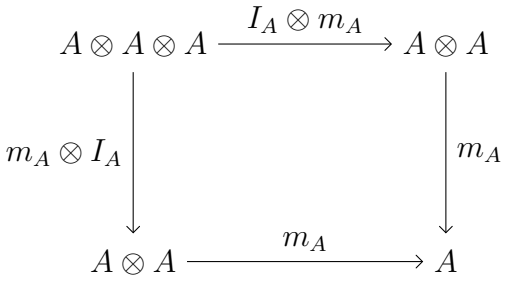
2.2 Algebras and coalgebras

In this section, we present the diagram-theoretic definition of a K-algebra and prove its equivalence with the usual definition. Afterwards, we see some basic examples and discuss quotient algebras and algebra homomorphisms. Next, we define coalgebras as co-objects to algebras formed by reversing the arrows in the diagrams for algebras, and give some examples. We introduce Sweedler notation to write the image of the comultiplication map and we show how it works to simplify computations. We define coideals, quotient algebras and algebra homomorphisms.

Let K be a field.

Definition 2.2.1. A K-**algebra** is a triple (A, m_A, λ_A) consisting of a K-vector space and K-linear maps $m_A : A \otimes A \to A$ and $\lambda_A : K \to A$ that satisfy the following conditions:

1. The diagram commutes



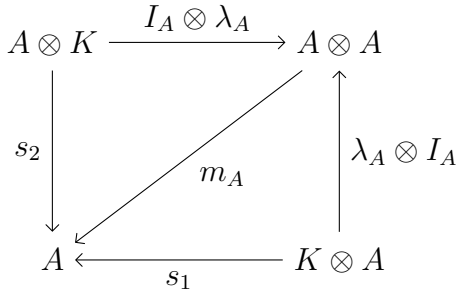
   where the map $I_A : A \to A$ is the identity map on A.

   Equivalently, we have for all $a, b, c \in A$,

$$m_A(I_A \otimes m_A)(a \otimes b \otimes c) = m_A(m_A \otimes I_A)(a \otimes b \otimes c) \tag{2.1}$$

   The map m_A is called the **multiplication map** and Condition (2.1) is the **associative property**.

2. The diagram commutes



   where the map $s_1 : K \otimes A \to A$ is defined by $r \otimes a \mapsto ra$ and the map $s_2 : A \otimes K \to A$ is defined by $a \otimes r \mapsto ra$.

   Equivalently, we have for all $r \in K, a \in A$,

$$m_A(I_A \otimes \lambda_A)(a \otimes r) = ra = m_A(m_A \otimes I_A)(r \otimes a) \tag{2.2}$$

   The map λ_A is called the **unit map** and Condition (2.2) is the **unit property**.

The K-algebra A is **commutative** if $m_A\tau = m_A$, where τ (or, if necessary, $\tau_{A\otimes A}$) denotes the **twist map** defined as $\tau(a \otimes b) = b \otimes a$.

Here is the usual definition of K-algebra.

Definition 2.2.2. A K-algebra is a set A endowed with a sum, a multiplication and a scalar multiplication by elements in K such that

1. A is a unitary ring with the sum and the multiplication,
2. A is a K-vector space with the sum and the scalar multiplication,
3. The following relation between the multiplication (of the ring) and scalar multiplication (of the vector space) is satisfied

$$r(ab) = (ra)b = a(rb), \forall\ r \in K,\ a, b \in A. \tag{2.3}$$

Our first task is to show that we really do not have a new definition of K-algebra.

Proposition 2.2.3. *Both definitions of K-algebras are equivalent.*

Proof. Let A be a K-algebra as in Definition 2.2.2. We already have that A is a K-vector space. We will first show that there exists a K-linear map m_A satisfying the associative property. We consider the multiplication in the ring: $A \times A \to A$, $(a, b) \mapsto ab$, which is K-bilinear (due to (2.3) and the distributive properties of multiplication on A). Since $A \otimes A$ is a tensor product, there exists a unique K-linear map $m_A : A \otimes A \to A$ defined as $m_A(\sum a \otimes b) = \sum m_A(a \otimes b) = \sum ab$. Thus, the associative property of the multiplication on A implies that (2.1) holds:

$$\begin{aligned} &m_A(I_A \otimes m_A)(a \otimes b \otimes c) = m_A(m_A \otimes I_A)(a \otimes b \otimes c) \Leftrightarrow \\ &\Leftrightarrow m_A(I_A(a) \otimes m_A(b \otimes c)) = m_A(m_A(a \otimes b) \otimes I_A(c)) \Leftrightarrow \\ &\Leftrightarrow m_A(a \otimes (bc)) = m_A((ab) \otimes c) \Leftrightarrow a(bc) = (ab)c = abc. \end{aligned}$$

Then, we have obtained

$$m_A(I_A \otimes m_A)(a \otimes b \otimes c) = m_A(m_A \otimes I_A)(a \otimes b \otimes c) \Leftrightarrow a(bc) = abc = (ab)c \tag{2.4}$$

We next show that there exists a K-linear map λ_A satisfying the unit property. We define $\lambda_A : K \to A$ as $\lambda_A(r) = r1_A$. Since scalar multiplication is distributive with respect to scalar addition, λ_A preserves addition, and since scalar multiplication is associative, it preserves scalar multiplication. Thus λ_A is linear. Finally, the formula (2.3) implies that Condition (2.2) holds:

$$\begin{cases} m_A(I_A \otimes \lambda_A)(a \otimes r) = m_A(a \otimes \lambda_A(r)) = a\lambda_A(r) = a(r1_A) = r(a1_A) = ra, \\ m_A(\lambda_A \otimes I_A)(r \otimes a) = m_A(\lambda_A(r) \otimes a) = \lambda_A(r)a = (r1_A)a = r(1_Aa) = ra, \end{cases}$$

We conclude that (A, m_A, λ_A) is a K-algebra.

Conversely, suppose that (A, m_A, λ_A) is a K-algebra as in Definition 2.2.1. We already have that A is a K-vector space. We see that it is a ring with unity, with

addition given by vector addition. We define multiplication on A as $ab = m_A(a \otimes b)$. It is associative by (2.1) and it is distributive with respect to addition by linearity. From (2.2) we obtain the unity: $1_A = \lambda_A(1_K)$, and so, A is a ring with unity.

Finally, we show that the relation between multiplication and scalar multiplication holds by linearity of m_A: for $a, b \in A, r \in K$,

$$\begin{cases} r(ab) = rm_A(a \otimes b) = m_A(ra \otimes b) = (ra)b, \\ r(ab) = rm_A(a \otimes b) = m_A(a \otimes rb) = a(rb), \end{cases}$$

We conclude that A is a K-algebra in the sense of Definition 2.2.2. □

We do some remarks about maps of algebras. Let (A, m_A, λ_A) be a K-algebra.

Remark 2.2.4. From now on, we will write $m_A(a \otimes b) = ab$, for all $a, b \in A$, and $\lambda_A(r) = r1_A$, for all $r \in K$.

Remark 2.2.5. Since K is a field and λ_A maps 1_K to 1_A, it is injective, and so $\ker(\lambda_A) = 0$. Therefore, by the isomorphism theorem, $K/ker(\lambda_A) \cong \lambda_A(K)$. Hence, the image $\lambda_A(K)$ is isomorphic to K. Thus, A contains a copy of K through the identification $r = r1$. The unit map can be given by $\lambda_A(r) = r$.

Example 2.2.6. The field K as a vector space over itself is a commutative K-algebra with multiplication map $m_K : K \otimes K \to K$ given by $m_K(r \otimes s) = rs$, and unit map $\lambda_K : K \to K$ defined as $\lambda_K(r) = r$. It is called the **trivial K-algebra**.

Example 2.2.7. The polynomial ring $K[x]$ is a commutative K-algebra with multiplication map $m_{K[x]} : K[x] \otimes K[x] \to K[x]$ given by the usual polynomial multiplication and unit map $\lambda_{K[x]} : K \to K[x]$ defined as $\lambda_{K[x]}(r) = r1$.

Example 2.2.8. Let G be a finite group with identity element 1. The group ring $K[G] = \left\{ \sum_{g \in G} r_g g \ : \ r_g \in K \right\}$ is a K-algebra called the **group algebra**.
Multiplication map $m_{K[G]} : K[G] \otimes K[G] \to K[G]$ is given by $m_{K[G]}(g \otimes h) = gh$, and unit map $\lambda_{K[G]} : K \to K[G]$ is defined as $\lambda_{K[G]}(r) = r1$. Clearly, $K[G]$ is commutative if, and only if, G is abelian.

Example 2.2.9. Let $L = K(\alpha)$ be a simple algebraic extension of K. Then L is a commutative K-algebra with multiplication map $m_L : L \otimes L \to L$ given by multiplication in the field L and unit map $\lambda_L : K \to L$ defined as $\lambda_L(r) = r$.

Example 2.2.10. We generalise the previous example. Let K be a subfield of a field L. Then L is a commutative K-algebra with multiplication map $m_L : L \otimes L \to L$ given by multiplication in the field L and unit map $\lambda_L : K \to L$ defined as $\lambda_L(r) = r$.

Definition 2.2.11. Let A, B be K-algebras. The **tensor product of algebras** $A \otimes B$ has the structure of a K-algebra with multiplication map given by

$$\begin{array}{rccl} m_{A \otimes B} : & (A \otimes B) \otimes (A \otimes B) & \to & A \otimes B \\ & (a \otimes b) \otimes (c \otimes d) & \mapsto & (m_A \otimes m_B)(I_A \otimes \tau \otimes I_B)(a \otimes (b \otimes c) \otimes d) \end{array}$$

that is,

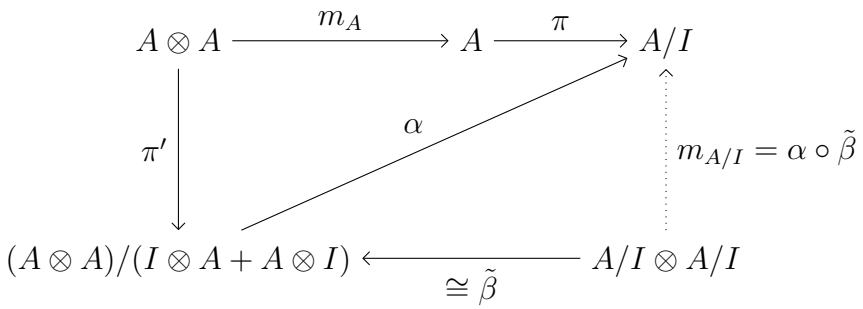
$$m_{A\otimes B}((a\otimes b)\otimes(c\otimes d)) = (m_A\otimes m_B)(I_A\otimes\tau\otimes I_B)(a\otimes(b\otimes c)\otimes d) =$$
$$= (m_A\otimes m_B)(a\otimes(c\otimes b)\otimes d) = ac\otimes bd,$$

and unit map defined as

$$\begin{array}{rccc} \lambda_{A\otimes B}: & K & \to & A\otimes B \\ & r & \mapsto & \lambda_A(r)\otimes 1_B \end{array}$$

Proposition 2.2.12. *Let A be a K-algebra and let I be an ideal of A. Then the quotient space A/I is a K-algebra.*

Proof. We need to define a multiplication map $m_{A/I}$ and a unit map $\lambda_{A/I}$. We will start with multiplication. The following diagram illustrates the idea of the proof:



Let $\pi : A \to A/I$ denote the canonical surjection. The composition $\pi\circ m_A$ is a K-linear map (since π and m_A are also linear) defined as $(\pi\circ m_A)(a\otimes b) = \pi(ab) = [ab]_I$. Note that $I\otimes A + A\otimes I$ is a subspace of $A\otimes A$. Since I is an ideal, $m_A(i\otimes a + b\otimes j) = m_A(i\otimes a) + m_A(b\otimes j) = ia + bj \in I, \forall\ i,j\in I, a,b\in A$, and so, $I\otimes A + A\otimes I \subseteq \ker(\pi\circ m_A)$. Let $\pi' : A\otimes A \to (A\otimes A)/(I\otimes A + A\otimes I)$ denote the canonical surjection. By the universal property of the quotient module, there exists a unique K-linear map $\alpha : (A\otimes A)/(I\otimes A + A\otimes I) \to A/I$ defined as $\alpha([a\otimes b]_{I\otimes A+A\otimes I}) = [ab]_I$.

By Proposition 2.1.5, there is a K-linear isomorphism $\tilde{\beta}$ between $A/I\otimes A/I$ and $(A\otimes A)/(I\otimes A + A\otimes I)$, defined as $\tilde{\beta}([a]_I\otimes[b]_I) = [a\otimes b]_{I\otimes A+A\otimes I}$. Therefore, let $m_{A/I} = \alpha\circ\tilde{\beta}$

$$\begin{array}{rccc} m_{A/I}: & A/I\otimes A/I & \to & A/I \\ & [a]_I\otimes[b]_I & \mapsto & [ab]_I \end{array}$$

It is easy to check that $m_{A/I}$ satisfies the associative property since m_A does.

Finally, we define the unit map as the composition of the unit map of A and the canonical surjection: $\lambda_{A/I} = \pi\circ\lambda_A$. It is easy to check that it satisfies the unit property since λ_A does. □

Definition 2.2.13. Let A be a K-algebra and let I be an ideal of A. The K-algebra A/I of the previous proposition is the **quotient algebra** of A by I.

Definition 2.2.14. Let (A, m_A, λ_A), (B, m_B, λ_B) be K-algebras. A K-**algebra homomorphism** from A to B is a map $\phi : A \to B$ that verifies:

1. $\phi(a+b) = \phi(a) + \phi(b)$, for all $a, b \in A$,
2. $\phi(m_A(a \otimes b)) = m_B(\phi(a) \otimes \phi(b)) \Leftrightarrow \phi(ab) = \phi(a)\phi(b)$, for all $a, b \in A$,
3. $\phi(\lambda_A(r)) = \lambda_B(r) \Leftrightarrow \phi(r1_A) = r1_B$, for all $r \in K$.

The first condition means that ϕ is a group homomorphism and, with the last two ones, it implies that it is a K-linear map: indeed, for all $a \in A, r \in K$,

$$\phi(ra) = \phi(r1_A a) \underset{(2)}{=} \phi(r1_A)\phi(a) \underset{(3)}{=} r1_B\phi(a) = r\phi(a).$$

A K-algebra homomorphism that is injective and surjective is a K-**algebra isomorphism**.

We will now describe objects that are dual (in some sense) to algebras; essentially forming them by reversing the arrows in the structure maps for algebras. These objects are called coalgebras.

Let C be a K-vector space.

Definition 2.2.15. A K-**coalgebra** is a triple $(C, \Delta_C, \varepsilon_C)$ consisting of a K-vector space and K-linear maps $\Delta_C : C \to C \otimes C$ and $\varepsilon_C : C \to K$ that satisfy the following conditions:

1. The diagram commutes

$$\begin{array}{ccc} C & \xrightarrow{\Delta_C} & C \otimes C \\ \Big\downarrow{\scriptstyle \Delta_C} & & \Big\downarrow{\scriptstyle I_C \otimes \Delta_C} \\ C \otimes C & \xrightarrow{\Delta_C \otimes I_C} & C \otimes C \otimes C \end{array}$$

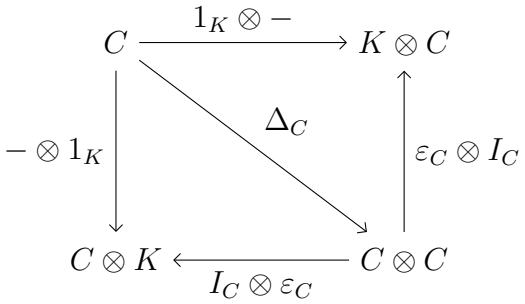
   where the map $I_C : C \to C$ is the identity map on C.

   Equivalently, we have for all $c \in C$,

$$(I_C \otimes \Delta_C)\Delta_C(c) = (\Delta_C \otimes I_C)\Delta_C(c) \tag{2.5}$$

   The map Δ_C is called the **comultiplication map** and Condition (2.4) is the **coassociative property**.

2. The diagram commutes



where the map $1_K \otimes - : C \to K \otimes C$ is defined by $c \mapsto 1_K \otimes c$ and the map $- \otimes 1_K : C \to C \otimes K$ is defined by $c \mapsto c \otimes 1_K$.

Equivalently, we have for all $c \in C$,

$$(\varepsilon_C \otimes I_C)\Delta_C(c) = 1_K \otimes c, \quad (I_C \otimes \varepsilon_C)\Delta_C(c) = c \otimes 1_K \tag{2.6}$$

The map ε_C is called the **counit map** and Condition (2.5) is the **counit property**.

The K-coalgebra C is **cocommutative** if $\tau\Delta_C = \Delta_C$.

We will now introduce **Sweedler notation** to write the image of comultiplication map. Sweedler notation is a special notation for discussion of operations in coalgebras. Let C be a K-coalgebra. For $c \in C$, Δ_C maps c to an element in $C \otimes C$, which is a sum of the form $\sum_{i=1}^{n} a_i \otimes b_i$.

Sweedler suggests not to make up new symbols like a and b, but rather use composed symbols $c_{(1)}$ and $c_{(2)}$. Therefore $\Delta_C(c) = \sum_{i=1}^{n} c_{(1)i} \otimes c_{(2)i}$.

Sweedler notation means that for certain manipulations involving just generic linear operations we actually do not need to think of the summation symbol i, so we can just write $\Delta_C(c) = \sum_{(c)} c_{(1)} \otimes c_{(2)}$.

We write the coassociative property using this notation. On the one hand,

$$(I_C \otimes \Delta_C)\Delta_C(c) = (I_C \otimes \Delta_C)\left(\sum_{(c)} c_{(1)} \otimes c_{(2)}\right) = \sum_{(c)} c_{(1)} \otimes \Delta_C(c_{(2)}) =$$

$$= \sum_{(c,c_{(2)})} c_{(1)} \otimes c_{(2)_{(1)}} \otimes c_{(2)_{(2)}} \tag{2.7}$$

On the other hand,

$$(\Delta_C \otimes I_C)\Delta_C(c) = (\Delta_C \otimes I_C)\Big(\sum_{(c)} c_{(1)} \otimes c_{(2)}\Big) = \sum_{(c)} \Delta_C(c_{(1)}) \otimes c_{(2)} =$$

$$= \sum_{(c,c_{(1)})} c_{(1)_{(1)}} \otimes c_{(1)_{(2)}} \otimes c_{(2)} \tag{2.8}$$

By the coassociative property, $(I_C \otimes \Delta_C)\Delta_C = (\Delta_C \otimes I_C)\Delta_C$. So, the expressions in (2.7) and (2.8) are equal. This common value is denoted as $\sum_{(c)} c_{(1)} \otimes c_{(2)} \otimes c_{(3)}$.

Likewise, we write the counit property using this notation. Note first that the scalar multiplication on C defines two maps $s_1 : K \otimes C \to C$ with $r \otimes c \mapsto rc$ and $s_2 : C \otimes K \to C$ with $c \otimes r \mapsto rc, \forall\ c \in C, r \in K$. Since $s_1(1 \otimes c) = c = s_2(c \otimes 1)$, the counit property (2.6) implies

$$s_1(\varepsilon_C \otimes I_C)\Delta_C(c) = c = s_2(I_C \otimes \varepsilon_C)\Delta_C(c), \forall\ c \in C, \tag{2.9}$$

that is to say,

$$c = s_1(\varepsilon_C \otimes I_C)\Delta_C(c) = s_1(\varepsilon_C \otimes I_C)\Big(\sum_{(c)} c_{(1)} \otimes c_{(2)}\Big) = s_1\Big(\sum_{(c)} \varepsilon_C(c_{(1)}) \otimes c_{(2)}\Big) =$$
$$= \sum_{(c)} \varepsilon_C(c_{(1)})c_{(2)},$$

$$c = s_2(I_C \otimes \varepsilon_C)\Delta_C(c) = s_2(I_C \otimes \varepsilon_C)\Big(\sum_{(c)} c_{(1)} \otimes c_{(2)}\Big) = s_2\Big(\sum_{(c)} c_{(1)} \otimes \varepsilon_C(c_{(2)})\Big) =$$
$$= \sum_{(c)} c_{(1)}\varepsilon_C(c_{(2)}) = \sum_{(c)} \varepsilon_C(c_{(2)})c_{(1)}.$$

All in all, we have obtained:

$$\sum_{(c)} \varepsilon_C(c_{(1)})c_{(2)} = c = \sum_{(c)} \varepsilon_C(c_{(2)})c_{(1)} \tag{2.10}$$

Example 2.2.16. The field K as a vector space over itself is a cocommutative K-coalgebra with comultiplication map $\Delta_K : K \to K \otimes K$ given by $\Delta_K(r) = r \otimes 1$, and counit map $\varepsilon_K : K \to K$ defined as $\varepsilon_K(r) = r$. It is called the **trivial K-coalgebra**.

In the next examples of a coalgebra C, Δ_C and ε_C are defined on basic elements and extended by linearity to the whole C.

Example 2.2.17. Let x be an indeterminate and let $C = K \oplus Kx$ be the direct sum of vector spaces, where $Kx = \{rx : r \in K\}$. The canonical basis is $\{1, x\}$. Then C is a K-coalgebra with comultiplication map $\Delta_C : C \to C \otimes C$ given by $\Delta_C(1) = 1 \otimes 1$, $\Delta_C(x) = x \otimes x$, and counit map $\varepsilon_C : C \to K$ defined as $\varepsilon_C(1) = \varepsilon_C(x) = 1$.

Example 2.2.18. Let x be an indeterminate and we consider $C = K \oplus Kx$, where the canonical basis is $\{1, x\}$. Then C is a K-coalgebra with comultiplication map $\Delta_C : C \to C \otimes C$ given by $\Delta_C(1) = 1 \otimes 1,\ \Delta_C(x) = 1 \otimes x + x \otimes 1$, and counit map $\varepsilon_C : C \to K$ defined as $\varepsilon_C(1) = 1,\ \varepsilon_C(x) = 0$.

Example 2.2.19. Let V denote an n-dimensional K-vector space with basis $\mathcal{B} = \{b_1, \ldots, b_n\}$. Then V is a cocommutative K-coalgebra with comultiplication map $\Delta_V : V \to V \otimes V$ given by $\Delta_V(b_i) = b_i \otimes b_i$, and counit map $\varepsilon_V : V \to K$ defined as $\varepsilon_V(b_i) = 1$, for all $i \in \{1, \ldots, n\}$.

Example 2.2.20. Let G be a finite group. The group ring $K[G]$ (defined as in Example 2.2.8) is a cocommutative K-coalgebra called the **group coalgebra**. Comultiplication map $\Delta_{K[G]} : K[G] \to K[G] \otimes K[G]$ is given by $\Delta_{K[G]}(g) = g \otimes g$, and counit map $\varepsilon_{K[G]} : K[G] \to K$ is defined as $\varepsilon_{K[G]}(g) = 1_K$.

Example 2.2.21. Let $K[x]$ be the K-vector space of polynomials in the indeterminate x, where the canonical basis is $\{1, x, x^2, \ldots\}$. Then $K[x]$ is a cocommutative K-coalgebra with comultiplication map $\Delta_{K[x]} : K[x] \to K[x] \otimes K[x]$ given by $\Delta_{K[x]}(x^m) = x^m \otimes x^m$, and counit map $\varepsilon_{K[x]} : K[x] \to K$ defined as $\varepsilon_{K[x]}(x^m) = 1$.

Example 2.2.22. Let $K[x]$ be the K-vector space of polynomials in the indeterminate x, where the canonical basis is $\{1, x, x^2, \ldots\}$. Then $K[x]$ is a cocommutative K-coalgebra with comultiplication map $\Delta_{K[x]} : K[x] \to K[x] \otimes K[x]$ given by $\Delta_{K[x]}(x^m) = \sum_{i=1}^{n} \binom{m}{i} x^i \otimes x^{m-i}$, and counit map $\varepsilon_{K[x]} : K[x] \to K$ defined as $\varepsilon_{K[x]}(x^m) = \delta_{0,m}$. It is called the **divided power coalgebra**.

Definition 2.2.23. Let C, D be K-coalgebras. The **tensor product of coalgebras** $C \otimes D$ has the structure of a K-coalgebra with comultiplication map given by

$$\begin{array}{rccl} \Delta_{C\otimes D}: & C \otimes D & \to & (C \otimes D) \otimes (C \otimes D) \\ & c \otimes d & \mapsto & (I_C \otimes \tau \otimes I_D)(\Delta_C \otimes \Delta_D)(c \otimes d) \end{array}$$

that is,

$$\Delta_{C\otimes D}(c \otimes d) = (I_C \otimes \tau \otimes I_D)(\Delta_C \otimes \Delta_D)(c \otimes d) = (I_C \otimes \tau \otimes I_D)(\Delta_C(c) \otimes \Delta_D(d)) =$$
$$= (I_C \otimes \tau \otimes I_D)\left(\sum_{(c,d)} c_{(1)} \otimes c_{(2)} \otimes d_{(1)} \otimes d_{(2)}\right) = \sum_{(c,d)} (c_{(1)} \otimes d_{(1)}) \otimes (c_{(2)} \otimes d_{(2)}),$$

and counit map defined as

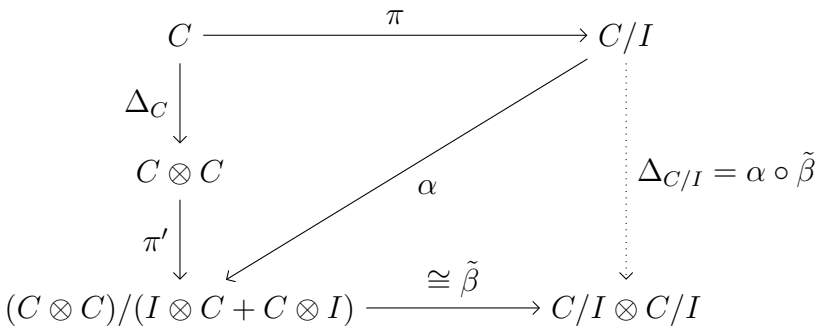
$$\begin{array}{rccl} \varepsilon_{C\otimes D}: & C \otimes D & \to & K \\ & c \otimes d & \mapsto & (\varepsilon_C \otimes \varepsilon_D)(c \otimes d) = \varepsilon_C(c)\varepsilon_D(d) \end{array}$$

We next discuss the analog of an ideal in a ring for a coalgebra.

Definition 2.2.24. Let C be a K-coalgebra. A subspace $I \subseteq C$ is a **coideal** of C if $\Delta_C(I) \subseteq I \otimes C + C \otimes I$ and $\varepsilon_C(I) = 0$ (that is, $I \subseteq \ker(\varepsilon_C)$).

Proposition 2.2.25. *Let C be a K-coalgebra and let I be a coideal of C. Then the quotient space C/I is a K-coalgebra.*

Proof. We need to define a comultiplication $\Delta_{A/I}$ and a unit $\varepsilon_{A/I}$. We will start with comultiplication. The following diagram illustrates the idea of the proof:



Let $\pi : C \to C/I$ denote the canonical surjection. Note that $I \otimes C + C \otimes I$ is a subspace of $C \otimes C$. Let $\pi' : C \otimes C \to (C \otimes C)/(I \otimes C + C \otimes I)$ denote the canonical surjection, and consider the composition $\pi' \circ \Delta_C$, which is a K-linear map (since π' and Δ_C are also linear).

Since I is a coideal, $\Delta_C(I) \subseteq I \otimes C + C \otimes I$, and so $I \subseteq \ker(\pi' \circ \Delta_C)$. By the universal property of the quotient module, there exists a unique K-linear map $\alpha : C/I \to (C \otimes C)/(I \otimes C + C \otimes I)$ defined as $\alpha([c]_I) = [\Delta_C(c)]_{I \otimes C + C \otimes I}$.

By Proposition 2.1.5, there is a K-linear isomorphism $\tilde{\beta}$ between the space $(C \otimes C)/(I \otimes C + C \otimes I)$ and $C/I \otimes C/I$, defined as $\tilde{\beta}([c \otimes d]_{I \otimes C + C \otimes I}) = [c]_I \otimes [d]_I$. Therefore, let $\Delta_{C/I} = \alpha \circ \tilde{\beta}$

$$\begin{array}{rccl} \Delta_{C/I} : & C/I & \to & C/I \otimes C/I \\ & [c]_I & \mapsto & \displaystyle\sum_{(c)} [c_{(1)}]_I \otimes [c_{(2)}]_I \end{array}$$

It is easy to check that $\Delta_{C/I}$ satisfies the coassociative property since Δ_C does.

Finally, since I is a coideal of A, $I \subseteq \ker(\varepsilon)$. Moreover, since π is the canonical surjection, by the universal property of the module quocient, there exists a unique K-linear map $\varepsilon_{C/I} : C/I \to K$ defined as $\varepsilon_{C/I}([c]_I) = \varepsilon_C(c)$. It is easy to check that it satisfies the counit property since ε_C does. □

Definition 2.2.26. Let C be a K-coalgebra and let I be a coideal of C. The K-coalgebra C/I of the previous proposition is the **quotient coalgebra** of C by I.

Definition 2.2.27. Let C be a K-coalgebra. A non-zero element $c \in C$ for which $\Delta_C(c) = c \otimes c$ is a **grouplike element** of C.

Proposition 2.2.28. *Let c be a grouplike element of a K-coalgebra C. Then it satisfies $\varepsilon_C(c) = 1$.*

Proof. Since c is grouplike,

$$1c = c \underset{(2.9)}{=} s_1(\varepsilon_C \otimes I_C)\Delta_C(c) = s_1(\varepsilon_C \otimes I_C)(c \otimes c) = s_1(\varepsilon_C(c) \otimes c) = \varepsilon_C(c)c \Rightarrow$$
$$\Rightarrow \varepsilon_C(c)c = 1c \Rightarrow (\varepsilon_C(c) - 1)c = 0.$$

Moreover, since K is a field and $c \neq 0$ (as it is a grouplike element), $\varepsilon_C(c)-1 = 0$, and hence $\varepsilon_C(c) = 1$. □

For instance, in Example 2.2.19, the grouplike elements of V are precisely those in the basis $\mathcal{B}$, and in Example 2.2.21, the grouplike elements of $K[x]$ are $1, x, x^2, \ldots$.

Proposition 2.2.29. *Let $K[x]$ be the divided power coalgebra. Then 1 is the only grouplike element.*

Proof. Recall that $K[x]$ is the coalgebra of Example 2.2.22, with comultiplication given by $\Delta_{K[x]}(x^m) = \sum_{i=1}^{n} \binom{m}{i} x^i \otimes x^{m-i}$, and counit defined as $\varepsilon_{K[x]}(x^m) = \delta_{0,m}$. Suppose $a_0 + a_1x + \cdots + a_nx^n$ is grouplike. By Proposition 2.2.28, we have

$$1 = \varepsilon_{K[x]}(a_0x^0 + a_1x + \cdots + a_nx^n) = a_0\ \varepsilon_{K[x]}(x^0) + a_1\ \varepsilon_{K[x]}(x) + \cdots + a_n\ \varepsilon_{K[x]}(x^n) =$$
$$= a_0\ 1 + a_1\ 0 + \cdots + a_n\ 0 = a_0 \Rightarrow a_0 = 1.$$

On the one hand, since $1 + a_1x + \cdots + a_nx^n$ is a grouplike element,

$$\Delta_{K[x]}(1 + a_1x + \cdots + a_nx^n) = (1 + a_1x + \cdots + a_nx^n) \otimes (1 + a_1x + \cdots + a_nx^n).$$

On the other hand, since $\Delta_{K[x]}$ is K-linear,

$$\Delta_{K[x]}(1x^0 + a_1x + \cdots + a_nx^n) = \Delta_{K[x]}(x^0) + a_1\ \Delta_{K[x]}(x) + \cdots + a_n\ \Delta_{K[x]}(x^n) =$$
$$= 1 \otimes 1 + a_1(1 \otimes x + x \otimes 1) + \cdots + a_n \sum_{i=0}^{n} \binom{n}{i} x^i \otimes x^{n-i}.$$

Note that $\{x^i \otimes x^j\}_{0 \leq i,j \leq n}$ is a linearly independent subset of $K[x] \otimes K[x]$. Developing the first equality, there is the term $a_nx^n \otimes a_nx^n = a_n^2(x^n \otimes x^n)$. If we define the degree of a term $x^i \otimes x^j$ as $i + j$, then our term has degree $2n$. As there is no term of degree bigger than n in the second equality, thus $a_n^2 = 0$, and so $a_n = 0$. Therefore, we have $\Delta_{K[x]}(1 + a_1x + \cdots + a_nx^n) = (1 + a_1x + \cdots + a_{n-1}x^{n-1}) \otimes (1 + a_1x + \cdots + a_{n-1}x^{n-1})$. Repeating the argument, we obtain $a_i^2 = 0$, and hence $a_i = 0$, for all $i \in \{1, \ldots, n\}$. □

Proposition 2.2.30. *Let C be a K-coalgebra and let $G(C)$ denote the set of grouplike elements of C. Then $G(C)$ is a linearly independent subset of C.*

Proof. If $G(C) = \emptyset$, then $G(C)$ is clearly linearly independent. If $G(C)$ contains exactly one grouplike element, then this element is non-zero, and so $G(C)$ is linearly independent. Thus, we assume that $G(C)$ contains at least two elements.

Reduction to absurdity. Suppose that $G(C)$ is linearly dependent. Let $m \geq 1$ be the largest integer for which $S = \{g_1, \ldots, g_m\}$ is a linearly independent subset of $G(C)$. Then $G(C) \setminus S \neq \emptyset$ (else $G(C)$ is linearly independent). Let $g \in G(C) \setminus S$. There exist scalars $r_i \in K$ such that $g = r_1 g_1 + \cdots + r_m g_m$. Since g is grouplike, $g \neq 0$, and so, there exists at least one $i \in \{1, \ldots, m\}$ for which $r_i \neq 0$.

On the one hand, since g is a grouplike element,

$$\Delta_C(g) = g \otimes g = \sum_{i=1}^{m} \sum_{j=1}^{m} r_i r_j (g_i \otimes g_j).$$

On the other hand, since Δ_C is K-linear and g_i are grouplike elements,

$$\Delta_C(g) = \Delta_C\left(\sum_{i=1}^{m} r_i g_i \right) = \sum_{i=1}^{m} r_i \Delta_C(g_i) = \sum_{i=1}^{m} r_i g_i \otimes g_i.$$

All in all, we have obtained $\displaystyle\sum_{i=1}^{m} \sum_{j=1}^{m} r_i r_j (g_i \otimes g_j) = \sum_{i=1}^{m} r_i g_i \otimes g_i.$

Note that $\{g_i \otimes g_j\}_{1 \leq i,j \leq m}$ is a linearly independent subset of $C \otimes C$. Since at the right side of the last equality there are no terms of the form $g_i \otimes g_j$, with $i \neq j$, then $r_i r_j = 0, \forall\ i \neq j$. Thus

$$\sum_{i=1}^{m} r_i^2 (g_i \otimes g_i) = \sum_{i=1}^{m} r_i (g_i \otimes g_i) \Rightarrow r_i^2 = r_i, \forall\ i \in \{1, \ldots, m\}.$$

For any $r_i \neq 0$, one has $r_j = 0, \forall\ j \neq i$ (since K is a field and $r_i r_j = 0$), and hence $r_i \neq 0$ for exactly one i. For this i, $r_i^2 = r_i$ implies $r_i = 1$. Therefore, $g = g_i$, which contradicts our choice of g. We conclude that $G(C)$ is linearly independent. □

Definition 2.2.31. Let $(C, \Delta_C, \varepsilon_C)$, $(D, \Delta_D, \varepsilon_D)$ be K-coalgebras. A K-**coalgebra homomorphism** from C to D is a map $\phi : A \to B$ that verifies:

1. ϕ is K-linear,
2. $(\phi \otimes \phi)\Delta_C(c) = \Delta_D(\phi(c))$, for all $c \in C$,
3. $\varepsilon_C(c) = \varepsilon_D(\phi(c))$, for all $c \in C$.

A K-coalgebra homomorphism that is injective and surjective is a K-**coalgebra isomorphism**.

Proposition 2.2.32. *Let C be a K-coalgebra. Then the counit map $\varepsilon_C : C \to K$ is a K-coalgebra homomorphism.*

Proof. Recall that in Example 2.2.16, we have seen that K is the trivial coalgebra with comultiplication given by $\Delta_K(r) = r \otimes 1$, and counit defined as $\varepsilon_K(r) = I_K(r) = r$. Moreover, note that $\varepsilon_C \otimes \varepsilon_C = (\varepsilon_C \otimes I_K)(I_C \otimes \varepsilon_C)$ trivially holds.

Let $c \in C$. We need to prove that ε_C satifies the two properties of the definition of coalgebra homomorphism. On the one hand, we have

$$(\varepsilon_C \otimes \varepsilon_C)\Delta_C(c) = (\varepsilon_C \otimes I_K)(I_C \otimes \varepsilon_C)\Delta_C(c) \underset{(2.6)}{=} (\varepsilon_C \otimes I_K)(c \otimes 1) = \\ = \varepsilon_C(c) \otimes 1 = \Delta_K(\varepsilon_C(c)).$$

On the other hand, we have $\varepsilon_C(c) = I_K(\varepsilon_C(c)) = \varepsilon_K(\varepsilon_C(c))$. Therefore, we conclude that ε_C is a K-coalgebra homomorphism. □

Proposition 2.2.33. *Let $\phi : C \to D$ be a homomorphism of K-coalgebras. If $c \in C$ is a grouplike element, then $\phi(c) \in D$ is a grouplike element.*

Proof. Since ϕ is a coalgebra homomorphism, $(\phi \otimes \phi)\Delta_C(a) = \Delta_D(\phi(a))$ holds for every $a \in C$. Since c is a grouplike element of C, it satisfies $\Delta_C(c) = c \otimes c$. Thus,

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

Hence, $\phi(c)$ is a grouplike element of D. □

2.3 Duality

We next consider the linear duals of algebras and coalgebras. There are two main results. The first one, which is easier to prove, is that if C is a coalgebra, then C^* is an algebra, where multiplication and unit maps are induced from the transpose of comultiplication and counit maps, respectively. But the converse of this statement is not true in general. In order to have the reciprocal result, we need to replace the dual space A^* with a certain subspace A° called the finite dual. Thus, the second important result is that if A is an algebra, then A° is coalgebra. Finally, as an application, we show that the finite dual $K[x]^\circ$ can be identified with the collection of linearly recursive sequences of all orders over K.

Let C be a K-coalgebra and let C^* be its linear dual.

Remark 2.3.1. For every field E and every E-vector space V, there exists the following K-vector space isomorphism

$$E \otimes_E V \cong V \ (\cong V \otimes_E E) \tag{2.11}$$

given by $r \otimes v \mapsto rv$, and $v \mapsto 1_E \otimes v$, for all $v \in V$, $r \in E$.

Theorem 2.3.2. *If C is a K-coalgebra, then C^* is a K-algebra.*

Proof. Recall that C is a triple $(C, \Delta_C, \varepsilon_C)$, where $\Delta_C : C \to C \otimes C$ is K-linear and satisfies the coassociative property and $\varepsilon_C : C \to K$ is K-linear and satisfies the counit property. We need to define a multiplication map m_{C^*} and a unit map λ_{C^*}.

We start considering the transpose of Δ_C, $\Delta_C^* : (C \otimes C)^* \to C^*$, which is a K-linear map defined as $\Delta_C^*(\psi) = \psi \circ \Delta_C$. Since $C^* \otimes C^* \subseteq (C \otimes C)^*$ (by Corollary 2.1.9), Δ_C^* restricts to a K-linear map

$$\begin{array}{rccl} m_{C^*} : & C^* \otimes C^* & \to & C^* \\ & f \otimes g & \mapsto & m_{C^*}(f \otimes g) = \Delta_C^*(f \otimes g) \end{array}$$

Now, we consider the transpose of ε_C, $\varepsilon_C^* : K^* \cong K \to C^*$, which is a K-linear map given by $\varepsilon_C^*(r) = r\varepsilon_C$. Set $\lambda_{C^*} = \varepsilon_C^*$. Observe that if we dualize the commutative diagrams of the definition of the coalgebra C, we obtain the commutative diagrams of the definition of the algebra C^*

$$\begin{array}{ccc} C^* & \xleftarrow{\quad m_{C^*} \quad} & C^* \otimes C^* \\ \uparrow{\scriptstyle m_{C^*}} & & \uparrow{\scriptstyle I_{C^*} \otimes m_{C^*}} \\ C^* \otimes C^* & \xleftarrow[m_{C^*} \otimes I_{C^*}]{} & C^* \otimes C^* \otimes C^* \end{array} \qquad , \qquad \begin{array}{ccc} C & \xleftarrow{\quad s_1 \quad} & K \otimes C \\ \uparrow{\scriptstyle s_2} & \nwarrow{\scriptstyle m_{C^*}} & \downarrow{\scriptstyle \lambda_{C^*} \otimes I_{C^*}} \\ C \otimes K & \xrightarrow{I_{C^*} \otimes \lambda_{C^*}} & C \otimes C \end{array}$$

It remains to show that $(1_K \otimes -)^* = s_1$ and $(- \otimes 1_K)^* = s_2$: indeed, for $f \in C^*$, $c \in C$, $r \in K$, we have

$$(1_K \otimes -)^*(r \otimes f)(c) = (r \otimes f)(1_K \otimes -)(c) = (r \otimes f)(1_K \otimes c) =$$
$$\underset{(K \cong K^*)}{=} r \otimes f(c) \underset{(2.11)}{=} rf(c) = (rf)(c) = s_1(r \otimes f)(c).$$

Similarly, one has $(- \otimes 1_K)^* = s_2$. Hence, $(C^*, m_{C^*}, \lambda_{C^*})$ is a K-algebra. □

We have just seen that if C is a coalgebra, then C^* is an algebra. Then if A is an algebra, we may wonder if A^* is a coalgebra. It is not true in general because the transpose of the multiplication map $m_A : A \otimes A \to A$ is $m_A^* : A^* \to (A \otimes A)^*$, where $A^* \otimes A^*$ is a proper subset of $(A \otimes A)^*$ if A is infinite dimensional over K. Therefore, m_A^* may not induce the required comultiplication map in A^*. In order for the transpose m_{A^*} to serve as a comultiplication map we need to replace A^* with a certain subspace of A^* called the finite dual.

Definition 2.3.3. Let A be a K-algebra. We already know that A is a vector space over K and a ring. An **ideal** I of A is **cofinite** if the quotient space A/I is finite dimensional.

Definition 2.3.4. Let A be a K-algebra. The **finite dual** A° of A is the following subspace of A: $A^\circ = \{f \in A^* : f(I) = 0 \text{ for some ideal } I \subseteq A \text{ cofinite}\}$.

Example 2.3.5. Let $\varphi_i \in K[x]^*$ be defined as $\varphi_i(x^j) = \delta_{i,j}$, for $i, j \geq 0$. Since φ_i clearly vanishes on the ideal (x^{i+1}) and $\dim(K[x]/(x^{i+1})) = i + 1$ (because $\{1, x, \ldots, x^i\}$ is a basis), then $\varphi_i \in K[x]^\circ$.

Proposition 2.3.6. *If A is finite dimensional as a K-vector space, then $A^\circ = A^*$.*

Proof. Since always $A^\circ \subseteq A^*$, it suffices to prove that $A^* \subseteq A^\circ$. Let $f \in A^*$, and we consider the ideal 0. It satisfies that $0 \subseteq A$, $A/0 = A$ is finite dimensional (by hypothesis) and $f(0) = 0$ (since f is linear). Thus $f \in A^\circ$. Consequently, $A^* \subseteq A^\circ$, and we conclude that $A^\circ = A^*$. □

In order to prove that if A is an algebra, A° is a coalgebra, we need three results.

Lemma 2.3.7. *Let I be an ideal of A and let $\pi : A \to A/I$ be the canonical surjection of vector spaces. Let $\pi^* : (A/I)^* \to A^*$ be the transpose defined as $\pi^*(f) = f \circ \pi$, for all $f \in (A/I)^*$. Then π^* is an injection.*

Proof. Let $f, g \in (A/I)^*$. Then for $a \in A$, we have

$$\pi^*(f)(a) = \pi^*(g)(a) \Rightarrow f(\pi(a)) = g(\pi(a)) \Rightarrow f([a]_I) = g([a]_I) \Rightarrow f = g.$$

Therefore, we conclude that π^* is injective. □

Proposition 2.3.8. *Let $f \in A^\circ$ and suppose that f vanishes on the ideal I of A. Then there exists a unique element $\overline{f} \in (A/I)^*$ for which $\pi^*(\overline{f}) = f$.*

Proof. Since $f \in A^\circ \subseteq A^*$, then $f \in A^*$, and so $f : A \to K$ is a K-linear map. Moreover, since $f(I) = 0$, then $I \subseteq \ker f$. Now, we consider the canonical surjection $\pi : A \to A/I$. Thus, by the universal property of the quotient vector space, there exists a unique K-linear map $\overline{f} : A/I \to K$ such that $f(a) = \overline{f}(\pi(a)) = \pi^*(\overline{f}(a))$, for all $a \in A$. Therefore, since π^* is an injection (by the previous lemma), we conclude that $\overline{f}$ is the unique element in $(A/I)^*$ for which $\pi^*(\overline{f}) = f$. □

Remark 2.3.9. If E is a finite dimensional K-vector space, $E^* \otimes E^* \cong (E \otimes E)^*$. Indeed, let $\{e_1, \ldots, e_n\}$ be a base of E and let $\{\omega_1, \ldots, \omega_n\}$ be its dual base, which is given by $\omega_i(e_j) = \delta_{i,j}$, for all $i, j \in \{1, \ldots, n\}$. Thus $\{e_i \otimes e_j\}_{1 \leq i,j \leq n}$ is a base of $E \otimes E$. Let $\{\eta_{ij}\}_{1 \leq i,j \leq n}$ be its dual base, which is defined as

$$\eta_{ij}(e_k \otimes e_l) = \left\{ \begin{array}{cc} 1 & \text{if } i = k, j = l \\ 0 & \text{otherwise} \end{array} \right\} = \delta_{ik}\delta_{jl}.$$

Therefore, we conclude that there is a K-vector space isomorphism between $E^* \otimes E^*$ and $(E \otimes E)^*$ given by $\omega_i \otimes \omega_j \mapsto \eta_{ij}$.

Proposition 2.3.10. *It is satisfied that* $m_A^*(A^\circ) \subseteq A^\circ \otimes A^\circ$.

Proof. Let $f \in A^\circ$. Then f vanishes on some cofinite ideal $I \subseteq A$. By the previous proposition, there exists a unique $\overline{f} \in (A/I)^*$ such that $\pi^*(\overline{f}) = f$.

Recall that, by Proposition 2.2.12, A/I is a K-algebra with multiplication map $m_{A/I} : A/I \otimes A/I \to A/I$ defined as $m_{A/I}([a]_I \otimes [b]_I) = [ab]_I$. Its transpose $m_{A/I}^* : (A/I)^* \to (A/I \otimes A/I)^*$ is given by $m_{A/I}^*(f) = f \circ m_{A/I}$. Since A/I is finite dimensional, by the previous remark one has that $(A/I)^* \otimes (A/I)^* \cong (A/I \otimes A/I)^*$, and so $m_{A/I}^* : (A/I)^* \to (A/I)^* \otimes (A/I)^*$.

Thus, for $a, b \in A$, we have

$$\begin{aligned} m_A^*(f)(a \otimes b) &= m_A^*(\pi^*(\overline{f}))(a \otimes b) = \pi^*(\overline{f})(m_A(a \otimes b)) = \pi^*(\overline{f})(ab) = \\ &= \overline{f}(\pi(ab)) = \overline{f}([ab]_I) = \overline{f}(m_{A/I}([a]_I \otimes [b]_I)) = m_{A/I}^*(\overline{f})([a]_I \otimes [b]_I) = \\ &= m_{A/I}^*(\overline{f})(\pi(a) \otimes \pi(b)) = \left(\sum_{(\overline{f})} \overline{f}_{(1)} \otimes \overline{f}_{(2)} \right)(\pi(a) \otimes \pi(b)) = \\ &= \sum_{(\overline{f})} \overline{f}_{(1)}(\pi(a)) \otimes \overline{f}_{(2)}(\pi(b)) = \sum_{(\overline{f})} \pi^*(\overline{f}_{(1)})(a) \otimes \pi^*(\overline{f}_{(2)})(b) = \\ &= \left(\sum_{(\overline{f})} \pi^*(\overline{f}_{(1)}) \otimes \pi^*(\overline{f}_{(2)}) \right)(a \otimes b). \end{aligned}$$

All in all, we have obtained $m_A^*(f)(a \otimes b) = \left(\sum_{(\overline{f})} \pi^*(\overline{f}_{(1)}) \otimes \pi^*(\overline{f}_{(2)}) \right)(a \otimes b)$.

It remains to show that $\pi^*(\overline{f}_{(1)}), \pi^*(\overline{f}_{(2)}) \in A^\circ$. Since $\overline{f}_{(1)}, \overline{f}_{(2)} \in (A/I)^*$, then $\pi^*(\overline{f}_{(1)}), \pi^*(\overline{f}_{(2)}) \in A^*$. Since I is a cofinite ideal, for $c \in I, i \in \{1, 2\}$, we have $\pi^*(\overline{f}_{(i)})(c) = \overline{f}_{(i)}(\pi(c)) = \overline{f}_{(i)}([c]_I) = \overline{f}_{(i)}([0]_I) = 0$. Thus $\pi^*(\overline{f}_{(1)}), \pi^*(\overline{f}_{(2)}) \in A^\circ$. Consequently, we conclude that $m_A^*(A^\circ) \subseteq A^\circ \otimes A^\circ$. □

Theorem 2.3.11. *If A is a K-algebra, then A° is a K-coalgebra.*

Proof. Recall that A is a triple (A, m_A, λ_A), where $m_A : A \otimes A \to A$, $m_A(a \otimes b) = ab$, is K-linear and satisfies the associative property and $\lambda_A : K \to A$, $\lambda_A(r) = r1_A$, is K-linear and satisfies the unit property. We need to define a comultiplication map Δ_{A° and a counit map ε_{A°.

We start considering the transpose of m_A, $m_A^* : A^* \to (A \otimes A)^*$, which is a K-linear map defined as $m_A^*(f) = f \circ m_A$. Since $A^\circ \subseteq A^*$ and $m_A^*(A^\circ) \subseteq A^\circ \otimes A^\circ$ (by Proposition 2.3.10), m_A^* restricts to a K-linear map

$$\begin{array}{rccc} \Delta_{A^\circ} : & A^\circ & \to & A^\circ \otimes A^\circ \\ & f & \mapsto & \Delta_{A^\circ}(f) = m_A^*(f) \end{array}$$

Now, we consider the transpose of λ_A, $\lambda_A^* : A^* \to K^* \cong K$, which is a K-linear map given by $\lambda_A^*(f) = f \circ \lambda_A$. Since $A^\circ \subseteq A^*$, λ_A^* restricts to a K-linear map

$$\begin{array}{rccc} \varepsilon_{A^\circ}: & A^\circ & \to & K \\ & f & \mapsto & \varepsilon_{A^\circ}(f) = \lambda_A^*(f) \end{array}$$

Observe that if we dualize the commutative diagrams of the definition of the algebra A, we obtain the commutative diagrams of the definition of the coalgebra A°

$$\begin{array}{ccc} A^\circ \otimes A^\circ \otimes A^\circ & \xleftarrow{I_{A^\circ} \otimes \Delta_{A^\circ}} & A^\circ \otimes A^\circ \\ \uparrow{\scriptstyle \Delta_{A^\circ} \otimes I_{A^\circ}} & & \uparrow{\scriptstyle \Delta_{A^\circ}} \\ A^\circ \otimes A^\circ & \xleftarrow[\Delta_{A^\circ}]{} & A^\circ \end{array} \quad , \quad \begin{array}{ccc} A^\circ \otimes K & \xleftarrow{I_{A^\circ} \otimes \varepsilon_{A^\circ}} & A^\circ \otimes A^\circ \\ \uparrow{\scriptstyle - \otimes 1_K} & \nearrow{\scriptstyle \Delta_{A^\circ}} & \downarrow{\scriptstyle \varepsilon_{A^\circ} \otimes I_A} \\ A^\circ & \xrightarrow[1_K \otimes -]{} & K \otimes A^\circ \end{array}$$

By Theorem 2.3.2, we know that $(1_K \otimes -)^* = s_1$ and $(- \otimes 1_K)^* = s_2$. Thus, $(1_K \otimes -)^{**} = 1_K \otimes - = s_1^*$ and $(- \otimes 1_K)^{**} = - \otimes 1_K = s_2^*$. Therefore, we conclude that $(A^\circ, \Delta_{A^\circ}, \varepsilon_{A^\circ})$ is a K-coalgebra. □

Proposition 2.3.12. *If (A, m_A, λ_A) is a commutative algebra, then $(A^\circ, \Delta_{A^\circ}, \varepsilon_{A^\circ})$ is a cocommutative colgebra, and if $(C, \Delta_C, \varepsilon_C)$ is a cocommutative coalgebra, then $(C^*, \Delta_{C^*}, \varepsilon_{C^*})$ is a commutative algebra.*

Proof. We will start with the first statement. Since A is an algebra, by Theorem 2.3.11, A° is a coalgebra. Now, we consider the twist map of $A \otimes A$, which is defined as $\tau_{A\otimes A}(a \otimes b) = b \otimes a$. Since $A^\circ \otimes A^\circ \subseteq A^* \otimes A^* \subseteq (A \otimes A)^*$ (by Corollary 2.1.9), its transpose restricted to $A^\circ \otimes A^\circ$ is

$$\begin{array}{rccc} \tau_{A\otimes A}^*: & A^\circ \otimes A^\circ & \to & A^\circ \otimes A^\circ \\ & f \otimes g & \mapsto & (f \otimes g) \circ \tau_{A\otimes A} \end{array}$$

Note that for $a, b \in A,\ f, g \in A^\circ$,

$$\tau_{A\otimes A}^*(f \otimes g)(a \otimes b) = (f \otimes g)(\tau_{A\otimes A}(a \otimes b)) = (f \otimes g)(b \otimes a) = f(b)g(a) =$$
$$= g(a)f(b) = (g \otimes f)(a \otimes b) \Rightarrow \tau_{A\otimes A}^*(f \otimes g) = g \otimes f.$$

In other words, $\tau_{A\otimes A}^*$ is the twist map of $A^\circ \otimes A^\circ$

$$\tau_{A\otimes A}^* = \tau_{A^\circ \otimes A^\circ} \tag{2.12}$$

Since the commutative diagrams of the definition of an algebra and a coalgebra are mutually dual, we conclude that A° is a cocommutative coalgebra.

Analogously, one has the second statement. □

We end this chapter with an application. Let $K[x]$ be the algebra of polynomials over the field K as in Example 2.2.7.

Definition 2.3.13. A **sequence** $\{s_n\}_{n\in\mathbb{N}}$ is called k**th-order linearly recursive over** K if there exists a natural k and coefficients $a_0, \ldots, a_{k-1} \in K$ such that for all $n \geq 0$, the following recurrence relation is satisfied

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \cdots + a_1 s_{n+1} + a_0 s_n. \tag{2.13}$$

The **characteristic polynomial** associated to the previous recurrence is

$$P(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_1 x - a_0.$$

Proposition 2.3.14. *The collection of kth-order linearly recursive sequences over K of all orders $k \geq 0$ can be identified with the finite dual $K[x]^\circ$.*

Proof. Let $\{s_n\}$ be a kth-order linearly recursive sequence over K with recursive relation $s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \cdots + a_1 s_{n+1} + a_0 s_n$, for all $n \geq 0$, and characteristic polynomial $P(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_1 x - a_0$, for $a_0, \ldots, a_{k-1} \in K$.

Note that we can identify $\{s_n\}$ with the element $s = \sum_{n=0}^{\infty} s_n\varphi_n \in K[x]^*$. Thus,

$$\begin{aligned} s(P(x)) &= \left(\sum_{n=0}^{\infty} s_n\varphi_n\right)(x^k - a_{k-1}x^{k-1} - \cdots - a_1 x - a_0) = \\ &= s_k - a_{k-1}s_{k-1} - \cdots - a_1 s_1 - a_0 s_0 \underset{(2.13)}{=} 0. \end{aligned}$$

It follows that $s(Q(x)P(x)) = 0$, for all $Q(x) = \sum_{i=0}^{n} b_i x^i \in K[x]$:

$$\begin{aligned} Q(x)P(x) = \sum_{i=0}^{n} b_i x^i P(x) \Rightarrow s(Q(x)P(x)) &= \sum_{i=0}^{n} b_i s(x^i P(x)) = \\ &= \sum_{i=0}^{n} b_i(x^{i+k} - a_{k-1}x^{i+k-1} - \cdots - a_1 x^{i+1} - a_0 x^i) = \\ = \sum_{i=0}^{n} b_i(s_{i+k} - a_{k-1}s_{i+k-1} - \cdots - a_1 s_{i+1} - a_0 s_i) &\underset{(2.13)}{=} \sum_{i=0}^{n} b_i\ 0 = 0. \end{aligned}$$

Hence s vanishes on the principal ideal $I = (P(x))$ of $K[x]$. Clearly $\dim(K[x]/I) = k$. We conclude that $s \in K[x]^\circ$.

Conversely, let $s = \sum_{n\geq 0} s_n\varphi_n \in K[x]^\circ$. Then s vanishes on a coideal $I \subseteq K[x]$. Since $K[x]$ is a principal ideal domain, there exists a polynomial $P(x) \in K[x]$ of degree k such that $I = (P(x))$. It is easy to check that s is a kth-order linearly recursive sequence over K with characteristic polynomial $P(x)$. □

3 Bialgebras and module algebras

In this chapter, we introduce bialgebras. Then, we show how a bialgebra B can act on an algebra giving it the structure of a left or right B-module algebra, and also how the bialgebra can act on a coalgebra endowing it with the structure of right or left B-module coalgebra. Finally, we prove the main result, which states that if B is a bialgebra, its finite dual B° is a bialgebra too.

3.1 Bialgebras

In this section, we introduce bialgebras, which are vector spaces that are both algebras and coalgebras such that comultiplication and counit maps are algebra homomorphisms, and give some basic examples. We show that $K[x]$ is a bialgebra in exactly two distinct ways. Afterwards, we define biideals and discuss quotient bialgebras and bialgebra homomorphisms.

Definition 3.1.1. A K-**bialgebra** is K-vector space B together with maps m_B, λ_B, Δ_B, ε_B that satisfy that (B, m_B, λ_B) is a K-algebra, $(B, \Delta_B, \varepsilon_B)$ is a K-coalgebra and Δ_B, ε_B are K-algebra homomorphisms.

A K-bialgebra B is **commutative** if it is a commutative algebra; B is **cocommutative** if it is a cocommutative coalgebra.

Remark 3.1.2. The requirement that $\Delta_B : B \to B \otimes B$ is an algebra homomorphism implies that

1. $\Delta_B(m_B(a \otimes b)) = m_{B\otimes B}(\Delta_B(a) \otimes \Delta_B(b)) \Leftrightarrow \Delta_B(ab) = \Delta_B(a)\Delta_B(b)$, that is,

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

2. $\Delta_B(\lambda_B(r)) = \lambda_{B\otimes B}(r) = \lambda_B(r) \otimes 1_B = r\ 1_B \otimes 1_B$, and so, in particular,

$$\Delta_B(\lambda_B(1_K)) = \Delta_B(1_B) = 1_B \otimes 1_B.$$

and the requirement that $\varepsilon_B : B \to K$ is an algebra homomorphism implies that

1. $\varepsilon_B(m_B(a \otimes b)) = m_K(\varepsilon_B(a) \otimes \varepsilon_B(b)) \Leftrightarrow \varepsilon_B(ab) = \varepsilon_B(a)\varepsilon_B(b)$,
2. $\varepsilon_B(\lambda_B(r)) = \lambda_K(r) = I_K(r) = r$, and so, in particular, $\varepsilon_B(1_B) = 1_K$.

Definition 3.1.3. Let B be a bialgebra. A **primitive element** of B is an element $b \in B$ such that $\Delta_B(b) = 1 \otimes b + b \otimes 1$.

Example 3.1.4. The field K as a vector space over itself is a commutative and cocommutative K-bialgebra (see Examples 2.2.6 and 2.2.16). It is called the **trivial** K**-bialgebra**.

Example 3.1.5. Let G be a finite group. From Example 2.2.8 and Example 2.2.20, $K[G]$ has the structure of an algebra and a cocommutative coalgebra, respectively. It is easy to check that comultiplication and counit maps are algebra homomorphisms, and so $K[G]$ is a cocommutative bialgebra. It is called the **group bialgebra**. It is commutative if, and only if, G is abelian.

Example 3.1.6. Let $K[x]$ be the K-vector space of polynomials in the indeterminate x. From Example 2.2.7 and Example 2.2.21, $K[x]$ has the structure of a commutative algebra and a cocommutative coalgebra, respectively. It is easy to check that $\Delta_{K[x]}$ and $\varepsilon_{K[x]}$ are algebra homomorphisms, and so $K[x]$ is a commutative and cocommutative bialgebra. One has that $\Delta_{K[x]}(x) = x \otimes x$. Hence it is called the **polynomial bialgebra with x grouplike**.

Example 3.1.7. Let $K[x]$ be the K-vector space of polynomials in the indeterminate x. From Example 2.2.7 and Example 2.2.22, $K[x]$ has the structure of a commutative algebra and a cocommutative coalgebra, respectively. It is easy to check that $\Delta_{K[x]}$ and $\varepsilon_{K[x]}$ are algebra homomorphisms, and so $K[x]$ is a commutative and cocommutative bialgebra. One has that $\Delta_{K[x]}(x) = 1 \otimes x + x \otimes 1$. Hence it is called the **polynomial bialgebra with x primitive**.

Definition 3.1.8. Let B, B' be K- bialgebras. Since B and B' are algebras and coalgebras, $B \otimes B'$ is an algebra and a coalgebra (Definitions 2.2.11 and 2.2.23). It is easy to show that $\Delta_{B\otimes B'}$ and $\varepsilon_{B\otimes B'}$ are algebra homomorphisms, and hence the **tensor product of bialgebras** $B \otimes B'$ has the structure of a K-bialgebra.

Definition 3.1.9. Let B be a K-bialgebra. A subspace $I \subseteq B$ is a **biideal** of B if it is both an ideal and a coideal.

Proposition 3.1.10. *Let B be a K-bialgebra and let I be a biideal of B. Then the quotient space is B/I is a K-bialgebra.*

Proof. By Proposition 2.2.12, B/I is a K-algebra, and by Proposition 2.2.25, B/I is a K-coalgebra. It is easy to show that $\Delta_{B/I}$ and $\varepsilon_{B/I}$ are algebra homomorphisms since Δ_B and ε_B are also algebra homomorphisms. Therefore, we conclude that B/I is a K-bialgebra. □

Definition 3.1.11. Let B be a K-bialgebra and let I be a biideal of B. The K-bialgebra B/I of the previous proposition is the **quotient bialgebra** B by I.

Definition 3.1.12. Let B, B' be bialgebras. A K-**bialgebra homomorphism** from B to B' is a $\phi : B \to B'$ which is both an algebra and a coalgebra homomorphism. A K-bialgebra homomorphism that is injective and surjective is a K-**bialgebra isomorphism**.

Surprisingly, the bialgebras structures on $K[x]$ given in the previous examples are the only bialgebra structures on $K[x]$ up to algebra isomorphism.

Proposition 3.1.13. *Suppose the polynomial algebra $K[x]$ is given the structure of a K-bialgebra. Then, there exists $z \in K[x]$ for which $K[z] = K[x]$ and z is either grouplike or z is primitive.*

Proof. Let $\lambda := \lambda_{K[x]}$, $\Delta := \Delta_{K[x]}$, $\varepsilon := \varepsilon_{K[x]}$ and $I := I_{K[x]}$. Recall $\{x^i \otimes x^j\}_{i,j\in\mathbb{N}}$ is a basis of $K[x] \otimes K[x]$. Then, we write

$$\Delta(x) = \sum_{i=0}^{m}\sum_{j=0}^{n} b_{i,j}\ x^i \otimes x^j \in K[x] \otimes K[x], \text{ for } b_{i,j} \in K.$$

Let l denote the highest degree of x that occurs in the left factors of the tensors in the sum $\Delta(x)$. Then, $b_{l,j} \neq 0$ for some $j \in \{0, \ldots, n\}$; let j' denote the maximal j for which $b_{l,j} \neq 0$. On the one hand,

$$(I \otimes \Delta)\Delta(x) = \sum_{i=0}^{m}\sum_{j=0}^{n} c\ x^i \otimes x^{j_1} \otimes x^{j_2} \in K[x] \otimes K[x] \otimes K[x].$$

Note that l is the highest degree of x that occurs in the left-most factors of the tensors in the sum $(I \otimes \Delta)\Delta(x)$. On the other hand,

$$(\Delta \otimes I)\Delta(x) = (\Delta \otimes I)\left(\sum_{i=0}^{m}\sum_{j=0}^{n} b_{i,j}\ x^i \otimes x^j\right) = \sum_{i=0}^{m}\sum_{j=0}^{n} b_{i,j}\ \Delta(x^i) \otimes x^j =$$
$$= \sum_{i=0}^{m}\sum_{j=0}^{n} b_{i,j}\ (\Delta(x))^i \otimes x^j = \sum_{i=0}^{m}\sum_{j=0}^{n} b_{i,j}\ \left(\sum_{\alpha=0}^{m}\sum_{\beta=0}^{n} b_{\alpha,\beta}\ x^\alpha \otimes x^\beta\right)^i \otimes x^j =$$
$$= b_{l,j'}^{l+1}\ x^{l^2} \otimes x^{lj'} \otimes x^{j'}\ +\ T,$$

where T is a sum of tensors in $K[x] \otimes K[x] \otimes K[x]$ of the form $c\ x^i \otimes x^j \otimes x^k$ with $i \leq l^2$, and, since $b_{l,j'} \neq 0$, $b_{l,j'}^{l+1}\ x^{l^2} \otimes x^{lj'} \otimes x^{j'}$ is the term with the highest degree of x that occurs in the left-most factors of the tensors in $(\Delta \otimes I)\Delta(x)$ (that is, it comes from making $i = \alpha = l$ and $j = \beta = j'$). In other words, l^2 is the highest degree of x that occurs in the left-most factors of the tensors in this sum. By the coassociative property of Δ, we have $l^2 = l$, and hence, either $l = 0$ or $l = 1$.

Now, let r denote the highest degree of x that occurs in the right factors of the tensors in the sum $\Delta(x)$. Repeating the argument above, one has that either $r = 0$ or $r = 1$. Consequently, $\Delta(x) = b_{0,0}(1 \otimes 1) + b_{0,1}(1 \otimes x) + b_{1,0}(x \otimes 1) + b_{1,1}(x \otimes x)$.

Let $y = x - \varepsilon(x)$. We see that $\varepsilon(y) = 0$:

$$\varepsilon(y) = \varepsilon(x - \varepsilon(x)) = \varepsilon(x - \varepsilon(x)1_K) = \varepsilon(x - \varepsilon(x)1_{K[x]}) = \varepsilon(x) - \varepsilon(x)\varepsilon(1_{K[x]}) =$$
$$= \varepsilon(x) - \varepsilon(x)\varepsilon(\lambda(1_K)) = \varepsilon(x) - \varepsilon(x)1_K = \varepsilon(x) - \varepsilon(x) = 0.$$

Let $\Delta(y) = \sum_{i=0}^{m}\sum_{j=0}^{n} a_{i,j}\ y^i \otimes y^j$. By comparing the leading coefficients in $(\Delta \otimes I)\Delta(y)$ and $(I \otimes \Delta)\Delta(y)$ as above, we conclude that $a_{i,j} = 0$ if $i > 1$ or $j > 1$. Thus, $\Delta(y) = a_{0,0}\ 1 \otimes 1 + a_{0,1}\ 1 \otimes y + a_{1,0}\ y \otimes 1 + a_{1,1}\ y \otimes y$. Since $\varepsilon(y) = 0$, we also have that $a_{0,0} = 0$ and $a_{0,1} = a_{1,0} = 1$. Indeed,

$$y \otimes 1 \underset{(2.6)}{=} (I \otimes \varepsilon)\Delta(y) =$$
$$= a_{0,0}\ 1 \otimes \underbrace{\varepsilon(1)}_{=1} + a_{0,1}\ 1 \otimes \underbrace{\varepsilon(y)}_{=0} + a_{1,0}\ y \otimes \underbrace{\varepsilon(1)}_{=1} + a_{1,1}\ y \otimes \underbrace{\varepsilon(y)}_{=0} \Leftrightarrow$$
$$\Leftrightarrow y \otimes 1 = a_{0,0}\ 1 \otimes 1 + a_{1,0}\ y \otimes 1 \Leftrightarrow a_{0,0} = 0, a_{1,0} = 1.$$

Similarly, one has $a_{0,1} = 1$. Therefore, $\Delta(y) = 1 \otimes y + y \otimes 1 + a\ y \otimes y$, for some $a \in K$. If $a = 0$, then $z = y$ is primitive and $K[z] = K[x]$ (since $y = x - \varepsilon(x)$, where $\varepsilon(x) \in K$). If $a \neq 0$, we define $z = 1 + ay$, and so z is grouplike and $K[z] = K[x]$.

Indeed, at the one hand, we have

$$z \otimes z = (1 + ay) \otimes (1 + ay) = 1 \otimes 1 + a(1 \otimes y) + a(y \otimes 1) + a^2(y \otimes y).$$

At the other hand, since Δ is K-linear and a K-algebra homomorphism, we have

$$\Delta(z) = \Delta(1 + ay) = \Delta(1) + a\Delta(y) = 1 \otimes 1 + a(1 \otimes y) + a(y \otimes 1) + a^2(y \otimes y).$$

□

Remark 3.1.14. As we have seen in Proposition 2.3.14, $K[x]^\circ$ is the collection of linearly recursive sequences over K. We have shown that $K[x]$ is a bialgebra in exactly two distinct ways, and so $K[x]^\circ$ has two different structures as a bialgebra (by Theorem 3.3.3). Hence, there are just two distinct ways of multiplying sequences in $K[x]^\circ$, which are called the **Hadamard product** and the **Hurwitz product**. However, we are not going to discuss these topics.

3.2 Module algebras and module coalgebras

In this section, we show how a bialgebra B can act on an algebra or a coalgebra endowing it with the structure of a right or left B-module algebra or coalgebra, respectively. That leads us to define a certain right or left action on the dual algebra B^*, so that B^* has the structure of a right or left B-module algebra, respectively.

Let B be a K-bialgebra.

Definition 3.2.1. Let A be a K-algebra and a left (resp. right) B-module with action denoted by "$\cdot$". Then A is a **left** (resp. **right**) **B-module K-algebra** if for $b \in B$, $a, a' \in A$, it satisfies

$$b \cdot (aa') = \sum_{(b)} (b_{(1)} \cdot a)(b_{(2)} \cdot a') \quad \text{and} \quad b \cdot 1_A = \varepsilon_B(b)1_A$$

$$(\text{resp. } (aa') \cdot b = \sum_{(b)} (a \cdot b_{(1)})(a' \cdot b_{(2)}) \quad \text{and} \quad 1_A \cdot b = 1_A\varepsilon_B(b) = 1_A\varepsilon_B(b)).$$

Let A, A' be K-algebras. A **left** (resp. **right**) **B-module K-algebra homomorphism** from A to A' is a K-linear map $\phi : A \to A'$ which is both an algebra and a left (resp. right) B-module homomorphism.

Definition 3.2.2. Let C be a K-coalgebra and a right (resp. left) B-module with action denoted by "$\cdot$". Then C is a **right** (resp. **left**) **B-module K-coalgebra** if for $b \in B$, $c \in C$, it satisfies

$$\Delta_C(c \cdot b) = \sum_{(c,b)} (c_{(1)} \cdot b_{(1)}) \otimes (c_{(2)} \cdot b_{(2)}) \quad \text{and} \quad \varepsilon_C(c \cdot b) = \varepsilon_C(c)\varepsilon_B(b) = \varepsilon_B(b)\varepsilon_C(c)$$

$$(\text{resp. } \Delta_C(b \cdot c) = \sum_{(b,c)} (b_{(1)} \cdot c_{(1)}) \otimes (b_{(2)} \cdot c_{(2)}) \quad \text{and} \quad \varepsilon_C(b \cdot c) = \varepsilon_B(b)\varepsilon_C(c)).$$

Let C, C' be K-coalgebras. A **right** (resp. **left**) **B-module K-coalgebra homomorphism** from C to C' is a K-linear map $\phi : C \to C'$ which is both a coalgebra and a right (resp. left) B-module homomorphism.

Definition 3.2.3. Note that there is a right (resp. left) B-module structure on B^* defined as $(f \leftharpoonup a)(b) = f(ab)$ (resp. $(a \rightharpoonup f)(b) = f(ba)$), for $a, b \in B$, $f \in B^*$. The action $\leftharpoonup$ is called the **right** (resp. **left**) **translate action**. For $a \in B$, $f \in B^*$, the element $f \leftharpoonup a$ is the **right** (resp. **left**) **B-translate of f by a**. Moreover, $f \leftharpoonup B = \{f \leftharpoonup b \ : \ b \in B\}$ (resp. $B \rightharpoonup f = \{b \rightharpoonup f \ : \ b \in B\}$) is a subspace of B^*.

Proposition 3.2.4. *The right (resp. left) translate action endows B^* with the structure of a right (resp. left) B-module algebra.*

Proof. In order to prove that B^* is a right B-module algebra, we need to show three things. Firstly, we see that B^* is a K-algebra. Indeed, since B is a bialgebra, it is a coalgebra, and by Theorem 2.3.2, B^* is an algebra. Secondly, we show that B^* is a right B-module. Indeed, B^* is a right B-module with vector addition given by the vector addition as a dual vector space and scalar multiplication given by the right translate action $\leftharpoonup$.

Finally, we see that the right translate action satisfies

$$(fg \leftharpoonup a)(b) = \Big(\sum_{(a)} (f \leftharpoonup a_{(1)})(g \leftharpoonup a_{(2)}) \Big)(b) \quad \text{and} \quad (1_{B^*} \leftharpoonup a)(b) = (1_{B^*}\varepsilon_B(a))(b).$$

On the one hand, for $f, g \in B^*$, $a, b \in B$, we have

$$(fg \leftharpoonup a)(b) = (fg)(ab) = m_{B^*}(f \otimes g)(ab) = \Delta_B^*(f \otimes g)(ab) = (f \otimes g)\Delta_B(ab) =$$

$$= (f \otimes g)\Delta_B(a)\Delta_B(b) = (f \otimes g)\Big(\sum_{(a)} a_{(1)} \otimes a_{(2)} \Big)\Big(\sum_{(b)} b_{(1)} \otimes b_{(2)} \Big) =$$

$$= (f \otimes g)\Big(\sum_{(a,b)} a_{(1)}b_{(1)} \otimes a_{(2)}b_{(2)} \Big) = \sum_{(a,b)} f(a_{(1)}b_{(1)})g(a_{(2)}b_{(2)}) =$$

$$= \sum_{(a,b)} (f \leftharpoonup a_{(1)})(b_{(1)})(g \leftharpoonup a_{(2)})(b_{(2)}) = \sum_{(a,b)} ((f \leftharpoonup a_{(1)}) \otimes (g \leftharpoonup a_{(2)}))(b_{(1)} \otimes b_{(2)}) =$$

$$= \Big(\sum_{(a)} (f \leftharpoonup a_{(1)}) \otimes (g \leftharpoonup a_{(2)}) \Big)\Big(\sum_{(b)} b_{(1)} \otimes b_{(2)} \Big) =$$

$$= \Big(\sum_{(a)} (f \leftharpoonup a_{(1)}) \otimes (g \leftharpoonup a_{(2)}) \Big) \Delta_B(b) =$$

$$= \Delta_B^* \Big(\sum_{(a)} (f \leftharpoonup a_{(1)}) \otimes (g \leftharpoonup a_{(2)}) \Big)(b) = \Big(\sum_{(a)} \Delta_B^*((f \leftharpoonup a_{(1)}) \otimes (g \leftharpoonup a_{(2)})) \Big)(b) =$$

$$= \Big(\sum_{(a)} m_{B^*}((f \leftharpoonup a_{(1)}) \otimes (g \leftharpoonup a_{(2)})) \Big)(b) = \Big(\sum_{(a)} (f \leftharpoonup a_{(1)})(g \leftharpoonup a_{(2)}) \Big)(b).$$

On the other hand, recall that multiplication map on B^* is a K-linear map $\lambda_{B^*} : K^* \cong K \to B^*$ defined as

$$\lambda_{B^*}(r)(b) = \begin{cases} r1_{B^*}(b) & \text{(Def. multiplication map)} \\ \varepsilon_B^*(r)(b) = r\varepsilon_B(b) & \text{(Theorem 2.3.2)} \end{cases}$$

Thus, we have that

$$\lambda_{B^*}(1_K) = 1_{B^*} = \varepsilon_B \tag{3.1}$$

Hence, for $a, b \in B$, we have

$$(1_{B^*} \leftharpoonup a)(b) = 1_{B^*}(ab) \underset{(3.1)}{=} \varepsilon_B(ab) = \varepsilon_B(a)\varepsilon_B(b) \underset{(3.1)}{=} 1_{B^*}(a)\varepsilon_B(b) = (1_{B^*}(a)\varepsilon_B)(b).$$

We conclude that B^* is a right B-module algebra. □

3.3 Duality

Finally, we prove the main result of this chapter, which sets that if B is a bialgebra, then its finite dual B° is also a bialgebra. In order to do it, we need the next lemma (we are not going to prove it) and the following remark.

Lemma 3.3.1. *Let B be a K-bialgebra and let $f \in B^*$. Then the following statements are equivalent:*

1. *$dim(f \leftharpoonup B) < \infty$,*
2. *$f \in B^\circ$.*

Remark 3.3.2. Let A be a K-algebra. For $f \in A^*$, the following equation holds

$$\lambda_A^*(f) = f(1_A) \tag{3.2}$$

Indeed, for $r \in K, f \in A^*$, we have

$$\lambda_A^*(f)(r) = f(\lambda_A(r)) = f(r1_A) = rf(1_A) = f(1_A)\, r \underset{(K \cong K^*)}{=} (f(1_A))(r).$$

Theorem 3.3.3. *If B is a K-bialgebra, then B° is a bialgebra.*

Proof. Recall that B is a K-vector space with maps m_B, λ_B, Δ_B, ε_B satisfying that (B, m_B, λ_B) is a K-algebra, $(B, \Delta_B, \varepsilon_B)$ is a K-coalgebra, and Δ_B, ε_B are K-algebra homomorphisms.

Firstly, we see that B° is an algebra. We need to construct a multiplication map m_{B° and a unit map λ_{B°. Since B is a coalgebra, by Theorem 2.3.2, B^* is an algebra with multiplication $m_{B^*} = \Delta_B^*|_{B^*\otimes B^*}$ and unit $\lambda_{B^*} = \varepsilon_B^*|_{B^*}$. We start with multiplication. Since $B^\circ \subseteq B^*$, m_{B^*} restricts to a K-linear map

$$\begin{array}{rccl} m_{B^\circ}: & B^\circ \otimes B^\circ & \to & B^* \\ & f \otimes g & \mapsto & m_{B^\circ}(f \otimes g) = m_{B^*}(f \otimes g) = fg \end{array}$$

We show that $m_{B^\circ}(B^\circ \otimes B^\circ) \subseteq B^\circ$. Since B is a bialgebra, by Proposition 3.2.4 the right translate action $\leftharpoonup$ endows B^* with the structure of a right B-module algebra, and so, the following equation is satisfied

$$(fg \leftharpoonup a)(b) = \left(\sum_{(a)} (f \leftharpoonup a_{(1)})(g \leftharpoonup a_{(2)}) \right)(b), \ \forall \ f, g \in B^*, \ a, b \in B.$$

In particular, it holds for $f, g \in B^\circ$. Thus $fg \leftharpoonup B \subseteq \text{span}((f \leftharpoonup B)(g \leftharpoonup B))$, for all $f, g \in B^\circ$. By the previous lemma, we have

$$f, g \in B^\circ \Rightarrow \dim(f \leftharpoonup B) < \infty, \dim(g \leftharpoonup B) < \infty \Rightarrow$$
$$\Rightarrow \dim(\text{span}((f \leftharpoonup B)(g \leftharpoonup B))) < \infty \Rightarrow \dim(fg \leftharpoonup B) < \infty \Rightarrow fg \in B^\circ.$$

Therefore, $m_{B^\circ}(B^\circ \otimes B^\circ) \subseteq B^\circ$. Moreover, m_{B° satisfies the associative property since m_{B^*} does.

We continue with unit. Set $\lambda_{B^\circ} = \lambda_{B^*}$, which is K-linear

$$\begin{array}{rccl} \lambda_{B^\circ}: & K & \to & B^* \\ & r & \mapsto & \lambda_{B^\circ}(r) = \lambda_{B^*}(r) = \varepsilon_B^*(r) = r\varepsilon_B \end{array}$$

We show that $\lambda_{B^\circ}(K) \subseteq B^\circ$. Since $\lambda_{B^\circ}(r) = r\varepsilon_B$, for all $r \in K$, it remains to see that ε_B vanishes on some cofinite ideal. Indeed, since $\varepsilon_B : B \to K$ is a K-linear, $\ker(\varepsilon_B)$ is an ideal of B. ε_B clearly vanishes on $\ker(\varepsilon_B)$ and $\ker(\varepsilon_B)$ is cofinite

$$B/\ker(\varepsilon_B) \cong \text{im}(\varepsilon_B) \subseteq K \Rightarrow \dim(B/\ker(\varepsilon_B)) \leq \dim_K(K) = 1 < \infty.$$

Hence, $\lambda_{B^\circ}(K) \subseteq B^\circ$. Moreover, λ_{B° satisfies the unit property since λ_{B^*} does.

Secondly, we show that B° is a coalgebra. Indeed, since B is an algebra, by Theorem 2.3.11, B° is a coalgebra with multiplication map $\Delta_{B^\circ} = m_B^*|_{B^\circ}$ and counit map $\varepsilon_{B^\circ} = \lambda_B^*|_{B^\circ}$.

Finally, we see that Δ_{B° and ε_{B° are K-algebra homomorphisms. We have to check that they both satisfy the two conditions of Remark 3.1.2. We start with comultiplication $\Delta_{B^\circ} : B^\circ \to B^\circ \otimes B^\circ$. We need to show that it satisfies

$$\Delta_{B^\circ}(fg) = \Delta_{B^\circ}(f)\Delta_{B^\circ}(g) \text{ and } \Delta_{B^\circ}(\lambda_{B^\circ}(r)) = r\ 1_{B^\circ} \otimes 1_{B^\circ}.$$

First of all, observe that, since B is a coalgebra, by Definition 2.2.23, $B \otimes B$ is also a coalgebra. Moreover, since we have already seen that B° is an algebra, by Definition 2.2.11, $B^\circ \otimes B^\circ$ is an algebra too. Therefore, the following equation holds

$$\Delta^*_{B\otimes B} = m_{B^\circ \otimes B^\circ} \tag{3.3}$$

Indeed,

$$m_{B^\circ\otimes B^\circ} = (m_{B^\circ} \otimes m_{B^\circ})(I_{B^\circ} \otimes \tau_{B^\circ\otimes B^\circ} \otimes I_{B^\circ}) =$$

$$\underset{(2.12)}{=} (m_{B^*} \otimes m_{B^*})(I_{B^*} \otimes \tau^*_{B\otimes B} \otimes I_{B^*}) = (\Delta^*_B \otimes \Delta^*_B)(I^*_B \otimes \tau^*_{B\otimes B} \otimes I^*_B) =$$

$$= (\Delta_B \otimes \Delta_B)^*(I_B \otimes \tau_{B\otimes B} \otimes I_B)^* = ((I_B \otimes \tau_{B\otimes B} \otimes I_B)(\Delta_B \otimes \Delta_B))^* = \Delta^*_{B\otimes B}.$$

On the one hand, for $f, g \in B^\circ$, $a, b \in B$, $\Delta_{B^\circ}(fg) = \Delta_{B^\circ}(f)\Delta_{B^\circ}(g)$ holds:

$$\Delta_{B^\circ}(fg)(a \otimes b) = \Delta_{B^\circ}(m_{B^\circ}(f \otimes g))(a \otimes b) = m^*_B(m_{B^\circ}(f \otimes g))(a \otimes b) =$$

$$= m_{B^\circ}(f \otimes g)m_B(a \otimes b) = m_{B^\circ}(f \otimes g)(ab) = \Delta^*_B(f \otimes g)(ab) = (f \otimes g)\Delta_B(ab) =$$

$$= (f \otimes g)\Delta_B(a)\Delta_B(b) = (f \otimes g)\Big(\sum_{(a)} a_{(1)} \otimes a_{(2)}\Big)\Big(\sum_{(b)} b_{(1)} \otimes b_{(2)}\Big) =$$

$$= (f \otimes g)\Big(\sum_{(a,b)} a_{(1)}b_{(1)} \otimes a_{(2)}b_{(2)}\Big) = \sum_{(a,b)} f(a_{(1)}b_{(1)})\ g(a_{(2)}b_{(2)}) =$$

$$= \sum_{(a,b)} f(m_B(a_{(1)} \otimes b_{(1)}))\ g(m_B(a_{(2)} \otimes b_{(2)})) =$$

$$= \sum_{(a,b)} m^*_B(f)(a_{(1)} \otimes b_{(1)})\ m^*_B(g)(a_{(2)} \otimes b_{(2)}) =$$

$$= \sum_{(a,b)} \Delta_{B^\circ}(f)(a_{(1)} \otimes b_{(1)})\ \Delta_{B^\circ}(g)(a_{(2)} \otimes b_{(2)}) =$$

$$= (\Delta_{B^\circ}(f) \otimes \Delta_{B^\circ}(g))(I_B \otimes \tau \otimes I_B)\Big(\sum_{(a,b)} a_{(1)} \otimes a_{(2)} \otimes b_{(1)} \otimes b_{(2)}\Big) =$$

$$= (\Delta_{B^\circ}(f) \otimes \Delta_{B^\circ}(g))(I_B \otimes \tau \otimes I_B)\Big[\Big(\sum_{(a)} a_{(1)} \otimes a_{(2)}\Big)\Big(\sum_{(b)} b_{(1)} \otimes b_{(2)}\Big)\Big] =$$

$$= (\Delta_{B^\circ}(f) \otimes \Delta_{B^\circ}(g))(I_B \otimes \tau \otimes I_B)(\Delta_B(a) \otimes \Delta_B(b)) =$$

$$= (\Delta_{B^\circ}(f) \otimes \Delta_{B^\circ}(g))(I_B \otimes \tau \otimes I_B)(\Delta_B \otimes \Delta_B)(a \otimes b) =$$

$$= (\Delta_{B^\circ}(f) \otimes \Delta_{B^\circ}(g))\Delta_{B\otimes B}(a \otimes b) = \Delta^*_{B\otimes B}(\Delta_{B^\circ}(f) \otimes \Delta_{B^\circ}(g))(a \otimes b) =$$

$$\underset{(3.3)}{=} m_{B^\circ\otimes B^\circ}(\Delta_{B^\circ}(f) \otimes \Delta_{B^\circ}(g))(a \otimes b) = (\Delta_{B^\circ}(f)\Delta_{B^\circ}(g))(a \otimes b).$$

On the other hand, for $r \in K$, $a, b \in B$, $\Delta_{B^\circ}(\lambda_{B^\circ}(r)) = r\ 1_{B^\circ} \otimes 1_{B^\circ}$ holds:

$$\Delta_{B^\circ}(\lambda_{B^\circ}(r))(a \otimes b) = m_B^*(\lambda_{B^\circ}(r))(a \otimes b) = (\lambda_{B^\circ}(r))m_B(a \otimes b) =$$
$$= \lambda_{B^\circ}(r)(ab) = \lambda_{B^*}(r)(ab) = \varepsilon_B^*(r)(ab) = r\varepsilon_B(ab) = r\varepsilon_B(a)\ \varepsilon_B(b) =$$
$$\underset{(3.1)}{=} r1_{B^*}(a)1_{B^*}(b) = r1_{B^\circ}(a)1_{B^\circ}(b) = r(1_{B^\circ} \otimes 1_{B^\circ})(a \otimes b).$$

We finish with counit $\varepsilon_{B^\circ} : B^\circ \to K$. We need to show that it satisfies

$$\varepsilon_{B^\circ}(fg) = \varepsilon_{B^\circ}(f)\varepsilon_{B^\circ}(g) \ \text{ and } \ \varepsilon_{B^\circ}(\lambda_{B^\circ}(r)) = r.$$

On the one hand, for $f, g \in B^\circ$, $r \in K$, $\varepsilon_{B^\circ}(fg) = \varepsilon_{B^\circ}(f)\varepsilon_{B^\circ}(g)$ holds:

$$\varepsilon_{B^\circ}(fg)(r) = \varepsilon_{B^\circ}(m_{B^\circ}(f \otimes g))(r) = \lambda_B^*(m_{B^\circ}(f \otimes g))(r) =$$
$$= (m_{B^\circ}(f \otimes g))\lambda_B(r) = (m_{B^\circ}(f \otimes g))(r1_B) = r(m_{B^\circ}(f \otimes g))(1_B) =$$
$$= r(m_{B^*}(f \otimes g))(1_B) = r(\Delta_B^*(f \otimes g))(1_B) = r(f \otimes g)(\Delta_B(1_B)) =$$
$$= r(f \otimes g)(1_B \otimes 1_B) = rf(1_B)g(1_B) \underset{(3.2)}{=} r\lambda_B^*(f)\lambda_B^*(g) =$$
$$= r\varepsilon_{B^\circ}(f)\varepsilon_{B^\circ}(g) \underset{(K \cong K^*)}{=} (\varepsilon_{B^\circ}(f)\varepsilon_{B^\circ}(g))(r).$$

On the other hand, for $r, s \in K$, $\varepsilon_{B^\circ}(\lambda_{B^\circ}(r)) = r$ holds:

$$\varepsilon_{B^\circ}(\lambda_{B^\circ}(r))(s) = \lambda_B^*(\lambda_{B^\circ}(r))(s) = (\lambda_{B^\circ}(r))\lambda_B(s) =$$
$$= (\lambda_{B^\circ}(r))(s1_B) = s(\lambda_{B^\circ}(r))(1_B) = s(\lambda_{B^*}(r))(1_B) =$$
$$= s(\varepsilon_B^*(r))(1_B) = sr\varepsilon_B(1_B) = sr1_K = rs \underset{(K \cong K^*)}{=} r(s).$$

Therefore, we conclude that B° is a K-bialgebra. □

4 Hopf algebras and Hopf Galois extensions

In this chapter, we introduce the notion of Hopf algebra. We prove an important result, which states that if H is a finite dimensional vector space, it is a Hopf algebra if, and only if, its linear dual is a Hopf algebra too. Then, we see that there is a Hopf algebra isomorphism between the dual of the group algebra $K[G]$ and the algebra of functions $\mathcal{O}(G)$. Afterwards, we give a characterization of Galois extensions in terms of $K[G]$ and use it to define Hopf Galois extensions. Finally, we discuss a basic example.

4.1 Hopf algebras

In this section, we introduce Hopf algebras, which are bialgebras with an additional map called the coinverse, and give some initial examples. We define convolution, a binary operation on linear transformations, and use it to show that the coinverse is an algebra anti-homomorphism and a coalgebra anti-homomorphism. Afterwards, we define Hopf ideals and discuss quotient Hopf algebras and Hopf algebra homomorphisms. We also prove that if H is finite dimensional, it is a Hopf algebra if, and only if, H^* is also a Hopf algebra. Ultimately, we see that the Hopf algebras $K[G]^*$ and $\mathcal{O}(G)$ are mutually dual.

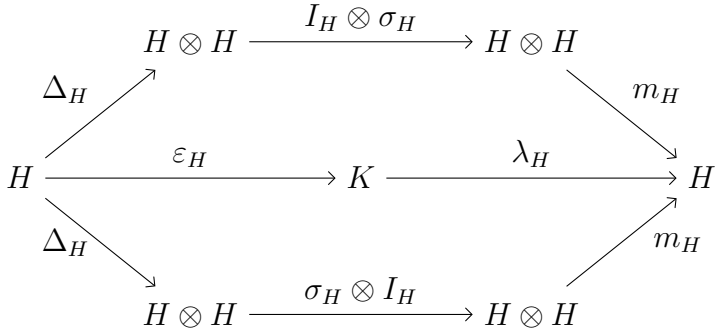
Definition 4.1.1. A K-**Hopf algebra** is a K-bialgebra $H = (H, m_H, \lambda_H, \Delta_H, \varepsilon_H)$ together with a K-linear map $\sigma_H : H \to H$ that satisfies the following condition: for all $h \in H$,

$$m_H(I_H \otimes \sigma_H)\Delta_H(h) = (\lambda_H \varepsilon_H)(h) = \varepsilon_H(h)1_H = m_H(\sigma_H \otimes I_H)\Delta_H(h) \tag{4.1}$$

that is, using Sweedler notation,

$$\sum_{(h)} h_{(1)}\sigma_H(h_{(2)}) = (\lambda_H \varepsilon_H)(h) = \varepsilon_H(h)1_H = \sum_{(h)} \sigma_H(h_{(1)})h_{(2)} \tag{4.2}$$

Equivalently, the following diagram commutes



The map σ_H is called the **coinverse** (or **antipode**) and Condition (4.1) is the **coinverse** (or **antipode**) **property**.

A K-Hopf algebra H is **commutative** if it is a commutative algebra; H is **cocommutative** if it is a cocommutative coalgebra. A K-Hopf algebra that is neither commutative nor cocommutative is a **quantum group**.

Example 4.1.2. The field K is a commutative and cocommutative K-Hopf algebra with coinverse map $\sigma_K : K \to K$ defined as $\sigma_K(r) = r = I_K(r)$. It is called the **trivial K-Hopf algebra**.

Example 4.1.3. Let G be a finite group. From Example 3.1.5, $K[G]$ has the structure of a cocommutative bialgebra. Hence, $K[G]$ is a cocommutative K-Hopf algebra with coinverse map $\sigma_{K[G]} : K[G] \to K[G]$ determined by $\sigma_{K[G]}(g) = g^{-1}$. It is called the **group Hopf algebra**. It is commutative if, and only if, G is abelian.

Example 4.1.4. Let $K[x]$ be the polynomial bialgebra with x primitive (Example 3.1.7), which is commutative and cocommutative. Hence, $K[x]$ is a commutative and cocommutative K-Hopf algebra with coinverse map $\sigma_{K[x]} : K[x] \to K[x]$ determined by $\sigma_{K[x]}(x^i) = (-x)^i$, for $i \geq 0$.

Remark 4.1.5. The polynomial bialgebra with x grouplike (Example 3.1.6) can not be endowed with the structure of a K-Hopf algebra.

In many ways, the group ring $K[G]$ of Example 4.1.3 is the canonical example that is generalized to the concept of Hopf algebra. Clearly, one has that $\sigma_{K[G]} \circ \sigma_{K[G]} = I_{K[G]}$, so the coinverse of $K[G]$ has order 2. We wonder whether we can generalize this result (we can not). However, we will see that there are some properties of Hopf algebras that guarantee that its coinverse map has order 2.

Definition 4.1.6. Let C be a K-coalgebra and A be a K-algebra. Let $\mathrm{Hom}_K(C, A)$ denote the collection of K-linear maps $\phi : C \to A$. We can define a multiplication on $\mathrm{Hom}_K(C, A)$ called **convolution**: for $f, g \in \mathrm{Hom}_K(C, A)$, $c \in C$,

$$(f * g)(c) = (m_A(f \otimes g)\Delta_C)(c) = \sum_{(c)} f(c_{(1)})g(c_{(2)}) \tag{4.3}$$

Proposition 4.1.7. *Let C be a K-coalgebra and let A be a K-algebra. Then $Hom_K(C, A)$ together with $*$ is a monoid.*

Proof. We show that the three axioms for a monoid hold. Firstly, we see that $*$ is an internal binary operation. Indeed, clearly $f * g = m_A \circ (f \otimes g) \circ \Delta_C \in \mathrm{Hom}_K(C, A)$. Secondly, we see that $*$ is associative: for $f, g, h \in \mathrm{Hom}_K(C, A)$, $c \in C$, we have

$$\begin{aligned}
(f * (g * h))(c) &\underset{(4.3)}{=} \sum_{(c)} f(c_{(1)})(g * h)(c_{(2)}) \underset{(4.3)}{=} \sum_{(c)} f(c_{(1)}) \sum_{(c_{(2)})} g(c_{(2)_{(1)}})h(c_{(2)_{(2)}}) = \\
&= \sum_{(c,c_{(2)})} f(c_{(1)})g(c_{(2)_{(1)}})h(c_{(2)_{(2)}}) \underset{(2.7)}{=} \sum_{(c)} f(c_{(1)})g(c_{(2)})h(c_{(3)}) \underset{(2.8)}{=} \\
&= \sum_{(c,c_{(1)})} f(c_{(1)_{(1)}})g(c_{(1)_{(2)}})h(c_{(2)}) = \sum_{(c)} \sum_{(c_{(1)})} f(c_{(1)_{(1)}})g(c_{(1)_{(2)}})h(c_{(2)}) = \\
&\underset{(4.3)}{=} \sum_{(c)} (f * g)(c_{(1)})h(c_{(2)}) \underset{(4.3)}{=} ((f * g) * h)(c).
\end{aligned}$$

Finally, we show that $\lambda_A \circ \varepsilon_C$ is the left and right identity element in $\mathrm{Hom}_K(C, A)$: for $\phi \in \mathrm{Hom}_K(C, A)$, $c \in C$, we have

$$(\lambda_A \varepsilon_C * \phi)(c) \underset{(4.3)}{=} \sum_{(c)} (\lambda_A \varepsilon_C)(c_{(1)})\phi(c_{(2)}) = \sum_{(c)} \lambda_A \underbrace{(\varepsilon_C(c_{(1)}))}_{\in K} \phi(c_{(2)}) =$$

$$= \sum_{(c)} \varepsilon_C(c_{(1)})\lambda_A(1_K)\phi(c_{(2)}) = \sum_{(c)} \varepsilon_C(c_{(1)}) 1_A \underbrace{\phi(c_{(2)})}_{\in A} = \sum_{(c)} \underbrace{\varepsilon_C(c_{(1)})}_{\in K} \phi(c_{(2)}) =$$

$$= \phi\Big(\sum_{(c)} \varepsilon_C(c_{(1)})c_{(2)} \Big) \underset{(2.10)}{=} \phi(c) \Rightarrow \phi * \lambda_A \varepsilon_C = \phi.$$

A similar calculation yields $\lambda_A \varepsilon_C * \phi = \phi$. Thus, we have obtained that

$$1_{(\mathrm{Hom}_K(C,A),*)} = \lambda_A \circ \varepsilon_C \tag{4.4}$$

Therefore, we conclude that $(\mathrm{Hom}_K(C, A), *)$ is a monoid. □

Proposition 4.1.8. *Let H be a K-Hopf algebra and let $Hom_K(H, H)$ be the monoid under convolution $*$. Then $\sigma_H * I_H = \lambda_H \varepsilon_H = I_H * \sigma_H$. In other words, σ_H is a left and right inverse of I_H under $*$.*

Proof. Since H is a K-Hopf algebra, H is both an algebra and a coalgebra. Thus, by the previous proposition, one has that $1_{(\mathrm{Hom}_K(H,H),*)} = \lambda_H \varepsilon_H$ (4.4).

We see that σ_H is a left and right inverse of I_H under $*$: for $h \in H$, we have:

$$(\sigma_H * I_H)(h) \underset{(4.3)}{=} m_H(\sigma_H \otimes I_H)\Delta_H(h) \underset{(4.1)}{=} (\lambda_H \varepsilon_H)(h) \underset{(4.1)}{=} m_H(I_H \otimes \sigma_H)\Delta_H(h) =$$

$$\underset{(4.3)}{=} (I_H * \sigma_H)(h) \Rightarrow \sigma_H * I_H = \lambda_H \varepsilon_H = I_H * \sigma_H.$$

Therefore, we conclude that σ_H is a left and right inverse of I_H under $*$. □

Convolution can be used to show that the coinverse map is an algebra antihomomorphism and so to set that the coinverse is an algebra homomorphism whenever the Hopf algebra is commutative.

Proposition 4.1.9. *Let H be a K-Hopf algebra with coinverse map σ_H. Then the following properties hold:*

1. *$\sigma_H(ab) = \sigma_H(b)\sigma_H(a)$, for all $a, b \in H$,*
2. *$\sigma_H(1_H) = 1_H$.*

Proof. Firstly, we see that $\sigma_H(ab) = \sigma_H(b)\sigma_H(a)$. Since H is a Hopf algebra, it is a coalgebra, and so $H \otimes H$ is also a coalgebra (Definition 2.2.23), with comultiplication $\Delta_{H\otimes H} = (I_H \otimes \tau \otimes I_H)(\Delta_H \otimes \Delta_H)$ given by $\Delta_{H\otimes H}(a \otimes b) = \sum_{(a,b)} a_{(1)} \otimes b_{(1)} \otimes a_{(2)} \otimes b_{(2)}$, and counit $\varepsilon_{H\otimes H}$ defined as $\varepsilon_{H\otimes H}(a \otimes b) = \varepsilon_H(a)\varepsilon_H(b)$. Moreover, since H is a Hopf algebra, it is an algebra, so we consider $\mathrm{Hom}_K(H \otimes H, H)$. Recall that $\lambda_H \varepsilon_{H\otimes H} = 1_{(\mathrm{Hom}_K(H\otimes H,H),*)}$ (4.4). Note that $m_H \in \mathrm{Hom}_K(H \otimes H, H)$.

We define two additional elements of $\mathrm{Hom}_K(H \otimes H, H)$ as follows:

$$\begin{array}{rccc} \sigma_H m_H: & H \otimes H & \to & H \\ & a \otimes b & \mapsto & \sigma_H(ab) \end{array}$$

$$\begin{array}{rccc} \phi = m_H(\sigma_H \otimes \sigma_H)\tau: & H \otimes H & \to & H \\ & a \otimes b & \mapsto & \sigma_H(b)\sigma_H(a) \end{array}$$

Note that, if we prove $\phi = \sigma_H m_H$, we have already finished. In order to show it, we will see that the following equations hold

$$m_H * \phi = \lambda_H \varepsilon_{H\otimes H} = \phi * m_H \tag{4.5}$$

$$m_H * \sigma_H m_H = \lambda_H \varepsilon_{H\otimes H} = \sigma_H m_H * m_H \tag{4.6}$$

On the one hand, we prove (4.5): for $a, b \in H$, we have

$$(m_H * \phi)(a \otimes b) \underset{(4.3)}{=} m_H(m_H \otimes \phi)\Delta_{H\otimes H}(a \otimes b) =$$

$$= m_H(m_H \otimes \phi)\Big(\sum_{(a,b)} a_{(1)} \otimes b_{(1)} \otimes a_{(2)} \otimes b_{(2)}\Big) =$$

$$= m_H\Big(\sum_{(a,b)} m_H(a_{(1)} \otimes b_{(1)}) \otimes \phi(a_{(2)} \otimes b_{(2)})\Big) =$$

$$= m_H\Big(\sum_{(a,b)} a_{(1)}b_{(1)} \otimes \sigma_H(b_{(2)})\sigma_H(a_{(2)})\Big) =$$

$$= \sum_{(a,b)} a_{(1)}b_{(1)}\sigma_H(b_{(2)})\sigma_H(a_{(2)}) = \sum_{(a)} a_{(1)}\Big(\sum_{(b)} b_{(1)}\sigma_H(b_{(2)})\Big)\sigma_H(a_{(2)}) =$$

$$\underset{(4.2)}{=} \sum_{(a)} a_{(1)}\underbrace{\varepsilon_H(b)}_{\in K}1_H\underbrace{\sigma_H(a_{(2)})}_{\in H} = \varepsilon_H(b)\sum_{(a)} a_{(1)}\sigma_H(a_{(2)}) \underset{(4.2)}{=} \underbrace{\varepsilon_H(b)}_{\in K}\underbrace{\varepsilon_H(a)}_{\in K}1_H =$$

$$= \varepsilon_H(a)\varepsilon_H(b)1_H = \varepsilon_{H\otimes H}(a \otimes b)1_H = \lambda_H(\varepsilon_{H\otimes H}(a \otimes b)) = (\lambda_H\varepsilon_{H\otimes H})(a \otimes b).$$

A similar calculation yields $\phi * m_H = \lambda_H \varepsilon_{H\otimes H}$, and so (4.5) holds.

On the other hand, we prove (4.6): for $a, b \in H$, we have

$$(m_H * \sigma_H m_H)(a \otimes b) \underset{(4.3)}{=} m_H(m_H \otimes \sigma_H m_H)\Delta_{H\otimes H}(a \otimes b) =$$

$$= m_H(m_H \otimes \sigma_H m_H)\Big(\sum_{(a,b)} a_{(1)} \otimes b_{(1)} \otimes a_{(2)} \otimes b_{(2)}\Big) =$$

$$= m_H\Big(\sum_{(a,b)} m_H(a_{(1)} \otimes b_{(1)}) \otimes (\sigma_H m_H)(a_{(2)} \otimes b_{(2)})\Big) =$$

$$= m_H\Big(\sum_{(a,b)} a_{(1)}b_{(1)} \otimes \sigma_H(a_{(2)}b_{(2)})\Big) = \sum_{(a,b)} a_{(1)}b_{(1)}\sigma_H(a_{(2)}b_{(2)}) \underset{(4.2)}{=} \varepsilon_H(ab)1_H =$$

$$= \varepsilon_H(a)\varepsilon_H(b)1_H = \varepsilon_{H\otimes H}(a \otimes b)1_H = \lambda_H(\varepsilon_{H\otimes H}(a \otimes b)) = (\lambda_H\varepsilon_{H\otimes H})(a \otimes b).$$

A similar calculation yields $\sigma_H m_H * m_H = \lambda_H \varepsilon_{H\otimes H}$, and so (4.6) holds.

Now, from (4.5) and (4.6), we obtain

$$m_H * \phi = m_H * \sigma_H m_H \Rightarrow \phi * (m_H * \phi) = \phi * (m_H * \sigma_H m_H) \Rightarrow$$

$$\Rightarrow (\phi * m_H) * \phi = (\phi * m_H) * \sigma_H m_H \underset{(4.5)}{\Rightarrow} \lambda_H \varepsilon_{H\otimes H} * \phi = \lambda_H \varepsilon_{H\otimes H} * \sigma_H m_H \Rightarrow$$

$$\underset{(4.4)}{\Rightarrow} 1_{(\mathrm{Hom}_K(H\otimes H,H),*)} * \phi = 1_{(\mathrm{Hom}_K(H\otimes H,H),*)} * \sigma_H m_H \Rightarrow \phi = \sigma_H m_H.$$

Finally, we show that $\sigma_H(1_H) = 1_H$. Indeed,

$$1_H = 1_K 1_H = \varepsilon_H(1_H)1_H \underset{(4.1)}{=} m_H(I_H \otimes \sigma_H)\Delta_H(1_H) =$$

$$= m_H(I_H \otimes \sigma_H)(1_H \otimes 1_H) = m_H(1_H \otimes \sigma_H(1_H)) = 1_H \underbrace{\sigma_H(1_H)}_{\in H} = \sigma_H(1_H).$$

Therefore, we conclude that σ_H is an algebra antihomomorphism. □

Corollary 4.1.10. *Let H be a K-Hopf algebra with coinverse map σ_H. If H is cocommutative, then $\sigma_H^2 = I_H$ (that is, σ_H has order 2).*

Proof. Since H is cocommutative, the equation $\tau\Delta_H = \Delta_H$ holds. We consider $Hom_K(H,H)$ endowed with convolution $*$. Note that σ_H, σ_H^2, I_H and $\lambda_H\varepsilon_H$ are all elements of $Hom_K(H,H)$. Thus, for $h \in H$, we have

$$(\sigma_H * \sigma_H^2)(h) \underset{(4.3)}{=} m_H(\sigma_H \otimes \sigma_H^2)\Delta_H(h) = m_H(\sigma_H \otimes \sigma_H^2)\tau\Delta_H(h) =$$

$$= m_H(\sigma_H \otimes \sigma_H^2)\tau\Big(\sum_{(h)} h_{(1)} \otimes h_{(2)}\Big) = m_H(\sigma_H \otimes \sigma_H^2)\Big(\sum_{(h)} h_{(2)} \otimes h_{(1)}\Big) =$$

$$= m_H\Big(\sum_{(h)} \sigma_H(h_{(2)}) \otimes \sigma_H(\sigma_H(h_{(1)}))\Big) = \sum_{(h)} \sigma_H(h_{(2)})\sigma_H(\sigma_H(h_{(1)})) =$$

$$\underset{\text{(Prop 4.1.9, 1)}}{=} \sum_{(h)} \sigma_H(\sigma_H(h_{(1)})h_{(2)}) = \sigma_H\Big(\sum_{(h)} \sigma_H(h_{(1)})h_{(2)}\Big) =$$

$$\underset{(4.2)}{=} \sigma_H(\underbrace{\varepsilon_H(h)}_{\in K} 1_H) = \varepsilon_H(h)\sigma_H(1_H) \underset{\text{(Prop 4.1.9, 2)}}{=} \underbrace{\varepsilon_H(h)}_{\in K} 1_H =$$

$$= \lambda_H(\varepsilon_H(h)) = (\lambda_H\varepsilon_H)(h) \Rightarrow \sigma_H * \sigma_H^2 = \lambda_H\varepsilon_H \underset{(4.4)}{=} 1_{(\mathrm{Hom}_K(H,H),*)}.$$

On the one hand,

$$I_H * (\sigma_H * \sigma_H^2) = I_H * 1_{(\mathrm{Hom}_K(H,H),*)} = I_H.$$

On the other hand,

$$I_H * (\sigma_H * \sigma_H^2) = (I_H * \sigma_H) * \sigma_H^2 \underset{\text{(Prop 4.1.8)}}{=} (\lambda_H\varepsilon_H) * \sigma_H^2 \underset{(4.4)}{=} 1_{(\mathrm{Hom}_K(H,H),*)} * \sigma_H^2 = \sigma_H^2.$$

Therefore, we conclude that $I_H = \sigma_H^2$. □

Analogously, convolution can be used to show that the coinverse map is a coalgebra antihomomorphism and hence to state that the coinverse is a coalgebra homomorphism whenever the Hopf algebra is cocommutative (we are not going to prove this because the proofs are very similar to the previous ones).

Proposition 4.1.11. *Let H be a K-Hopf algebra with coinverse map σ_H. Then the following properties hold:*

1. $\tau(\sigma_H \otimes \sigma_H)\Delta_H = \Delta_H \sigma_H$,
2. $\varepsilon_H \sigma_H = \varepsilon_H$.

Corollary 4.1.12. *Let H be a K-Hopf algebra with coinverse map σ_H. If H is commutative, then $\sigma_H^2 = I_H$ (that is, σ_H has order 2).*

Definition 4.1.13. Let H, H' be K-Hopf algebras. Since H and H' are bialgebras, $H \otimes H'$ is a bialgebra (Definition 3.1.8). Therefore, the **tensor product of Hopf algebras** $H \otimes H'$ has the structure of a K-Hopf algebra with coinverse map defined as

$$\begin{array}{rccc} \sigma_{H\otimes H'}: & H \otimes H' & \to & H \otimes H' \\ & a \otimes b & \mapsto & (\sigma_H \otimes \sigma_{H'})(a \otimes b) = \sigma_H(a) \otimes \sigma_{H'}(b) \end{array}$$

Definition 4.1.14. Let H be a K-Hopf algebra. A subspace $I \subseteq H$ is a **Hopf ideal** of H if it is a biideal that satisfies $\sigma_H(I) \subseteq I$.

Proposition 4.1.15. *Let H be a K-Hopf algebra and let I be a Hopf ideal of H. Then the quotient space H/I is a K-Hopf algebra.*

Proof. By Proposition 3.1.10, H/I is a K-bialgebra. Recall that multiplication is defined as $m_{H/I}([a]_I \otimes [b]_I) = [ab]_I$, unit is given by $\lambda_{H/I}(r) = [\lambda_H(r)]_I$, comultiplication is defined as $\Delta_{H/I}([h]_I) = \sum_{(h)} [h_{(1)}]_I \otimes [h_{(2)}]_I$ and counit is given by $\varepsilon_{H/I}([h]_I) = \varepsilon_H(h)$. So, we need to define a coinverse map $\sigma_{H/I}$ which satisfies the coinverse property. The following diagram illustrates the idea of the proof:

$$\begin{array}{ccc} I & \xrightarrow{\sigma_H} & I \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ H/I & \xrightarrow{\sigma_{H/I}} & H/I \end{array}$$

Since I is a K-Hopf ideal, $\sigma_H(I) \subseteq I$, and considering the canonical surjection $\pi : I \to H/I$ as K-vector spaces, σ_H induces a K-linear map $\sigma_{H/I} : H/I \to H/I$ defined as $\sigma_{H/I}([h]_I) = [\sigma_H(h)]_I$. We see that $\sigma_{H/I}$ satisfies the coinverse property: for $[h]_I \in H/I$, we have

$$m_{H/I}(\sigma_{H/I} \otimes I_{H/I})\Delta_{H/I}([h]_I) = m_{H/I}(\sigma_{H/I} \otimes I_{H/I})\left(\sum_{(h)} [h_{(1)}]_I \otimes [h_{(2)}]_I\right) =$$

$$= m_{H/I}\left(\sum_{(h)} \sigma_{H/I}([h_{(1)}]_I) \otimes I_{H/I}([h_{(2)}]_I)\right) = m_{H/I}\left(\sum_{(h)} [\sigma_H(h_{(1)})]_I \otimes [h_{(2)}]_I\right) =$$

$$= \sum_{(h)} [\sigma_H(h_{(1)})h_{(2)}]_I = \Big[\sum_{(h)} \sigma_H(h_{(1)})h_{(2)} \Big]_I \underset{(4.2)}{=} [\underbrace{\varepsilon_H(h)}_{\in K} 1_H]_I = \varepsilon_H(h)[1_H]_I =$$
$$= \varepsilon_H(h)1_{H/I} = \varepsilon_{H/I}([h]_I)1_{H/I} \Rightarrow m_{H/I}(\sigma_{H/I} \otimes I_{H/I})\Delta_{H/I}([h]_I) = \varepsilon_{H/I}([h]_I)1_{H/I}.$$

Similarly, one has $m_{H/I}(I_{H/I} \otimes \sigma_{H/I})\Delta_{H/I}([h]_I) = \varepsilon_{H/I}([h]_I)1_{H/I}$. Therefore, we conclude that H/I is a K-Hopf algebra. □

Definition 4.1.16. Let H be a K-Hopf algebra and let I be a Hopf ideal of H. The K-Hopf algebra H/I of the previous proposition is the **quotient Hopf algebra** of H by I.

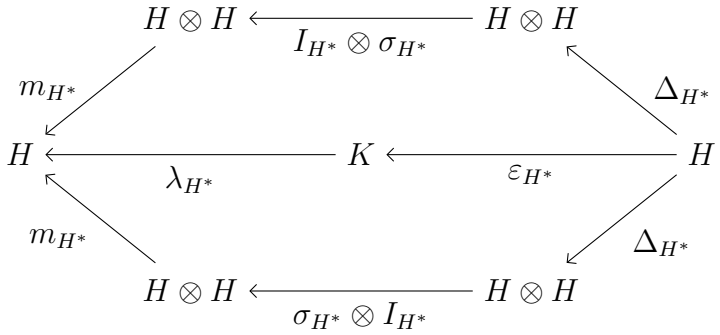
Definition 4.1.17. Let H, H' be K-Hopf algebras with coinverse maps $\sigma_H, \sigma_{H'}$ (resp.). A **K-Hopf algebra homomorphism** from H to H' is a map $\phi : H \to H'$ that is a K-bialgebra homomorphism and verifies $\phi(\sigma_H(h)) = \sigma_{H'}(\phi(h))$, for all $h \in H$. A K-Hopf algebra homomorphism that is injective and surjective is a **K-Hopf algebra isomorphism**.

Now, we prove one of the main results of this section.

Theorem 4.1.18. *Let H be a finite dimensional K-vector space. Then H is a K-Hopf algebra if, and only if, H^* is a K-Hopf algebra.*

Proof. Since H is finite dimensional, by Proposition 2.3.6, $H^\circ = H^*$. Since H is a Hopf algebra, it is a bialgebra, and by Theorem 3.3.3, H^* is also a bialgebra. So we need to define a coinverse map σ_{H^*} which satisfies the coinverse property. We consider the transpose of σ_H, $\sigma_H^* : H^* \to H^*$, which is a K-linear map defined as $\sigma_H^*(f) = f \circ \sigma_H$. Set $\sigma_{H^*} = \sigma_H^*$.

Observe that if we dualize the commutative diagram of the definition of the Hopf algebra H, we obtain the commutative diagram of the definition of the Hopf algebra H^*



Conversely if H^* is a K-Hopf algebra, by the argument done before, $H^{**} = H$ is a K-Hopf algebra. □

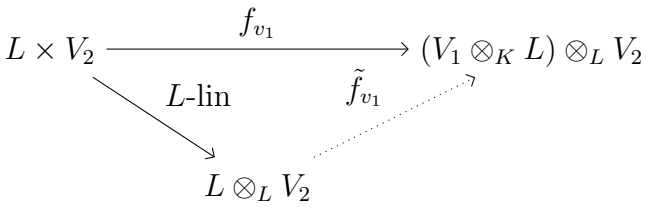
Now, we are going to do the scalar extension of a Hopf algebra, which will be useful later on. But first of all, we need to observe the following things.

Remark 4.1.19. Let $L|K$ be a field extension and let V be a vector space over K. Since L is a K-vector space too, $V \otimes_K L$ is clearly a K-vector space. Moreover, $V \otimes_K L$ is an L-vector space with scalar multiplication defined as $\lambda(v \otimes_K r) = v \otimes_K \lambda r$, for all $\lambda \in L$, $v \otimes_K r \in V \otimes_K L$. Hence, if $f : V_1 \to V_2$ is a K-linear map, then $f \otimes I_L : V_1 \otimes_K L \to V_2 \otimes_K L$ is an L-linear map.

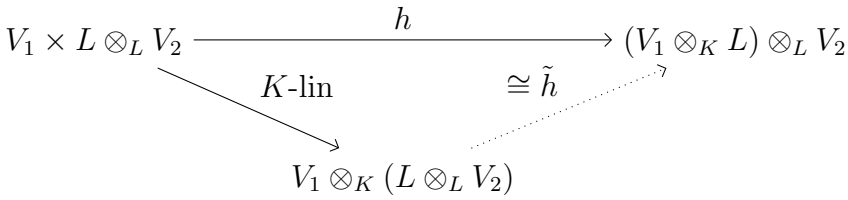
Lemma 4.1.20. *Let $L|K$ be a field extension. Let V_1 be a K-vector space and let V_2 be an L-vector space. Then there exists a K-vector space isomorphism*

$$(V_1 \otimes_K L) \otimes_L V_2 \cong V_1 \otimes_K (L \otimes_L V_2) \tag{4.7}$$

Proof. Recall that, by the previous remark, $V_1 \otimes_K L$ is an L-vector space. For every $v_1 \in V_1$, there is an L-bilinear map $f_{v_1} : L \times V_2 \to (V_1 \otimes_K L) \otimes_L V_2$ defined as $f_{v_1}(r, v_2) = (v_1 \otimes_K r) \otimes_L v_2$. Thus, by the definition of tensor product, there exists an L-linear map $\tilde{f}_{v_1}$ as follows



Furthermore, there is a K-bilinear map $h : V_1 \times L \otimes_L V_2 \to (V_1 \otimes_K L) \otimes_L V_2$ given by $h(v_1, \alpha) = \tilde{f}_{v_1}(\alpha)$. Thus, by the definition of tensor product, there exists a K-linear map $\tilde{h}$ as follows



Since the elements of the form $v_1 \otimes_K (r \otimes_L v_2)$ generate $V_1 \otimes_K (L \otimes_L V_2)$ and the elements of the form $(v_1 \otimes_K r) \otimes_L v_2$ generate $(V_1 \otimes_K L) \otimes_L V_2$, $\tilde{h}$ is a K-vector space isomorphism, and we conclude that $(V_1 \otimes_K L) \otimes_L V_2 \cong V_1 \otimes_K (L \otimes_L V_2)$. □

Proposition 4.1.21. *Let H be a K-Hopf algebra and let L be a field extension of K. Then $H \otimes_K L$ is an L-Hopf algebra.*

Proof. Note that by the associativity of tensor product, we have

$$(H \otimes_K L) \otimes_L \underbrace{(H \otimes_K L)}_{L-\text{vector space}} \underset{(4.7)}{\cong} H \otimes_K (L \otimes_L \underbrace{(H \otimes_K L)}_{L-\text{vector space}}) \cong$$
$$\underset{(2.11)}{\cong} H \otimes_K (H \otimes_K L) \cong (H \otimes_K H) \otimes_K L.$$

By construction, this is a K-vector space isomorphism (Lemma 4.1.20), but furthermore, it is an L-vector space isomorphism (Remark 4.1.19). Now, we define multiplication, unit, comultiplication, counit and coinverse maps:

1. $m_{H\otimes_K L} : (H \otimes_K L) \otimes_L (H \otimes_K L) \cong (H \otimes_K H) \otimes_K L \to H \otimes_K L$ is defined as $m_{H\otimes_K L} = m_H \otimes I_L$,
2. $\lambda_{H\otimes_K L} : L \cong (K \otimes_K L) \to H \otimes_K L$ is given by $\lambda_{H\otimes_K L} = \lambda_H \otimes I_L$,
3. $\Delta_{H\otimes_K L} : H \otimes_K L \to (H \otimes_K L) \otimes_L (H \otimes_K L) \cong (H \otimes_K H) \otimes_K L$ is defined as $\Delta_{H\otimes_K L} = \Delta_H \otimes I_L$,
4. $\varepsilon_{H\otimes_K L} : H \otimes_K L \to L$ is given by $\varepsilon_{H\otimes_K L} = \varepsilon_H \otimes I_L$,
5. $\sigma_{H\otimes_K L} : H \otimes_K L \to H \otimes_K L$ is defined as $\sigma_{H\otimes_K L} = \sigma_H \otimes I_L$.

By definition, they are K-linear maps, but furthermore, they are L-linear maps (Remark 4.1.19). It is easy to check that they satisfy multiplication, unit, comultiplication, counit and coinverse properties, respectively, since $m_H, \lambda_H, \Delta_H, \varepsilon_H, \sigma_H$ do. Hence, we conclude that $H \otimes_K L$ is an L-Hopf algebra. □

We close this section with an example of a dual Hopf algebra.

Proposition 4.1.22. *Let G be a finite group. There exists a K-Hopf algebra isomorphism between $K[G]^*$ and $\mathcal{O}(G) := K^G = \{f : G \to K\}$.*

Proof. We start considering $\mathcal{O}(G)$ with basis $\{e_g : g \in G\}$, where $e_g(h) := \delta_{g,h}$. Note that $\mathcal{O}(G)$ is a K-vector space with operations defined from those of K. We define multiplication, unit, comultiplication, counit and coinverse maps:

1. $m_{\mathcal{O}(G)} : \mathcal{O}(G) \otimes \mathcal{O}(G) \to \mathcal{O}(G)$ is determined by $m_{\mathcal{O}(G)}(e_g \otimes e_h) = \delta_{g,h} e_g$, that is, $m_{\mathcal{O}(G)}(e_g \otimes e_h)(f) = \delta_{g,h} e_g(f) = \delta_{g,h}\delta_{g,f}$;
2. $\lambda_{\mathcal{O}(G)} : K \to \mathcal{O}(G)$ is defined as $\lambda_{\mathcal{O}(G)}(r) = \sum_{g\in G} r e_g$, that is, $\lambda_{\mathcal{O}(G)}(r)(g) = r$;
3. $\Delta_{\mathcal{O}(G)} : \mathcal{O}(G) \to \mathcal{O}(G) \otimes \mathcal{O}(G)$ is determined by $\Delta_{\mathcal{O}(G)}(e_g) = \sum_{uv=g} e_u \otimes e_v$, that is, $\Delta_{\mathcal{O}(G)}(e_g)(h_1 \otimes h_2) = \sum_{uv=g} e_u(h_1) e_v(h_2) = \sum_{uv=g} \delta_{u,h_1}\delta_{v,h_2} = \delta_{g,h_1h_2}$;
4. $\varepsilon_{\mathcal{O}(G)} : \mathcal{O}(G) \to K \cong K^*$ is determined by $\varepsilon_{\mathcal{O}(G)}(e_g) = \delta_{g,1_G}$, that is, $\varepsilon_{\mathcal{O}(G)}(e_g)(r) = r\delta_{g,1_G}$;
5. $\sigma_{\mathcal{O}(G)} : \mathcal{O}(G) \to \mathcal{O}(G)$ is determined by $\sigma_{\mathcal{O}(G)}(e_g) = e_{g^{-1}}$, that is, $\sigma_{\mathcal{O}(G)}(e_g)(h) = e_{g^{-1}}(h) = \delta_{g^{-1},h}$.

It is easy to check that they satisfy multiplication, unit, comultiplication, counit and coinverse properties, respectively. Hence, $\mathcal{O}(G)$ is a K-Hopf algebra.

Now, we consider the K-Hopf algebra $K[G]$ (Example 4.1.3), with multiplication defined as $m_{K[G]}(g \otimes h) = gh$, unit given by $\lambda_{K[G]}(r) = r1_G$, comultiplication defined as $\Delta_{K[G]}(g) = g \otimes g$, counit given by $\varepsilon_{K[G]}(g) = 1_K$, and coinverse defined as $\sigma_{K[G]}(g) = g^{-1}$. Its canonical basis is $\mathcal{B} = \{g : g \in G\}$.

We consider its linear dual $K[G]^* = \{K[G] \to K \text{ linear}\}$. The dual basis of $\mathcal{B}$ is $\{\omega^g : \omega^g(h) = \delta_{g,h}, \text{ for } g \in G\}$. The map sending e_g to ω^g is a K-vector space isomorphism from $\mathcal{O}(G)$ onto $K[G]^*$. Thus, from now on, we identify both of them by means of this isomorphism.

Recall that, since $K[G]$ is finite dimensional as a K-vector space, by Remark 2.3.9, $(K[G] \otimes K[G])^* = K[G]^* \otimes K[G]^*$. So, it remains to show that $m^*_{K[G]} = \Delta_{\mathcal{O}(G)}$, $\lambda^*_{K[G]} = \varepsilon_{\mathcal{O}(G)}$, $\Delta^*_{K[G]} = m_{\mathcal{O}(G)}$, $\varepsilon^*_{K[G]} = \lambda_{\mathcal{O}(G)}$ and $\sigma^*_{K[G]} = \sigma_{\mathcal{O}(G)}$. Indeed,

1. $m^*_{K[G]} : K[G]^* \to K[G]^* \otimes K[G]^*$, $m^*_{K[G]}(\omega^g) \mapsto \omega^g \circ m_{K[G]}$ satisfies

$$m^*_{K[G]}(\omega^g)(h_1 \otimes h_2) = \omega^g(m_{K[G]}(h_1 \otimes h_2)) = \omega^g(h_1 h_2) = \\ = \delta_{g,h_1h_2} = \Delta_{\mathcal{O}(G)}(e_g)(h_1 \otimes h_2);$$

2. $\lambda^*_{K[G]} : K[G]^* \to K \cong K^*$, $\lambda^*_{K[G]}(\omega^g) \mapsto \omega^g \circ \lambda_{K[G]}$ satisfies

$$\lambda^*_{K[G]}(\omega^g)(r) = \omega^g(\lambda_{K[G]}(r)) = \omega^g(r1_G) = r\omega^g(1_G) = r\delta_{g,1_G} = \varepsilon_{\mathcal{O}(G)}(e_g)(r);$$

3. $\Delta^*_{K[G]} : K[G]^* \otimes K[G]^* \to K[G]^*$, $\Delta^*_{K[G]}(\omega^g \otimes \omega^h) \mapsto (\omega^g \otimes \omega^h) \circ \Delta_{K[G]}$ satisfies

$$\Delta^*_{K[G]}(\omega^g \otimes \omega^h)(f) = (\omega^g \otimes \omega^h)(\Delta_{K[G]}(f)) = (\omega^g \otimes \omega^h)(f \otimes f) = \\ = \omega^g(f) \otimes \omega^h(f) = \delta_{g,f}\delta_{h,f} = \delta_{g,h}\delta_{g,f} = m_{\mathcal{O}(G)}(e_g \otimes e_h)(f);$$

4. $\varepsilon^*_{K[G]} : K \to K[G]^*$, $\varepsilon^*_{K[G]}(r) = r\varepsilon_{K[G]}$ satisfies

$$\varepsilon^*_{K[G]}(r)(g) = r\varepsilon_{K[G]}(g) = r1_K = r = \lambda_{\mathcal{O}(G)}(r)(g);$$

5. $\sigma^*_{K[G]} : K[G]^* \to K[G]^*$, $\sigma^*_{K[G]}(\omega^g) = \omega^g \circ \sigma_{K[G]}$ satisfies

$$\sigma^*_{K[G]}(\omega^g)(h) = \omega^g(\sigma_{K[G]}(h)) = \omega^g(h^{-1}) = \delta_{g,h^{-1}} = \delta_{g^{-1},h} = \sigma_{\mathcal{O}(G)}(e_g)(h).$$

Therefore, the Hopf algebras $K[G]^*$ and $\mathcal{O}(G)$ are mutually dual. □

4.2 Hopf Galois extensions

In this section, we prove that L is a Galois extension of K with group G if, and only if, it is a Galois $K[G]$-extension of K. This leads us to define Hopf Galois extensions and to give the fundamental theorem of Hopf Galois theory. Finally, we give a typical example of a Hopf Galois extension which is not Galois.

Let L be a finite field extension of K. Let $\mathrm{Aut}_K L$ denote the group of field automorphisms of L that fix K elementwise and let G be a subgroup of $\mathrm{Aut}_K L$. Recall that $K[G]$ is a K-Hopf algebra (Example 4.1.3).

Observe L is a left $K[G]$-module with scalar multiplication given by

$$\left(\sum_{g\in G} a_g g\right)\cdot x = \sum_{g\in G} a_g g(x), \text{ for all } a_g \in K,\ x \in L.$$

Proposition 4.2.1. *Let $L|K$ be a finite extension and let G be a subgroup of $Aut_K L$. Then L is a left $K[G]$-module algebra.*

Proof. Recall that $K[G]$ is a K-Hopf algebra (Example 4.1.3), with comultiplication defined as $\Delta(g) = g \otimes g$, and counit given by $\varepsilon(g) = 1_K$. Recall also that L is an algebra (Example 2.2.6) and a left $K[G]$-module. We need to prove that, for all $h \in K[G], x, y \in L$, it is verified

$$h\cdot(xy) = \sum_{(h)} (h_{(1)}\cdot x)(h_{(2)}\cdot y) \quad \text{and} \quad h\cdot 1_L = \varepsilon(h)1_L.$$

Let $h = \sum_{g\in G} a_g g$, $x, y \in L$. Note that

$$\Delta(h) = \Delta\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g\ g\otimes g = \sum_{(h)} h_{(1)}\otimes h_{(2)} \Rightarrow h_{(1)} = a_g g,\ h_{(2)} = g.$$

On the one hand,

$$h\cdot(xy) = \left(\sum_{g\in G} a_g g\right)\cdot(xy) = \sum_{g\in G} a_g g(xy) = \sum_{g\in G} a_g g(x)g(y) =$$
$$= \sum_{g\in G} a_g (g\cdot x)(g\cdot y) = \sum_{g\in G} (a_g g\cdot x)(g\cdot y) = \sum_{g\in G} (h_{(1)}\cdot x)(h_{(2)}\cdot y).$$

On the other hand,

$$h\cdot 1_L = \left(\sum_{g\in G} a_g g\right)\cdot 1_L = \sum_{g\in G} a_g g(1_L) = \sum_{g\in G} a_g 1_L = \left(\sum_{g\in G} a_g\right)1_L = \varepsilon(h)1_L.$$

We conclude that L is a left $K[G]$-module algebra. □

Now, we give a characterization of Galois extensions. First of all, we need the next lemma.

Lemma 4.2.2. *The elements of G form a linearly independent set of vectors over L.*

Proof. Since $L|K$ is a finite extension and $G \leq \mathrm{Aut}_K L$, then G is finite, so we write $G = \{g_1, \ldots, g_n\}$. Reduction to absurdity. If $\{g_1, \ldots, g_n\}$ is not linearly independent over L, there exists a smallest positive integer $m \in \{1, \ldots, n\}$, a set of distinct integers $i_1, \ldots, i_m \in \{1, \ldots, n\}$ and non-zero coefficients $a_1, \ldots, a_m \in L$ for which

$$a_1 g_{i_1} + \cdots + a_m g_{i_m} = 0 \tag{4.8}$$

Since $g_{i_{m-1}} \neq g_{i_m}$, there exists a non-zero element $y \in L$ such that $g_{i_{m-1}}(y) \neq g_{i_m}(y)$, and so $g_{i_m}(y) \neq 0$. Now, note that, for any $x \in L$, we have

$$\begin{gathered} a_1 g_{i_1}(yx) + \cdots + a_{m-1} g_{i_{m-1}}(yx) + a_m g_{i_m}(yx) = 0 \Rightarrow \\ \Rightarrow a_1 g_{i_1}(y) g_{i_1}(x) + \cdots + a_{m-1} g_{i_{m-1}}(y) g_{i_{m-1}}(x) + a_m g_{i_m}(y) g_{i_m}(x) = 0 \Rightarrow \\ \Rightarrow a_1 g_{i_1}(y) g_{i_1} + \cdots + a_{m-1} g_{i_{m-1}}(y) g_{i_{m-1}} + a_m g_{i_m}(y) g_{i_m} = 0, \end{gathered}$$

and so,

$$a_1 g_{i_1}(y) g_{i_1} + \cdots + a_{m-1} g_{i_{m-1}}(y) g_{i_{m-1}} + a_m g_{i_m}(y) g_{i_m} = 0 \tag{4.9}$$

Now, dividing (4.9) by $g_{i_m}(y)$, which is non-zero, one has

$$a_1 \frac{g_{i_1}(y)}{g_{i_m}(y)} g_{i_1} + \cdots + a_{m-1} \frac{g_{i_{m-1}}(y)}{g_{i_m}(y)} g_{i_{m-1}} + a_m g_{i_m} = 0,$$

and substracting (4.8) gives

$$\underbrace{\left(a_1 \frac{g_{i_1}(y)}{g_{i_m}(y)} - a_1\right)}_{\in L} g_{i_1} + \cdots + \underbrace{\left(a_{m-1} \frac{g_{i_{m-1}}(y)}{g_{i_m}(y)} - a_{m-1}\right)}_{\in L} g_{i_{m-1}} = 0$$

Finally, by hypothesis, $a_{m-1} \neq 0$, and since $g_{i_{m-1}}(y) \neq g_{i_m}(y)$, $\frac{g_{i_{m-1}}(y)}{g_{i_m}(y)} \neq 1$. Thus, we obtain $a_{m-1} \frac{g_{i_{m-1}}(y)}{g_{i_m}(y)} - a_{m-1} \neq 0$, and so we have a contradiction of the minimality of m. Therefore, we conclude that G is linearly independent. □

Since the field L is a K-vector space, we consider $\mathrm{End}_K L = \mathrm{Hom}_K(L, L)$, which is a K-vector space with addition defined pointwise as $(\phi+\psi)(x) = \phi(x) + \psi(x)$, and scalar multiplication given pointwise by $(r\phi)(x) = r\phi(x)$, for $\phi, \psi \in \mathrm{Hom}_K(L, L)$, $r \in K$, $x \in L$. Since $G \leq \mathrm{Aut}_K L$, G is a subgroup of $\mathrm{End}_K L$. Hence, there is a K-linear map

$$\begin{array}{rccl} \varphi: & L \otimes_K K[G] & \to & \mathrm{End}_K L \\ & x \otimes g & \mapsto & \varphi(x \otimes g): \ L \to L \\ & & & \qquad\qquad y \mapsto \varphi(x \otimes g)(y) = x(g \cdot y) = xg(y) \end{array}$$

Theorem 4.2.3. *Let K be a field of characteristic 0. Let $L|K$ be a finite extension and let G be a subgroup of $Aut_K L$. Then the map $\varphi : L \otimes_K K[G] \to End_K L$ is a bijection if, and only if, L is a Galois extension of K with group G.*

Proof. Let $G = \{g_1, \ldots, g_n\}$. Suppose that $G = \mathrm{Gal}(L|K)$. We need to show that φ is a bijection. Firstly, we see that it is an injection. It suffices to prove $\mathrm{Ker}(\varphi) = 0$. Indeed, let $\sum_{i=1}^{n} a_i g_i \in K[G]$, $x, y \in L$, and suppose

$$\varphi\left(x \otimes \sum_{i=1}^{n} a_i g_i\right)(y) = x\left(\sum_{i=1}^{n} a_i g_i \cdot y\right) = x\left(\sum_{i=1}^{n} a_i g_i(y)\right) = \sum_{i=1}^{n} x a_i g_i(y) = 0.$$

By Lemma 4.2.2, $\{g_1, \ldots, g_n\}$ is linearly independent over L. Thus $xa_i = 0$, for all $i \in \{1, \ldots, n\}$, and so $x = 0$ or $a_i = 0$, for all $i \in \{1, \ldots, n\}$. Consequently $x \otimes \sum_{i=1}^{n} a_i g_i = \sum_{i=1}^{n} (x \otimes a_i g_i) = 0$. Therefore $\mathrm{Ker}(\varphi) = 0$, and so, φ is injective.

Finally, to see that φ is a bijection, it suffices to show that $\dim_K(L \otimes_K K[G]) = \dim_K(\mathrm{End}_K L)$. Indeed, since $G = \mathrm{Gal}(L|K)$, we have $|G| = [L : K] = \dim_K L$.

On the one hand, $\dim_K(\mathrm{End}_K L) = (\dim_K L)^2$. On the other hand,

$$\dim_K(L \otimes_K K[G]) = \dim_K L \, \dim_K K[G] = \dim_K L \, |G| = \dim_K L \, \dim_K L.$$

All in all, $\dim_K(L \otimes_K K[G]) = \dim_K(\mathrm{End}_K L)$, and so, φ is a bijection.

Conversely, suppose that φ is bijective. We need to show that $G = \mathrm{Gal}(L|K)$. Since φ is a bijection,

$$\dim_K(L \otimes_K K[G]) = \dim_K(\mathrm{End}_K L) \Rightarrow \dim_K L \, |G| = (\dim_K L)^2 \Rightarrow$$
$$\Rightarrow |G| = \dim_K L = [L : K] \Rightarrow |G| = [L : K].$$

By the primitive element theorem, there exists $\alpha \in L$ such that $L = K(\alpha)$, with $P(x) = \mathrm{irr}(\alpha, K)$ of degree $[L : K]$. We see that $L|K$ is Galois, that is, it is normal and separable. Since $\mathrm{char}(K) = 0$, $L|K$ is separable. Since $L = K(\alpha)$ and $G \leq \mathrm{Aut}_K L$, the elements of G are determined by the image of α. Moreover, since $|G| = [L : K] = \deg(P(x))$, every root of $P(x)$ is the image of α by some automorphism of G. Thus, each element of G moves α to some distinct root of $P(x)$, and so L is the splitting field of $P(x)$ over K. Hence, $L|K$ is normal, and therefore, it is Galois, that is, $\mathrm{Aut}_K L = \mathrm{Gal}(L|K)$.

By hypothesis, $G \leq \mathrm{Aut}_K L = \mathrm{Gal}(L|K)$, and since $|\mathrm{Gal}(L|K)| = [L : K] = |G|$, we conclude that $G = \mathrm{Gal}(L|K)$. □

The previous theorem motivates the notion of a Hopf Galois extension. We just need to replace $K[G]$ with a K-Hopf algebra.

Definition 4.2.4. A **Hopf Galois extension** with K-Hopf algebra H is a finite field extension $L|K$ with a K-Hopf algebra H such that L is a left H-module algebra and $\varphi : L \otimes_K H \to \mathrm{End}_K L$, defined as $\varphi(x \otimes h)(y) = x(h \cdot y)$, is a K-vector space isomorphism. The action of H on L is called **Hopf action**, and the pair of the Hopf algebra H with the Hopf action is called **Hopf Galois structure on** $L|K$.

Remark 4.2.5. If $L|K$ is a Hopf Galois extension of degree n, then the K-Hopf algebra H has dimension n: indeed, since φ is an isomorphism,

$$\dim_K(L \otimes_K H) = \dim_K(\mathrm{End}_K L) \Rightarrow n \, \dim_K H = n^2 \Rightarrow \dim_K H = n.$$

Remark 4.2.6. Whereas a Galois extension determines the Galois group (it is unique), a field extension may be Hopf Galois with different Hopf Galois structures.

The **fundamental theorem of Hopf Galois theory** in its general form says:

Theorem 4.2.7 ([G-P], Th 5.1, page 256)**.** *Let $L|K$ be a Hopf Galois extension with K-Hopf algebra H and let W be a sub-Hopf algebra of H. We define*

$$Fix(W) := \{x \in L : w \cdot x = \varepsilon(w)x, \text{ for all } w \in W\}.$$

Then the map $Fix : \{W \subseteq H \text{ sub-Hopf algebra}\} \to \{E \text{ field } : K \subseteq E \subseteq L\}$ is injective and inclusion-reversing.

Observe the fundamental theorem of Galois theory is stronger than this one since it gives a bijective correspondence, whereas the Hopf Galois theorem just gives an injection. In the next chapter, we will give a bijective correspondence for a particular type of Hopf Galois extensions.

Finally, we close this chapter with an example of a Hopf Galois extension which is not Galois.

Example 4.2.8. The extension $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$.

Let $\alpha := \sqrt[3]{2}$. We consider the extension $\mathbb{Q}(\alpha)|\mathbb{Q}$, which is finite of degree 3, since $\text{irr}(\alpha, \mathbb{Q})(x) = x^3 - 2$. Its basis is $\{1, \alpha, \alpha^2\}$. We see that it is Hopf Galois.

We consider the $\mathbb{Q}$-Hopf algebra $H = \mathbb{Q}[c, s]/(3s^2+c^2-1, (2c+1)s, (2c+1)(c-1))$. Its $\mathbb{Q}$-basis is $\{1, c, s\}$, so it has dimension 3. Since H is a quotient of the polynomial algebra, it is an algebra with usual quotient operations. Moreover, we can define comultiplication, counit and coinverse maps so that H is a Hopf algebra:

$$\begin{array}{lll} \Delta(1) = 1 \otimes 1, & \Delta(c) = c \otimes c - 3s \otimes s, & \Delta(s) = c \otimes s + s \otimes c, \\ \varepsilon(1) = 1, & \varepsilon(c) = 1, & \varepsilon(s) = 0, \\ \sigma(1) = 1, & \sigma(c) = c, & \sigma(s) = -s, \end{array}$$

$\mathbb{Q}(\alpha)$ is a left H-module algebra: indeed, it is clearly an algebra, it is a left H-module with action defined as follows

$$\begin{array}{lll} c \cdot 1 = 1, & c \cdot \alpha = -\frac{1}{2}\alpha, & c \cdot \alpha^2 = -\frac{1}{2}\alpha^2, \\ s \cdot 1 = 0, & s \cdot \alpha = \frac{1}{2}\alpha, & s \cdot \alpha^2 = -\frac{1}{2}\alpha^2, \end{array}$$

and the two conditions of the definition are satisfied: for $x, y \in \mathbb{Q}(\alpha)$,

$$\begin{array}{ll} c \cdot (xy) = (c \cdot x)(c \cdot y) - 3(s \cdot x)(s \cdot y), & c \cdot 1_{\mathbb{Q}(\alpha)} = c \cdot 1 = 1 = \varepsilon(c)1, \\ s \cdot (xy) = (c \cdot x)(s \cdot y) + (s \cdot x)(c \cdot y), & s \cdot 1_{\mathbb{Q}(\alpha)} = s \cdot 1 = 0 = \varepsilon(s)1. \end{array}$$

Finally, $\varphi : \mathbb{Q}(\alpha) \otimes_{\mathbb{Q}} H \to \text{End}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$, which is given by $\varphi(x \otimes h)(y) = x(h \cdot y)$, is a $\mathbb{Q}$-vector space isomorphism.

Note that $Fix(H) = \mathbb{Q}$: indeed, if $x \in \mathbb{Q}(\alpha)$, then

$$x \in \mathbb{Q} \;\Leftrightarrow\; c \cdot x = x = \varepsilon(c)x \;\text{ and }\; s \cdot x = 0 = \varepsilon(s)x.$$

5 Separable Hopf Galois extensions

In this chapter, we introduce first cohomology sets and define a vector space to be a form of another when they become isomorphic under scalar extension. We show that forms are classified by a first cohomology set and we apply this theory to Hopf algebras in order to classify their forms. Next, we characterize the Hopf Galois character of a separable field extension in terms of groups. Since proofs are beyond the scope of this dissertation, we do not include them. Finally, we explain how the Magma program works, summarize the main results and discuss an example.

5.1 Classification of forms

In this section, we consider two groups A and G such that A is a G-module and introduce 1-cocycles, maps of G into A satisfying a certain condition, which leads us to define the first cohomology group, if A is abelian, and more generally, the first cohomology set. Afterwards, we define a tensor x of type (p, q) over a vector space V and use it to set when (V, x) is a form of another one. Then, we classify forms. Finally, we apply this theory to Hopf algebras in order to classify their forms.

Let A, G be groups such that A is a left G-module with action denoted by "$\cdot$".

Definition 5.1.1. A 1-**cocycle of** G **into** A is a map $f : G \to A$ satisfying the identity $f(gg') = g \cdot f(g') + f(g)$. It is also called a **crossed homomorphism**. Let $C^1(G, A)$ denote the collection of 1-cocycles of G into A.

Firstly, we consider the case in which A is abelian. In this case, it is easy to check that $C^1(G, A)$ is an abelian group. Moreover, if the action is trivial, the condition of being cocycle means that f is a group homomorphism.

Definition 5.1.2. Let f be a 1-cocycle of G into A. It is a 1-**coboundary of** G **into** A if there exists $a \in A$ such that $f(g) = g \cdot a - a$, for all $g \in G$. Let $B^1(G, A)$ denote the collection of 1-coboundaries of G into A, which is a normal subgroup of $C^1(G, A)$ (since $C^1(G, A)$ is abelian).

Definition 5.1.3. The group $H^1(G, A)$ is defined as the quotient of $C^1(G, A)$ by $B^1(G, A)$. It is called the **first cohomology group of** G **with values in** A. Note that if G acts trivially on A, one has $H^1(G, A) = \mathrm{Hom}(G, A)$.

In other words, $B^1(G, A)$ defines the following equivalence relation on $C^1(G, A)$:

$$f_1 \sim f_2 \Leftrightarrow f_2 - f_1 \in B^1(G, A) \Leftrightarrow f_2(g) = g \cdot a - a + f_1(g), \text{ for some } a \in A.$$

Now, we consider the case in which A is not abelian. Write A multiplicatively. In this case, it has no interest to define $B^1(G, A)$, but we can also define $H^1(G, A)$.

Definition 5.1.4. The set $H^1(G, A)$ is defined as the quotient of $C^1(G, A)$ by the equivalence relation $\sim$ defined as

$$f_1 \sim f_2 \Leftrightarrow \text{there exists } a \in A \text{ such that } f_2(g) = a^{-1} f_1(g)(g \cdot a).$$

It is called the **first cohomology set of** G **with values in** A.

We define a specific type of tensors.

Definition 5.1.5. Let V be a vector space over K and let p, q be natural numbers. A **tensor of type** (p, q) **over** V is an element of $\bigotimes^p V \otimes \bigotimes^q V^*$.

Let V be a K-vector space provided with a fixed tensor x of type (p, q) over V.

Definition 5.1.6. Let V' be a K-vector space provided with a fixed tensor x' of type (p, q) over V'. The pairs (V, x) and (V', x') are K-**isomorphic** if there exists a K-linear isomorphism $f : V \to V'$ such that $\left(\bigotimes^p f \otimes \bigotimes^q (f^{-1})^*\right)(x) = x'$.

Let $L|K$ be a finite Galois extension with group G. Let $V_L = L \otimes_K V$ be the L-vector space obtained by extending scalars. Observe the tensor x defines a tensor $x_L = 1_L \otimes_K x$ of type (p, q) over V_L in the following way: since $x \in \bigotimes_K^p V \otimes_K \bigotimes_K^q V^*$, $x_L \in L \otimes_K \bigotimes_K^p V \otimes_K \bigotimes_K^q V^* \cong \bigotimes_L^p V_L \otimes_L \bigotimes_L^q V_L^*$.

Definition 5.1.7. Let V' be a K-vector space provided with a fixed tensor x' of type (p, q) over V'. The pair (V', x') is an $L|K$-**form of** (V, x) (or just a **form**) if (V_L, x_L) and (V'_L, x'_L) are L-isomorphic.

Let $E_{V,x}(L|K)$ denote the collection of K-isomorphism classes of pairs (V', x') which are forms of (V, x). Our goal is to interpret $E_{V,x}(L|K)$ as a first cohomology set. In order to do it, we define $A_L = \mathrm{Aut}_L(V_L, x_L)$ (it is not necessarily abelian), and we will define a bijection between $E_{V,x}(L|K)$ and $H^1(G, A_L)$.

We start seeing that the group G acts on A_L. First of all, it acts on V_L as follows: for a fixed $g \in G$,

$$\begin{array}{rccc} g \otimes I_V : & L \otimes_K V & \to & L \otimes_K V \\ & r \otimes_K v & \mapsto & g(r) \otimes_K v \end{array}$$

Next, given $f \in A_L$, we define $g \cdot f := (g \otimes I_V) \circ f \circ (g^{-1} \otimes I_V)$, which is an L-automorphism of V_L. Thus, G acts on A_L.

Now, we compare $E_{V,x}(L|K)$ with $H^1(G, A_L)$. Let $(V', x') \in E_{V,x}(L|K)$ and let $f : V_L \to V'_L$ be an L-isomorphism. We can generalize the previous action

$$g \cdot f := (g \otimes I_{V'}) \circ f \circ (g^{-1} \otimes I_V).$$

We define the following element of A_L: $\rho_g := f^{-1} \circ g \cdot f$. Furthermore, it is easy to show that the following map is a 1-cocycle

$$\begin{array}{rccc} \rho : & G = \mathrm{Gal}(L|K) & \to & A_L = \mathrm{Aut}_L(V_L) \\ & g & \mapsto & \rho_g = f^{-1} \circ g \cdot f \end{array}$$

and that changing f has the effect of replacing ρ with an equivalent 1-cocycle.

Hence, $[\rho] \in H^1(G, A_L)$ is well-determined, and we have defined a map

$$\begin{array}{rccc} \theta: & E_{V,x}(L|K) & \to & H^1(G, A_L) \\ & (V', x') & \mapsto & [\rho] \end{array}$$

Theorem 5.1.8. *The map θ just defined is a bijection, that is, $L|K$-forms of (V, x) can be identified with 1-cocycles of Gal$(L|K)$ into Aut$_L(L \otimes_K V, 1_L \otimes_K x)$.*

We can repeat this argument for a K-vector space V provided with a finite number of tensors over V. In order to apply this result to Hopf algebras, we need to make the following remark:

Remark 5.1.9. Let V be a finite dimensional vector space over K and let n, m be naturals. There is a K-linear isomorphism

$$\mathrm{Hom}_K(\bigotimes^n V, \bigotimes^m V) \cong \bigotimes^n V^* \otimes \bigotimes^m V$$

given by $\omega_1 \otimes \cdots \otimes \omega_n \otimes v_1 \otimes \cdots \otimes v_m \mapsto \varphi$, where $\varphi \in \mathrm{Hom}_K(\bigotimes^n V, \bigotimes^m V)$ is defined as $\varphi(e_1 \otimes \cdots \otimes e_n) = \omega_1(e_1) \ldots \omega_n(e_n)(v_1 \otimes \cdots \otimes v_m)$.

Let $(H, m_H, \lambda_H, \Delta_H, \varepsilon_H, \sigma_H)$ be a K-Hopf algebra. Observe we can see multiplication, unit, comultiplication, counit and coinverse maps as tensors: indeed,

1. Multiplication: $m_H \in \mathrm{Hom}_K(H \otimes H, H) \cong H^* \otimes H^* \otimes H$, so it is a tensor of type (1,2) over H.
2. Unit: $\lambda_H \in \mathrm{Hom}_K(H^0 := K, H) \cong H$, so it is a tensor of type (1,0) over H.
3. Comultiplication: $\Delta_H \in \mathrm{Hom}_K(H, H \otimes H) \cong H^* \otimes H \otimes H$, so it is a tensor of type (2,1) over H.
4. Counit: $\varepsilon_H \in \mathrm{Hom}_K(H, H^0) \cong H^*$, so it is a tensor of type (0,1) over H.
5. Coinverse: $\sigma_H \in \mathrm{Hom}_K(H, H) \cong H^* \otimes H$, so it is a tensor of type (1,1) over H.

Let $L|K$ be a finite Galois extension with group G. We consider $H_L = L \otimes_K H$, which is the L-Hopf algebra obtained by extending escalars (Proposition 4.1.21). Set $t := \{m_H, \lambda_H, \Delta_H, \varepsilon_H, \sigma_H\}$. Observe that (H, t) isomorphisms are Hopf algebra isomorphisms. Let $E_{H,t}(L|K)$ denote the collection of K-isomorphism classes of pairs (H', t') which are forms of (H, t), and let $A_L = \mathrm{Aut}_L(H_L, t_L)$. Repeating the previous construction, we define the map

$$\begin{array}{rccc} \theta: & E_{H,t}(L|K) & \to & H^1(G, A_L) \\ & (H', t') & \mapsto & [\rho] \end{array}$$

Theorem 5.1.10. *The map θ is a bijection, that is, $L|K$-forms of Hopf algebras (H, t) can be identified with 1-cocycles of Gal$(L|K)$ into Aut$_L(L \otimes_K H, 1_L \otimes_K t)$.*

5.2 Hopf Galois character in terms of groups

In this section, we start reviewing and defining some important notions about groups. Then, we characterize the Hopf Galois character of a separable field extension in terms of groups. Finally, we define a special type of Hopf Galois extensions called almost classical Galois extensions, for which the Galois correspondence is bijective.

Definition 5.2.1. Let G be a group. A subgroup $H \subseteq G$ is **normal in** G, $H \trianglelefteq G$, if for every $g \in G$ and for every $h \in H$, it is satisfied $ghg^{-1} \in H$, that is, $gHg^{-1} \subseteq H$.

Proposition 5.2.2. *$H \subseteq G$ is normal if, and only if, $gH = Hg$, for every $g \in G$. In other words, $H \subseteq G$ is normal if, and only if, left and right cosets coincide.*

Definition 5.2.3. Let G be a group and let $N \subseteq G$ be a subgroup. We define the **normalizer of** N **in** G as $\mathrm{Norm}_G N = \{g \in G : gng^{-1} \in N, \text{ for all } n \in N\}$.

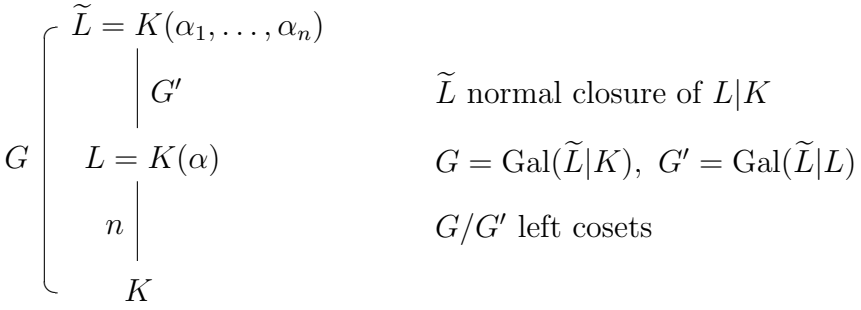
Let $H \subseteq G$ be a subgroup. N is **normalized by** H if for every $h \in H$ and for every $n \in N$, it is satisfied $hnh^{-1} \in N$. Equivalently, N is normalized by H if, and only if, $H \subseteq \mathrm{Norm}_G N$.

Definition 5.2.4. Let G be a group and let $G' \subseteq G$ be a subgroup. A subgroup $N \subseteq G$ is a **normal complement of** G' **in** G if $N \trianglelefteq G$, $|N| = [G : G']$ and $NG' = G$.

Definition 5.2.5. A subgroup N of S_n is **transitive** if the action of N on $\{1, \ldots, n\}$ is transitive, that is, for every $i, j \in \{1, \ldots, n\}$, there exists $m \in N$ such that $m(i) = j$. N is also called **transitive group of degree** n. Moreover, N is **regular** if it is transitive and this m is unique for every $i, j \in \{1, \ldots, n\}$.

Proposition 5.2.6. *$N \subseteq S_n$ is regular if, and only if, N is transitive and $|N| = n$.*

Let $L|K$ be a finite separable field extension of degree n and let $\widetilde{L}$ be its normal closure. Let $G = \mathrm{Gal}(\widetilde{L}|K) = \mathrm{Aut}_K \widetilde{L}$ and $G' = \mathrm{Gal}(\widetilde{L}|L)$. By the primitive element theorem, there exists $\alpha \in L$ such that $L = K(\alpha)$. Let $f = \mathrm{irr}(\alpha, K)$, which has degree n, and we denote $\{\alpha_1 := \alpha, \ldots, \alpha_n\}$ its roots, so that $\widetilde{L} = K(\alpha_1, \ldots, \alpha_n)$.



Observe $[G : G'] = n$. Let $S = G/G' = \{gG' : g \in G\}$ be the left cosets, and we consider $\mathrm{Perm}(S) \cong S_n$. Clearly, G acts on G/G', so there is a group homomorphism

$$\begin{array}{rccl} \lambda : & G & \to & S_n \cong \mathrm{Perm}(G/G') \\ & g & \mapsto & [hG' \mapsto ghG'] \end{array}$$

Next, we show that the action of G on G/G' is equivalent to the Galois action of G on $\{\alpha_1, \ldots, \alpha_n\}$. Indeed, for $g_1, g_2 \in G$, we have

$$g_1(\alpha) = g_2(\alpha) \Leftrightarrow (g_2^{-1}g_1)(\alpha) = \alpha \Leftrightarrow g_2^{-1}g_1 \in G' = \mathrm{Aut}_{K(\alpha)}\widetilde{L} \Leftrightarrow g_1 \in g_2G'.$$

Thus, there is an injective map of $\{\text{conjugates of } \alpha\} = \{\text{roots of } \mathrm{irr}(\alpha, K)\}$ into $\{\text{left cosets } G/G'\}$, given by $g(\alpha) \mapsto gG'$. Since the cardinal of these two sets is the same, we conclude that it is a bijection.

Since the Galois action of G on $\{\alpha_1, \ldots, \alpha_n\}$ is transitive and faithful, G is embedded into S_n as a transitive group. Therefore, from now on, we will identify G with its image by λ. Note that changing $\lambda(G)$ by a conjugated subgroup in S_n is equivalent to renumerate the roots $\{\alpha_1, \ldots, \alpha_n\}$.

Now, we characterize the Hopf Galois character of a separable field extension in terms of groups.

Theorem 5.2.7. *Let $L|K$ be a finite separable field extension of degree n and let $\widetilde{L}$ be its normal closure. Let $G = Gal(\widetilde{L}|K)$. The following conditions are equivalent:*

1. *There exists a K-Hopf algebra H such that $L|K$ is Hopf Galois with Hopf algebra H,*
2. *There exists a regular subgroup N of S_n normalized by G.*

More precisely, there is a bijection

$$\{(H, \cdot) \text{ } H\text{-}G \text{ structure on } L|K\} \leftrightarrow \{N \text{ regular subgroup of } S_n \text{ normalized by } G\}.$$

Moreover, the K-Hopf algebra H is an $\widetilde{L}|K$-form of $K[N]$. In other words,

$$\widetilde{L} \otimes_K H \cong \widetilde{L} \otimes_K K[N] \cong \widetilde{L}[N].$$

In particular, H is cocommutative, so that by Corollary 4.1.10, its coinverse map has ordre 2.

Definition 5.2.8. We refer to the isomorphism class of N as the **type of the Hopf Galois structure**.

We are going to explain how we can construct a Hopf Galois structure given N. Let $\{x_i : i \in \{1, \ldots, [\widetilde{L} : K]\}\}$ be a K-basis of $\widetilde{L}$ as a K-vector space. So, we write

$$\widetilde{L}[N] = \left\{ \sum_{m \in N} \lambda_m m : \lambda_m \in \widetilde{L} \right\}, \text{ where } \lambda_m = \sum_{i=1}^{[\widetilde{L}:K]} \mu_{i,m} x_i, \text{ for } \mu_{i,m} \in K.$$

Note that $\widetilde{L}[N]$ is a K-algebra (since it is an $\widetilde{L}$-Hopf algebra) of dimension $n[\widetilde{L} : K]$:

$$\dim_K(\widetilde{L}[N]) = \dim_K(\widetilde{L} \otimes_K H) = \dim_K \widetilde{L} \dim_K H = [\widetilde{L} : K][L : K] = [\widetilde{L} : K]n.$$

We can define a sub-K-algebra of $\widetilde{L}[N]$ as follows. Observe G acts on $\widetilde{L}[N]$ (both on coefficients λ_m and on elements m) as

$$g\Big(\sum_{m\in N}\lambda_m m\Big)=\sum_{m\in N} g(\lambda_m)gmg^{-1},$$

where $g(\lambda_m)$ is the Galois action and $gmg^{-1}\in N$ (since N is normalized by G). So we define H as the subalgebra of $\widetilde{L}[N]$ of fixed elements by the previous action

$$H:=\{x\in\widetilde{L}[N]: g(x)=x,\ \text{for all } g\in G\}.$$

Note that, for all $g\in G$, $x\in H$, we have

$$g(x)=g\Big(\sum_{m\in N}\lambda_m m\Big)=\sum_{m\in N} g(\lambda_m)gmg^{-1}=\sum_{m\in N} g(\lambda_{g^{-1}mg})m=\sum_{m\in N}\lambda_m m=x,$$

so we have obtained the relation satisfied by the coefficients of elements in H

$$\lambda_m=g(\lambda_{g^{-1}mg}),\ \text{for all } g\in G.$$

Finally, we enumerate left cosets of S from 1 until n: $\mathrm{id}G'=G', g_2G', \dots, g_nG'$. Observe that elements in S_n can be seen as permutations of left cosets. In particular, elements in N can also be seen as permutations of left cosets, so that given $m\in N$, $m^{-1}(1)$ corresponds to a certain g_iG', for $i\in\{1,\dots,n\}$. Therefore, we define the following K-linear map on basic elements and extend it by linearity

$$\begin{array}{rccl}\psi: & \widetilde{L}[N] & \to & \mathrm{End}_K\widetilde{L}\\ & m\in N & \mapsto & g_i \text{ such that } m^{-1}(1)=g_iG'=[g_i]\\ & r\in\widetilde{L} & \mapsto & [f\mapsto rf]\end{array}$$

Since $\psi(h)(x)\in L$, for all $h\in H$, $x\in L$, ψ induces by restriction the Hopf action $\psi_H: H\to \mathrm{End}_K L$. Finally, $\varphi: L\otimes_K H\to \mathrm{End}_K L$ is a K-vector space isomorphism.

The previous theorem does not tell us whether the subgroup N is contained in $G\subseteq S_n$ or not. The case $N\subseteq G$ leads to an interesting type of Hopf Galois extension.

Proposition 5.2.9. *Let $L|K$ be a finite separable field extension of degree n and let $\widetilde{L}$ be its normal closure. Let $G=Gal(\widetilde{L}|K)$ and $G'=Gal(\widetilde{L}|L)$. The following conditions are equivalent:*

1. *There exists a normal complement N of G' in G,*
2. *There exists a regular subgroup N of S_n normalized by G and contained in G.*

Definition 5.2.10. If $L|K$ is an extension satisfying the equivalent conditions of the previous proposition, then $L|K$ is an **almost classical Galois extension**.

Theorem 5.2.11. *If $L|K$ is an almost classical Galois extension, for the Hopf Galois structure of $L|K$ corresponding to the normal complement N of G' in G, the Galois correspondence is bijective.*

5.3 Examples of separable extensions of degree 8

In this section, we explain how the Magma program works and sum up the main results obtained performing it for separable extensions of degree 8 (see Appendix for the code and more results). Finally, we discuss a concrete example of an extension of degree 8 of $\mathbb{Q}$ and, using Theorem 5.2.7, we make the construction of the Hopf Galois structure corresponding to a regular subgroup of S_8 given by the Magma program.

We explain how the program works. Let $L|K$ be a finite separable field extension of degree 8 and let L' be its normal closure. Let $G = \mathrm{Gal}(L'|K)$ and $G' = \mathrm{Gal}(L'|L)$. Recall that G acts transitively and faithfully on G/G', and so there is a group homomorphism $G \hookrightarrow S_8 \cong \mathrm{Perm}(G/G')$. Therefore, considering all possible Galois groups of $L'|K$ is equivalent to consider all transitive groups of degree 8. We start counting transitive groups of order i and degree 8. Those of order 8 correspond to $L|K$ Galois and are the regular subgroups of S_8 (by Proposition 5.2.6). Then we construct a function that finds a normal complement of a subgroup H of a group G (if there exists any) and go on with the main program.

By Theorem 5.2.7, we determine all Hopf Galois structures looking for all regular subgroups of S_8 normalized by G. Moreover, by Proposition 5.2.9, we distinguish almost classical Galois extensions looking for a normal complement of G' in G. We set $G' = \mathrm{St}(1) = \mathrm{St}([\mathrm{id}])$ because, since we have seen that the action of G on G/G' is equivalent to the Galois action of G on $\{\alpha_1, \ldots, \alpha_n\}$, then

$$\mathrm{St}([\mathrm{id}]) \underset{([\mathrm{id}]=G' \leftrightarrow \alpha_1=\alpha)}{=} \mathrm{St}(\alpha) = \{g \in G = \mathrm{Aut}_K L' : g(\alpha) = \alpha\} = \mathrm{Aut}_{K(\alpha)} L' = G'.$$

The output of the program is the whole list of regular subgroups for every G.

In the following table we show the number of Hopf Galois structures of each type for a Galois extension $L|K$.

Table 1: Galois extensions

	Hopf Galois structures				
Galois group	C_8	$C_4 \times C_2$	$C_2 \times C_2 \times C_2$	$D_{2\cdot 4}$	Q_8
C_8	2	0	0	2	2
$C_4 \times C_2$	4	10	4	6	2
$C_2 \times C_2 \times C_2$	0	42	8	42	14
$D_{2\cdot 4}$	2	14	6	6	2
Q_8	6	6	2	6	2

Example 5.3.1. The extension $\mathbb{Q}(\sqrt[8]{2})|\mathbb{Q}$.

$$G\left\{\begin{array}{ll} \widetilde{L}=\mathbb{Q}(\alpha,i) & \alpha:=\sqrt[8]{2} \text{ satisfies } \alpha^8=2 \\ \quad 2 \,\Big|\, G' & L|\mathbb{Q} \text{ separable} \\ L=\mathbb{Q}(\alpha) & \widetilde{L} \text{ normal closure of } L|\mathbb{Q} \\ \quad 8 \,\Big|\, x^8-2 & [\widetilde{L}:\mathbb{Q}]=16 \\ K=\mathbb{Q} & G=\mathrm{Gal}(\widetilde{L}|\mathbb{Q}),\ G'=\mathrm{Gal}(\widetilde{L}|L) \end{array}\right.$$

The $\mathbb{Q}$-basis of $\widetilde{L}$ is $\{1,\alpha,\dots,\alpha^7,i,i\alpha,\dots,i\alpha^7\}$. Let $f:=\mathrm{irr}(\alpha,\mathbb{Q})(x)=x^8-2$, so that it roots are $\{\alpha\ \xi^k\}_{k=0}^7$, where $\xi^k:=\xi_8^k=\left(\frac{1+i}{\sqrt{2}}\right)^k=\left(\frac{1+i}{\alpha^4}\right)^k$ are the eighth roots of unity.

Firstly, we determine G. If $g\in G=\mathrm{Gal}(\mathbb{Q}(\alpha,i)|\mathbb{Q})$, g is determined by a generator system of the extension, for instance, $\{\alpha,i\}$. Thus

$$\begin{array}{l} g(\alpha)\in \mathrm{Roots}(\mathrm{irr}(\alpha,\mathbb{Q}))=\mathrm{Roots}(x^8-2)=\{\alpha\ \xi^k\}_{k=0}^7 \\ g(i)\in \mathrm{Roots}(\mathrm{irr}(i,\mathbb{Q}))=\mathrm{Roots}(x^2+1)=\{i,-i\} \end{array}$$

Since there are only $8\cdot 2=16$ possible ways of defining automorphisms and $|G|=|\mathrm{Gal}(\widetilde{L}|K)|=16$, each of these 16 assignations actually define an automorphism. We write

$$\sigma:\ \begin{array}{ccc} \alpha & \mapsto & \xi\alpha \\ i & \mapsto & i \end{array} \qquad\qquad \tau:\ \begin{array}{ccc} \alpha & \mapsto & \alpha \\ i & \mapsto & -i \end{array}$$

Note that $\sigma(\xi)=-\xi=\xi^5$ and $\tau(\xi)=\xi^7$: indeed,

$$\sigma(\xi)=\sigma\left(\tfrac{1+i}{\alpha^4}\right)=\tfrac{1+i}{\xi^4\alpha^4}\underset{(\xi^4=-1)}{=}-\tfrac{1+i}{\alpha^4}=-\xi$$
$$\tau(\xi)=\tau\left(\tfrac{1+i}{\alpha^4}\right)=\tfrac{1-i}{\alpha^4}=\xi^7$$

Observe also that τ has clearly degree 2 and σ has degree 8: indeed,

$$\alpha \underset{1}{\overset{\sigma}{\longmapsto}} \xi\alpha \underset{2}{\overset{\sigma}{\longmapsto}} \xi^6\alpha \underset{3}{\overset{\sigma}{\longmapsto}} \xi^7\alpha \underset{4}{\overset{\sigma}{\longmapsto}} -\alpha \underset{5}{\overset{\sigma}{\longmapsto}} \xi^5\alpha \underset{6}{\overset{\sigma}{\longmapsto}} \xi^2\alpha \underset{7}{\overset{\sigma}{\longmapsto}} \xi^3\alpha \underset{8}{\overset{\sigma}{\longmapsto}} \alpha$$

Moreover, note that $\tau\sigma\tau=\sigma^3$: indeed,

$$\tau\sigma(\tau(\alpha))=\tau(\sigma(\alpha))=\tau(\xi\alpha)=\xi^7\alpha=\sigma^3(\alpha),$$
$$\tau\sigma(\tau(i))=\tau(\sigma(-i))=\tau(-i)=i=\sigma^3(i),$$

Therefore, we conclude $G=\langle\sigma,\tau:\sigma^8=\mathrm{id},\tau^2=\mathrm{id},\tau\sigma\tau=\sigma^3\rangle$. Recall that one has $\lambda:G\hookrightarrow S_8$. We have observed that the transitive subgroup of S_8 verifying these relations is $8\mathrm{T}8=\langle(1,2,3,4,5,6,7,8),(1,3)(2,6)(5,7)\rangle$.

Now, we order the roots in order to identify correctly G as a Galois group with 8T8. We set

$$\alpha_1=\alpha,\ \alpha_2=\xi\alpha,\ \alpha_3=\xi^6\alpha,\ \alpha_4=\xi^7\alpha,\ \alpha_5=-\alpha,\ \alpha_6=\xi^5\alpha,\ \alpha_7=\xi^2\alpha,\ \alpha_8=\xi^3\alpha.$$

One has that σ gives $(1,2,3,4,5,6,7,8)$ and τ gives $(2,4)(3,7)(6,8)$. We can check with Magma that they are well-identified as follows:

```
H1:=TransitiveGroup(8,8);
H2:=sub<Sym(8)|(1,2,3,4,5,6,7,8),(2,4)(3,7)(6,8)>;
IsConjugate(Sym(8),H1,H2);//we already know that they are conjugates
true Id
```

Secondly, we consider a regular subgroup of S_8 normalized by G

$$N=\langle(1,2,3,4,5,6,7,8)\rangle=\langle\rho\rangle=\{\mathrm{id},\rho,\dots,\rho^7\}\cong C_8$$

and we determine the corresponding Hopf algebra

$$H=\left\{x=\sum_{k=0}^{7}\lambda_{\rho^k}\rho^k\in\widetilde{L}[N]:g(x)=x,\ \text{for all } g\in G\right\}.$$

In order to do it, recall that $\lambda_{\rho^k}=g(\lambda_{g^{-1}\rho^k g})$ holds for every $g\in G=\langle\sigma,\tau\rangle$, that is, for $g=\sigma$ and $g=\tau$. We calculate λ_{ρ^k} for every $k\in\{0,\dots,7\}$: since $\sigma=\rho$, observe

- $\lambda_{\mathrm{id}}=g(\lambda_{\mathrm{id}})$, for $g=\sigma$ and $g=\tau$, so that $\lambda_{\mathrm{id}}\in\mathbb{Q}$,
- $\lambda_{\rho^k}=\sigma(\lambda_{\sigma^{-1}\rho^k\sigma})=\sigma(\lambda_{\rho^{-1}\rho^k\rho})=\sigma(\lambda_{\rho^k})\Rightarrow\lambda_{\rho^k}=\sigma(\lambda_{\rho^k})$, so that $\lambda_{\rho^k}\in\widetilde{L}^{\langle\sigma\rangle}=\{x\in\widetilde{L}:\sigma(x)=x\}=\mathbb{Q}(i)=\{r+si:r,s\in\mathbb{Q}\}$,
- $\lambda_{\rho^k}=\tau(\lambda_{\tau^{-1}\rho^k\tau})=\tau(\lambda_{\tau^{-1}\sigma^k\tau})=\tau(\lambda_{(\tau^{-1}\sigma\tau)\dots(\tau^{-1}\sigma\tau)})\underset{(\tau\sigma\tau=\sigma^3)}{=}\tau(\lambda_{\sigma^{3k}})=\tau(\lambda_{\rho^{3k}})$, so that $\lambda_{\rho^k}=\tau(\lambda_{\rho^{3k}})\underset{(\tau^2=\mathrm{id})}{\Leftrightarrow}\lambda_{\rho^{3k}}=\tau(\lambda_{\rho^k})$.

Using these results, we obtain

- Since $\lambda_{\mathrm{id}}\in\mathbb{Q}$, we set $\lambda:=\lambda_{\mathrm{id}}$,
- $\rho\mapsto\rho^3\mapsto\rho^9=\rho$, so that $\lambda_\rho=a+bi$ and $\lambda_{\rho^3}=\tau(a+bi)=a-bi$, where $a,b\in\mathbb{Q}$,
- $\rho^2\mapsto\rho^6\mapsto\rho^{18}=\rho^2$, so that $\lambda_{\rho^2}=c+di$ and $\lambda_{\rho^6}=\tau(c+di)=c-di$, where $c,d\in\mathbb{Q}$,
- $\rho^4\mapsto\rho^{12}=\rho^4\Rightarrow\lambda_{\rho^4}\in\widetilde{L}^{\langle\tau\rangle}\underset{(\lambda_{\rho^4}\in\widetilde{L}^{\langle\sigma\rangle})}{\Rightarrow}\lambda_{\rho^4}\in\widetilde{L}^{\langle\sigma,\tau\rangle}=\widetilde{L}^G=\mathbb{Q}$, so that $\mu:=\lambda_{\rho^4}$,
- $\rho^5\mapsto\rho^{15}=\rho^7\mapsto\rho^{21}=\rho^5$, so that $\lambda_{\rho^5}=e+fi$ and $\lambda_{\rho^7}=\tau(e+fi)=e-fi$, where $e,f\in\mathbb{Q}$.

Hence, $x \in H$ can be written as

$$\begin{aligned} x \;=\; \textstyle\sum_{k=0}^{7} \lambda_{\rho^k}\rho^k \;&=\; \lambda\mathrm{id} + (a+bi)\rho + (c+di)\rho^2 + (a-bi)\rho^3 + \mu\rho^4 + \\ &\quad (e+fi)\rho^5 + (c-di)\rho^6 + (e-fi)\rho^7 \\ &=\; \lambda\mathrm{id} + a(\rho+\rho^3) + b(\rho-\rho^3)i + c(\rho^2+\rho^6) + \\ &\quad d(\rho^2-\rho^6)i + \mu\rho^4 + e(\rho^5+\rho^7) + f(\rho^5-\rho^7)i, \end{aligned}$$

so that H is a $\mathbb{Q}$-Hopf algebra with $\mathbb{Q}$-basis

$$\{\mathrm{id},\ \rho+\rho^3,\ (\rho-\rho^3)i,\ \rho^2+\rho^6,\ (\rho^2-\rho^6)i,\ \rho^4,\ \rho^5+\rho^7,\ (\rho^5-\rho^7)i\}.$$

Finally, we determine the Hopf action $\psi|_H : H \to \mathrm{End}_{\mathbb{Q}}L$. In order to do it, we need to see how $\psi : \widetilde{L}[N] \to \mathrm{End}_{\mathbb{Q}}\widetilde{L}$ is defined. Recall that $\psi(\rho^k) = g_j \in G$ such that $(\rho^k)^{-1}(1) = g_jG'$. Since $G' = \mathrm{Aut}_{\mathbb{Q}(\alpha)}\widetilde{L}$ fixes α, then $G' = \langle\tau\rangle$, and so we can write and enumerate left cosets as follows $G/G' = \{\underset{1}{[\mathrm{id}]}, \underset{2}{[\sigma]}, \ldots, \underset{8}{[\sigma^7]}\}$.

Hence, we have the following K-linear map

$$\begin{array}{rrcl} \psi: & \widetilde{L}[N] & \to & \mathrm{End}_{\mathbb{Q}}\widetilde{L} \\ & \rho^k \in N & \mapsto & \sigma^{-k} \text{ since } ((\rho^k)^{-1})(1) = (\rho^{-k})(1) = [\sigma^{-k}] \\ & r \in \widetilde{L} & \mapsto & [f \mapsto rf] \end{array}$$

which induces by restriction the Hopf action

$$\begin{array}{rrcl} \psi|_H: & H & \to & \mathrm{End}_{\mathbb{Q}}L = \mathrm{End}_{\mathbb{Q}}\mathbb{Q}(\alpha) \\ & \mathrm{id} & \mapsto & \mathrm{id} \\ & \rho+\rho^3 & \mapsto & \sigma^{-1}+\sigma^{-3} = \sigma^7+\sigma^5 \\ & (\rho-\rho^3)i & \mapsto & (\sigma^{-1}-\sigma^{-3})i = (\sigma^7-\sigma^5)i \\ & \rho^2+\rho^6 & \mapsto & \sigma^{-2}+\sigma^{-6} = \sigma^6+\sigma^2 \\ & (\rho^2-\rho^6)i & \mapsto & (\sigma^{-2}-\sigma^{-6})i = (\sigma^6-\sigma^2)i \\ & \rho^4 & \mapsto & \sigma^{-4} = \sigma^4 \\ & \rho^5+\rho^7 & \mapsto & \sigma^{-5}+\sigma^{-7} = \sigma^3+\sigma \\ & (\rho^5-\rho^7)i & \mapsto & (\sigma^{-5}-\sigma^{-7})i = (\sigma^3-\sigma)i \end{array}$$

and doing simple calculations, one can see that $\psi|_H(H)$ is actually a subset of $\mathrm{End}_{\mathbb{Q}}L$:

$$\begin{aligned} &\mathrm{id}(\alpha) = \alpha, && (\sigma^7+\sigma^5)(\alpha) = -\alpha^5, \\ &((\sigma^7-\sigma^5)i)(\alpha) = -\alpha^5, && (\sigma^6+\sigma^2)(\alpha) = 0, \\ &((\sigma^6-\sigma^2)i)(\alpha) = -\alpha^9, && \sigma^4(\alpha) = -\alpha, \\ &(\sigma^3+\sigma)(\alpha) = \alpha^5, && ((\sigma^3-\sigma)i)(\alpha) = \alpha^5. \end{aligned}$$

6 Conclusions

This memory shows the constructive theory we have had to develop in order to reach, on the one hand, to Hopf Galois extensions and, on the other hand, to its characterization in terms of groups. In the first part, we prove all the results in detail whereas proofs of the last part are beyond the scope of this dissertation. However, we came to understand the constructive idea well enough to apply it to an example.

Since there is a characterization of the Galois character in terms of groups, we use Magma to obtain all Hopf Galois structures of separable field extensions of degree 8. Due to the degree of difficulty of this theory, we thought it would be more complex to design computer software, but finally we have found a short and elegant way to do it. In Appendix we show the whole code of the program.

An important part of the basic knowledge that we have needed to carry out this project has been achieved in Algebraic Structures and Algebraic Equations, which are obligatory subjects of the Mathematics Degree.

A Magma code and some results

```
//Let L|K be a separable field extension of degree g=[L|K]=8
//Let L' be its normal closure, G=Gal(L'|K), G'=Gal(L'|L)

g:=8;
S:=Sym(g); Order(S);
n:=NumberOfTransitiveGroups(g); n;

40320
50

//We calculate the number of transitive groups of Sg of order i
m:=1;
for i in [g..Order(S) by g] do
  count:=0;
  for j in [m..n] do
    if Order(TransitiveGroup(g,j)) eq i then
      m:=m+1;
      count:=count+1;
    elif count ne 0 then
      print "The number of transitive groups of order"; i;
      print "is"; count;
      print "-----";
      if i eq g then
        triv:=count; //triv means that L|K is Galois
      end if;
      delete(count);
      break;
    end if;
  end for; //j
end for; //i
print "The number of transitive groups of order";
Order(S); print "is 1";
delete(count);

The number of transitive groups of order 8 is 5
-----
The number of transitive groups of order 16 is 6
-----
The number of transitive groups of order 24 is 3
-----
The number of transitive groups of order 32 is 8
-----
The number of transitive groups of order 48 is 2
-----
```

```
The number of transitive groups of order 56 is 1
-----
The number of transitive groups of order 64 is 6
-----
The number of transitive groups of order 96 is 3
-----
The number of transitive groups of order 128 is 1
-----
The number of transitive groups of order 168 is 2
-----
The number of transitive groups of order 192 is 4
-----
The number of transitive groups of order 288 is 1
-----
The number of transitive groups of order 336 is 1
-----
The number of transitive groups of order 384 is 1
-----
The number of transitive groups of order 576 is 2
-----
The number of transitive groups of order 1152 is 1
-----
The number of transitive groups of order 1344 is 1
-----
The number of transitive groups of order 20160 is 1
-----
The number of transitive groups of order 40320 is 1


//We calculate subgroups G=Gal(L'|K) when L'=L
for i in [1..triv] do
TransitiveGroup(g,i);
print "----------";
end for;


Permutation group acting on a set of cardinality 8
Order = 8 = 2^3
    (1, 2, 3, 4, 5, 6, 7, 8)
C(8)=8
----------
Permutation group acting on a set of cardinality 8
Order = 8 = 2^3
    (1, 2, 3, 8)(4, 5, 6, 7)
    (1, 5)(2, 6)(3, 7)(4, 8)
4[x]2
```

```
----------
Permutation group acting on a set of cardinality 8
Order = 8 = 2^3
    (1, 8)(2, 3)(4, 5)(6, 7)
    (1, 3)(2, 8)(4, 6)(5, 7)
    (1, 5)(2, 6)(3, 7)(4, 8)
E(8)=2[x]2[x]2
----------
Permutation group acting on a set of cardinality 8
Order = 8 = 2^3
    (1, 2, 3, 8)(4, 5, 6, 7)
    (1, 6)(2, 5)(3, 4)(7, 8)
D_8(8)=[4]2
----------
Permutation group acting on a set of cardinality 8
Order = 8 = 2^3
    (1, 2, 3, 8)(4, 5, 6, 7)
    (1, 7, 3, 5)(2, 6, 8, 4)
Q_8(8)
----------


//FUNCTION that calculates a normal complement
//of a subgroup H of G (if there exists any)
normcomp:=function(G,H)
  NS:=NormalSubgroups(G);
  for i in [1..#NS] do
    N:=NS[i]`subgroup;
    if Index(G,H) eq Order(N) then
      //if N=<S> and H=<T>, then NH=<SUT>
      SUT:=[x: x in Generators(N) join Generators(H)];
      NH:=sub<G|SUT>;
      //In order to know if NH=G, it suffices to see
      //that both of them have the same order
      if Order(NH) eq Order(G) then
        return N;
      end if;
      delete(SUT); delete(NH);
    end if;
    delete(N);
  end for;
  //if there is no N, it returns the trivial group
  return sub<G|Id(G)>;
end function;
```

```
//MAIN PROGRAM
TG:=[TransitiveGroup(g,i) : i in [1..triv]]; //Reg. subg. of Sg
NTG:=[Normalizer(S,TG[i]) : i in [1..triv]];
T:=[Transversal(S,NTG[i]) : i in [1..triv]];
Trans:=[[x : x in T[i]]   : i in [1..triv]];
//Transversal calculates right cosets; since we want the left ones,
//we calculate TGij doing (Trans[i][j]^-1)*x*Trans[i][j]
//instead of Trans[i][j]*x*(Trans[i][j]^-1)

for k in [1..n] do
  G:=TransitiveGroup(g,k); //it is contained in Sg
  print "-----------------------------------------------------";
  print "-----------------------------------------------------";
  print "We are at the transitive group"; k; print "which is"; G;
  print "-----------------------------------------------------";
  print "-----------------------------------------------------";

  //STABILIZER AND NORMAL COMPLEMENT: Almost classical Galois ext.
  if k gt triv then
    H:=Stabilizer(G,1); //H=G'
    N:=normcomp(G,H);
    if Order(N) gt 1 then //there exists N
      print "------------------------------";
      print "The stabilizer of 1 is"; H;
      print "------------------------------";
      print "The normal complement N of H in G is"; N;
      print "------------------------------";
    end if;
  end if;

  //REGULAR SUBGROUPS OF Sg NORMALIZED BY G
  for i in [1..triv] do
    count:=0;
    for j in [1..#T[i]] do
      //#T[i] is the number os conjugacy classes of TG[i]
      TGij:=sub<S|{(Trans[i][j]^-1)*x*Trans[i][j]:x in Generators(TG[i])}>;
      //we see whether TGij is normalized by G
      NTGij:=Normalizer(S,TGij);
      if G subset NTGij then
        print "The regular subgroup"; TGij;
        print "is normalized by G";
        print "----------------";
        count:=count+1;
      end if;
      delete(TGij); delete(NTGij);
    end for; //j
```

```
    if count ne 0 then
      if i eq 1 then
        print "The number of subgroups conjugated to C8";
        print "normalized by G is";
        count; print "-------------------------";
      elif i eq 2 then
        print "The number of subgroups conjugated to C4xC2";
        print "normalized by G is";
        count; print "-------------------------";
      elif i eq 3 then
        print "The number of subgroups conjugated to C2xC2xC2";
        print "normalized by G is";
        count; print "-------------------------";
      elif i eq 4 then
        print "The number of subgroups conjugated to D4";
        print "normalized by G is";
        count; print "-------------------------";
      elif i eq 5 then
        print "The number of subgroups conjugated to Q8";
        print "normalized by G is";
        count; print "-------------------------";
      end if;
    end if;
    delete(count);
  end for;//i

  delete(G);
  if k gt triv then
    delete(H); delete(N);
  end if;
end for;//k

delete(g); delete(S); delete(n); delete(triv);
```

As a sample of the results obtained performing this program, we list in the following table the number of Hopf Galois structures of each type up to the first five transitive groups, which are shown in Section 5.3.

Table 2: Non-Galois extensions

	Hopf Galois structures				
Transitive group	C_8	$C_4 \times C_2$	$C_2 \times C_2 \times C_2$	$D_{2\cdot 4}$	Q_8
8T6	2	0	0	2	2
8T7	2	0	0	2	2
8T8	2	0	0	2	2
8T9	0	10	4	6	2
8T10	0	6	4	0	0
8T11	2	6	2	6	2
8T12	0	0	2	0	2
8T13	0	0	2	0	2
8T14	0	0	4	0	0
8T15	2	0	0	2	2
8T16	0	0	0	2	2
8T17	0	0	0	2	2
8T18	0	6	4	0	0
8T19	0	2	2	0	0
8T20	0	2	2	0	0
8T22	0	6	2	6	2
8T23	0	0	0	0	2
8T24	0	0	2	0	0
8T25	0	0	1	0	0
8T26	0	0	0	2	2
8T29	0	2	2	0	0
8T32	0	0	2	0	2
8T33	0	0	1	0	0
8T34	0	0	3	0	0
8T36	0	0	1	0	0
8T37	0	0	2	0	0
8T39	0	0	2	0	0
8T40	0	0	0	0	2
8T41	0	0	1	0	0
8T48	0	0	1	0	0

Observe there are some transitive groups which do not give any Hopf Galois structure; specifically, they are

$$8\mathrm{T}i, \text{ for } i \in \{21, 27, 28, 30, 31, 35, 38, 42, 43, 44, 45, 46, 47, 49, 50\}.$$

Note that $8\mathrm{T}49 = A_8$ and $8\mathrm{T}50 = S_8$.

References

[C-S] Chase, Stephen U; Sweedler, Moss E. *Hopf Algebras and Galois Theory*. Vol 97. Berlin: Springer-Verlag; 1969 (Lecture Notes in Mathematics).

[Co] Coward, Anonymous. *Sweedler notation* [Internet]. Published 19/11/2009 [Actualized 03/08/2015; Accessed 29/02/2016].
Electronic address: https://ncatlab.org/nlab/show/Sweedler+notation.

[D-N-R] Dăscălescu, Sorin; Năstăsescu, Constantin; Raianu, Şerban. *Hopf Algebras, An Introduction*. New York: Marcel Dekker; 2001.

[D'An] D'Andrea, Carlos. *Sucesiones Linealmente Recursivas* [Internet]; University of Barcelona: 2005.
Electronic address: https://atlas.mat.ub.edu/personals/dandrea/slr05.pdf.

[G-P] Greither, Cornelius; Pareigis, Bodo. *Hopf Galois Theory of Separable Field Extensions*. Journal of Algebra. 1987; vol 106: 239-258.

[La] Lang, Serge. *Algebra*. Revised Third Edition. USA: Springer; 2002 (Graduate Texts in Mathematics).

[Se1] Serre, Jean-Pierre. *Local Fields*. New York: Springer-Verlag; 1979 (Graduate Texts in Mathematics).

[Se2] Serre, Jean-Pierre. *Cohomologie Galoisienne*. Cinquième édition, révisée et complétée; vol. 5. Springer-Verlag; 1994 (Lecture Notes in Mathematics).

[Un] Underwood, Robert G. *Fundamentals of Hopf Algebras*. Cham: Springer; 2015 (Universitext).