Chapter 1

Preliminaries on Galois theory and Hopf algebras

1 Field theory and Galois theory

Field theory is motivated by the study of algebraic equations and their solutions, or equivalently, the study of polynomials and their roots. The easiest example is that of a second degree polynomial

$$ax^2 + bx + c, \quad a, b, c \in \mathbb{Q}$$

for which the expression

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{1.1}$$

provides its two roots. If $b^2 - 4ac$ is not the square of an integer, these roots are not rational numbers, but in any case they they lie in a field properly containing $\mathbb{Q}$. The usual situation is that an equation with coefficients in a field K has its solutions in a *bigger* field L. This is why the basic notion in field theory is that of extensions of fields.

Definition 1.1.1. *An extension of fields is a pair (L, K) where L and K are fields such that there is a ring monomorphism (or embedding) $\iota\colon K \hookrightarrow L$. We will say that L/K is an extension of fields (or simply an extension) or that L is a field extension of K.*

Typically, the embedding $\iota\colon K \hookrightarrow L$ will be just the inclusion, which corresponds to the situation in which $K \subseteq L$. For convenience, and unless specified otherwise, we will always assume we are in this situation.

1.1 Finite and algebraic extensions

If L/K is an extension of fields, L is naturally endowed with K-vector space structure.

Definition 1.1.2. *Let L/K be an extension of fields.*

1. *The degree of L/K, denoted by $[L : K]$, is defined as the dimension of L as a K-vector space.*

2. *We say that L/K is finite if its degree $[L:K]$ is finite.*

3. *We say that L/K is quadratic (resp. cubic, resp. quartic) if $[L:K]=2$ (resp. $[L:K]=3$, resp. $[L:K]=4$).*

Example 1.1.3. 1. $\mathbb{C}/\mathbb{Q}$ and $\mathbb{R}/\mathbb{Q}$ are extensions of fields with infinite degree.

2. $\mathbb{C}/\mathbb{R}$ is a quadratic field extension, since $\mathbb{C}$ has basis $\{1,i\}$ as an $\mathbb{R}$-vector space.

When we have fields L, E and K such that $K\subseteq E\subseteq L$, we will say that E is an intermediate field of the extension L/K.

Proposition 1.1.4 (Multiplicativity of degrees)**.** *Let E be an intermediate field on L/K. The extension L/K is finite if and only if so are L/E and E/K. In that case,*

$$[L:K]=[L:E][E:K]$$

Among the real numbers, we usually distinguish between rationals and irrationals. But also, among the irrational numbers, there are those that are roots of polynomials with rational coefficients (such as those expressed by radicals), which are called algebraic, and those that do not enjoy this property (like e or π), called transcendental. More generally:

Definition 1.1.5. *Let L/K be an extension of fields.*

1. *We say that $\alpha\in L$ is algebraic over K if it is a root of some non-zero polynomial $f\in K[X]$. Otherwise, we will say that α is transcendental.*

2. *We say that L/K is algebraic if all elements of L are algebraic over K.*

There is the following basic result.

Proposition 1.1.6. *Any finite field extension is algebraic.*

The converse does not hold in general. For instance, the field of complex algebraic numbers over $\mathbb{Q}$ is an algebraic extension of $\mathbb{Q}$ that is not finite.

1.2 Subfield generated by a subset

We can construct easily finite extensions of fields from a field K and a subset of a field extension L of K.

Definition 1.1.7. *Let L/K be an extension of fields and let S be a subset of L. The subfield of L generated by K and S, denoted by $K(S)$, is defined as the intersection of all subfields of L containing K of S.*

The subfield of L generated by K and S can also be seen as the minimal subfield of L containing both K and S.

Suppose that $S=\{\alpha_1,\dots,\alpha_n\}$. It is routine to check that

$$K(S)=\Big\{\frac{f(\alpha_1,\dots,\alpha_n)}{g(\alpha_1,\dots,\alpha_n)}:\ f,g\in K[X_1,\dots,X_n],\ g(\alpha_1,\dots,\alpha_n)\neq 0\Big\}.$$

We will also denote $K(S)\equiv K(\alpha_1,\dots,\alpha_n)$.

When the elements of S are algebraic, then $K(S)$ is actually the minimal subring of L containing both K and S. Thus, in order to describe the elements of $K(S)$, it is enough to consider polynomial expressions of the elements of S.

Proposition 1.1.8. *Let L/K be a field extension and let $S = \{\alpha_1, \ldots, \alpha_n\} \subset L$ be a set of algebraic elements over K. Then*

$$K(S) = \Big\{ f(\alpha_1, \ldots, \alpha_n) : \ f \in K[X_1, \ldots, X_n] \Big\}.$$

Example 1.1.9.

1. Let $f(x) = x^2 + ax + b$ with $a, b \in \mathbb{Q}$ be a monic quadratic polynomial and let α be a root of f, that is,

$$\alpha \in \left\{ \frac{-a + \sqrt{a^2 - 4b}}{2}, \frac{-a - \sqrt{a^2 - 4b}}{2} \right\}.$$

   It can be easily checked that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{a^2 - 4b})$. Now, since $\sqrt{a^2 - 4b}$ is algebraic,

$$\mathbb{Q}(\sqrt{a^2 - 4b}) = \{x + y\sqrt{a^2 - 4b} \ \mid \ x, y \in \mathbb{Q}\}.$$

   As a $\mathbb{Q}$-vector space, this has $\mathbb{Q}$-basis $\{1, \sqrt{a^2 - 4b}\}$. Therefore, $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a quadratic extension of $\mathbb{Q}$.

2. Let $L = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Since $\sqrt{3}$ and $\sqrt{5}$ are algebraic,

$$L = \{a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15} \ \mid \ a, b, c, d \in \mathbb{Q}\}.$$

   We see that $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$ is a $\mathbb{Q}$-basis of L, so $L/\mathbb{Q}$ is a quartic extension.

3. The field $\mathbb{Q}(\pi)$ is the subfield of $\mathbb{R}$ generated by $\mathbb{Q}$ and π. It is not algebraic over $\mathbb{Q}$, since π is transcendental.

Normally, in field theory, to verify a property in an extension $K(S)/K$, it is enough to verify it for S. This is the case for the algebraic property.

Proposition 1.1.10. *Let L/K be an extension of fields and let $S \subseteq L$ be such that $L = K(S)$. If all the elements of S are algebraic over K, then L/K is an algebraic extension.*

1.2.1 Simple and finitely generated extensions

Definition 1.1.11. *Let L/K be an extension of fields.*

1. *We say that L/K is simple if there is some $\alpha \in L$ such that $L = K(\alpha)$. In that case, we will say that α is a primitive element of L/K.*

2. *We say that L/K is finitely generated if there are $\alpha_1, \ldots, \alpha_n \in L$ such that $L = K(\alpha_1, \ldots, \alpha_n)$.*

Before, we saw that every finite extension is algebraic but the converse does not hold. In fact, the notion of finite generation provides a characterization.

Proposition 1.1.12. *An extension of fields L/K is finite if and only if it is algebraic and finitely generated.*

In particular, if L/K is finite, then it is finitely generated, but the converse in general does not hold (the extension $\mathbb{Q}(\pi)/\mathbb{Q}$ above serves as a counterexample).

1.2.2 The compositum of fields

Let L/K be an extension of fields and let E and F be intermediate fields of L/K. In Definition 1.1.7, we may take E as ground field and $S = F$, so that $E(F)$ is the minimal subfield of L containing both E and F. Now, changing the roles of E and F, $F(E)$ is also the minimal subfield of L containing both E and F, so $E(F) = F(E)$.

Definition 1.1.13. *Let K be a field with algebraic closure $\overline{K}$. Let E and F be two extensions of K contained in $\overline{K}$. The compositum of E and F is the minimal subfield of $\overline{K}$ containing both E and F.*

If $E = K(\alpha_1, \ldots, \alpha_n)$ and $F = K(\beta_1, \ldots, \beta_m)$, then

$$EF = K(\{\alpha_i \beta_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}).$$

1.3 Minimal polynomial of an element

Let L/K be an algebraic extension and fix $\alpha \in L$. Let us consider the map

$$\begin{array}{rccc} \Phi_\alpha \colon & K[X] & \longrightarrow & L \\ & f(X) & \longmapsto & f(\alpha) \end{array}.$$

It is a ring homomorphism with kernel

$$\mathrm{Ker}(\Phi_\alpha) = \{f \in K[X] \mid f(\alpha) = 0\}.$$

Recall that $K[X]$ is a principal ideal domain (PID). Then, $\mathrm{Ker}(\Phi_\alpha)$ is a principal ideal, that is, it is generated by a single polynomial. If f is such a generator and $u \in K^\times$, then uf is another generator. If we multiply by the inverse of the leading coefficient of f, we obtain a monic polynomial, which is the only monic generator of $\mathrm{Ker}(\Phi_\alpha)$.

Definition 1.1.14. *Let L/K be an algebraic extension and let $\alpha \in L$. The minimal polynomial of α over K, denoted by* $\mathrm{min.poly.}(\alpha, K)$*, is the monic generator of* $\mathrm{Ker}(\Phi_\alpha)$.

The minimal polynomial of α over K is equivalently defined as the monic polynomial in $K[X]$ with minimal degree having α as a root, and therefore it is irreducible over K. Its degree is actually the degree of $K(\alpha)$:

Proposition 1.1.15. *Let L/K be an extension and let $\alpha \in L$ be an algebraic element over K. Then, $K(\alpha)/K$ is a finite extension and*

$$[K(\alpha) : K] = \deg(\mathrm{min.poly.}(\alpha, K)).$$

Moreover, calling $n := [K(\alpha) : K]$, $\{x^i\}_{i=0}^{n-1}$ is a K-basis of $K(\alpha)$.

We say that any two roots of the same minimal polynomial are conjugate.

1.4 Embeddings, isomorphisms and automorphisms of fields

In our context, an embedding is nothing but an injective homomorphism (i.e, a monomorphism) of fields $\tau\colon L \hookrightarrow E$. Note that the requirement of injectivity is equivalent to σ being non-trivial, since its kernel is either 0 or L.

Definition 1.1.16. *Let $\tau\colon L \hookrightarrow E$ be an embedding and let K be a subfield of L. If $\tau(x) = x$ for all $x \in K$, we will say that τ is a K-embedding.*

Following the usual terminology, a bijective K-embedding is a K-isomorphism. Two fields are said to be K-isomorphic if there exists a K-isomorphism between them. A K-automorphism is a K-isomorphism $\tau\colon L \longrightarrow L$. The group of K-automorphisms of L will be denoted by $\mathrm{Aut}_K(L)$.

Definition 1.1.17. *Let $\sigma\colon K \hookrightarrow E$ and $\tau\colon L \hookrightarrow E$ be two embeddings. We say that τ is an extension of σ if $K \subseteq L$ and $\tau\,|_K = \sigma$.*

Theorem 1.1.18. *Let L/K be an algebraic extension, and let E be a field such that there is an embedding $\sigma\colon K \hookrightarrow E$. Let $S \subseteq L$ be such that $L = K(S)$. If all the polynomials in $\{\text{min.poly.}(\alpha, K) \mid \alpha \in S\}$ have all their roots in L, there is some embedding $\tau\colon L \hookrightarrow E$ that extends σ.*

1.5 Splitting fields and algebraic closure

As already mentioned, a quadratic polynomial with rational coefficients may not have its roots in $\mathbb{Q}$, which is in fact the usual situation. Instead, its roots lie in a quadratic field. More generally:

Theorem 1.1.19 (Fundamental theorem of algebra)**.** *The roots of a polynomial with coefficients in the field $\mathbb{C}$ of complex numbers lie in $\mathbb{C}$.*

Some people say the name of this theorem is unfortunate: it is not *fundamental*, nor it is *of algebra*. In our case, it provides an illustration of the concepts we consider in this part.

Definition 1.1.20. *We say that a field K is algebraically closed if every polynomial with coefficients in K has all its roots in K.*

The fundamental theorem of algebra just states that $\mathbb{C}$ is algebraically closed. Actually, there is a smaller field that is algebraically closed; namely, the field of complex algebraic numbers. Since it is algebraic over $\mathbb{Q}$, it is obtained from adjoining to $\mathbb{Q}$ the roots of all polynomials with rational coefficients. This is what we call an algebraic closure of $\mathbb{Q}$. In general:

Definition 1.1.21. *An algebraic closure of a field K is an algebraically closed field $\overline{L}$ such that $\overline{L}/K$ is an algebraic extension.*

Theorem 1.1.22 (Steinitz)**.** *A field K possesses an algebraic closure and it is unique up to K-isomorphism.*

In particular, if f has its coefficients in a subfield K of the field of algebraic numbers, all its roots are algebraic numbers. In general, for any other field, we can find an extension with this property.

Proposition 1.1.23. *Let K be a field. There is a field extension L of K such that every polynomial $f \in K[X]$ has all its roots in L.*

This allows us to make the following definition.

Definition 1.1.24. *Let L/K be an extension of fields. Let $\mathcal{F} \subseteq K[X]$ and let S be the set of the roots of all polynomials in $\mathcal{F}$. We say that L is a splitting field of $\mathcal{F}$ over K if $L = K(S)$.*

Note that if we choose $\mathcal{F} = K[X]$, we recover the notion of algebraic closure. As in that case, the splitting field always exists and is essentially unique.

Proposition 1.1.25. *Let K be a field and let $\mathcal{F} \subseteq K[X]$ be a subset of non-constant polynomials. Then, there is a splitting field of $\mathcal{F}$ over K and it is unique up to K-isomorphism.*

Example 1.1.26. The polynomial $f(x) = x^4 - 2$ has roots $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$, so its splitting field over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[4]{2}, i)$.

1.6 Normal extensions

The class of normal extensions is fundamental in order to understand the notion of Galois extension. It is defined as follows.

Definition 1.1.27. *Let L/K be an algebraic extension and let $\overline{L}$ be an algebraic closure of L. We say that L/K is normal if for every K-embedding $\sigma\colon L \longrightarrow \overline{L}$ we have that $\sigma(L) = L$ (equivalently, $\sigma \in \mathrm{Aut}_K(L)$).*

In other words, the normal extensions of K are those that are invariant under K-embeddings, which turn out to be K-automorphisms. There are many characterizations for normality, but we will just stand with this one.

Proposition 1.1.28. *Let L/K be an algebraic extension. Then L/K is normal if and only if for every polynomial $f \in K[X]$ with some root in L, f possesses all its roots in L.*

The explanation lies in the fact that the image of a root of a polynomial $f \in K[X]$ by an embedding $\sigma\colon L \longrightarrow \overline{L}$ is necessarily a root of f. Moreover:

Proposition 1.1.29. *Let L/K be a normal extension and let $\alpha, \beta \in L$ be elements with the same minimal polynomial over K. Then, there is some $\sigma \in \mathrm{Aut}_K(L)$ such that $\sigma(\alpha) = \beta$.*

Example 1.1.30.

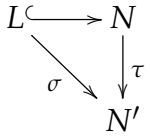
1. Every quadratic extension L/K is normal. Indeed, there is $n \in K$ such that $L = K(\sqrt{n})$, and given an embedding $\sigma\colon L \longrightarrow \overline{L}$, we have $\sigma(\sqrt{n}) = -\sqrt{n}$, so $\sigma(L) = L$.
2. Let $\alpha = \sqrt[3]{2}$ be the real root of $x^3 - 2$. Then $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not normal, because $\zeta_3\alpha$ is another root of $x^3 - 2$, where $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$, and $\zeta_3\alpha \notin \mathbb{Q}(\alpha)$.

It is not true that the class of normal extensions is transitive, that is, for fields $K \subseteq E \subseteq L$, it may happen that L/K is normal but E/K is not. However, we have the following result.

Proposition 1.1.31. *Let K, L and E be fields with $K \subseteq E \subseteq L$. If L/K is normal, then so is L/E.*

There is a notion of normal closure.

Definition 1.1.32. *Let L/K be an algebraic extension. We say that a normal extension N of K containing L is a normal closure of L/K if it is the smallest extension of K with this property. More accurately, for every normal extension N'/K and every K-embedding $\sigma\colon L \hookrightarrow N'$ there is some K-embedding $\tau\colon N \hookrightarrow N'$ making the following diagram commutative:*



In these notes, we will usually write $\widetilde{L}$ for the normal closure of a field extension L/K. The following result provides a method to find a normal closure, and in particular, it proves its existence.

Proposition 1.1.33. *Let L/K be an algebraic extension and let $S \subseteq L$ be such that $L = K(S)$. A normal closure of L/K is the splitting field of $\mathcal{F} = \{\text{min.poly.}(\alpha, K) \mid \alpha \in S\}$ over K.*

As in the case of the algebraic closure, the uniqueness is up to K-isomorphisms.

Proposition 1.1.34. *The normal closure of an algebraic extension L/K is unique up to K-isomorphism.*

Example 1.1.35.

1. If L/K is a normal extension, its normal closure is $\widetilde{L} = L$.
2. Let $L = \mathbb{Q}(\alpha)$ where α is the real root of $x^3 - 2$. The other conjugates of α are $\zeta_3\alpha$ and $\zeta_3^2\alpha$. Therefore, the normal closure of $L/\mathbb{Q}$ is $\widetilde{L} = \mathbb{Q}(\alpha, \zeta_3)$.

1.7 Separable extensions

The notion of separability for an extension is related with the (absence of) multiplicity of roots.

Definition 1.1.36. *Let K be a field. We say that a polynomial $f \in K[X]$ is separable if it does not possess multiple roots in an algebraic closure of K.*

Equivalently, a polynomial $f \in K[X]$ is separable if it has no multiple roots in any extension of K where f has all its roots (such as the splitting field of f over K).

Definition 1.1.37. *Let L/K be an algebraic extension of fields.*

1. *We say that an element $\alpha \in L$ is separable if* $\text{min.poly.}(\alpha, K)$ *is separable.*
2. *We say that L/K is separable if every element of L is separable.*

As in the case of algebraic extensions, the class of separable extensions is transitive.

Proposition 1.1.38. *Suppose that L, K, E are fields with $K \subseteq E \subseteq L$. Then L/K is separable if and only if L/E and E/K are separable.*

For a polynomial f with coefficients in a field K, let us write f' for the formal derivative of f. Then, f has no multiple roots in an algebraic closure if and only if f and f' have no common factors other than constants.

Definition 1.1.39. *A field K is said to be perfect if every algebraic extension of K is separable.*

Recall that the characteristic of a field K, denoted $\mathrm{char}(K)$, is the smallest non-negative integer n such that $n1 = 0$, and it is either 0 (if there is no such an n) or a prime p.

Proposition 1.1.40. *Fields with characteristic zero and finite fields are perfect.*

We finish the section with the following important theorem.

Theorem 1.1.41 (Primitive element theorem)**.** *A finite and separable extension is simple, that is, it admits some primitive element.*

Since $\mathbb{Q}$ has characteristic zero, every algebraic extension of $\mathbb{Q}$ is separable. In particular, every finite extension of $\mathbb{Q}$ is simple.

1.8 Galois extensions

Given a polynomial $f \in K[X]$, we would be happy with a formula as (1.1): an expression that provides all its roots after a finite number of calculations. This is also the situation with degree 3 and 4 equations, but from degree 5 on it does not hold in general. A characterization for the existence of such an expression was found by Galois, whose main idea was to study the permutations of the roots that preserve the algebraic operations between them. In the modern language, these are the automorphisms of the field generated by $\mathbb{Q}$ and the roots. His findings motivated the development of the so called Galois theory.

Definition 1.1.42. *Let L/K be an extension of fields. We say that L/K is Galois if it is normal and separable.*

Note that joining Propositions 1.1.31 and 1.1.38, we obtain:

Corollary 1.1.43. *Let K, L and E be fields with $K \subseteq E \subseteq L$. If L/K is Galois, then so is L/E.*

We have seen that an algebraic extension L/K is normal if for every $f \in K[X]$, f has all its roots in L. On the other hand, L/K is separable if for every $f \in K[X]$, the roots of f in an algebraic closure are all different. We deduce:

Corollary 1.1.44. *Let L/K be a finite Galois extension of degree n. Then L/K possesses n different embeddings, all of which are K-automorphisms.*

It is the group of these K-automorphisms what we define as the Galois group.

Definition 1.1.45. *Let L/K be a Galois extension. The Galois group of L/K, denoted $\mathrm{Gal}(L/K)$, is defined as the group of K-automorphisms of L.*

For a Galois extension L/K with Galois group G, we will sometimes say that L/K is G-Galois.

Note that for an extension L/K which is not Galois, it makes perfect sense to consider the group of K-automorphisms of L. Sometimes, in literature, the Galois group is defined as such regardless of whether the extension is Galois or not. Even though this is not our choice, such a group can be used to give a characterization for the Galois condition.

Proposition 1.1.46. *Let L/K be an algebraic extension and let $G = \mathrm{Aut}_K(L)$. Denote*

$$L^G := \{x \in L \mid \sigma(x) = x \text{ for all } \sigma \in G\}.$$

Then L/K is Galois if and only if $L^G = K$.

The fact, observed by Galois, that the permutations of the roots preserving the algebraic structure form a group, can be formulated in the modern language as follows.

Theorem 1.1.47 (Galois)**.** *Let L/K be a degree n Galois extension with group G and let $f \in K[X]$ be a degree n irreducible polynomial with roots in L. Then G permutes transitively the roots of f, so there is a group monomorphism $G \hookrightarrow S_n$ by which G maps to a transitive group.*

Remark 1.1.48. Suppose that $S = \{\alpha_0, \ldots, \alpha_{n-1}\}$ is the set of roots of f. If the degree of L/K is a prime number p, then G is isomorphic to a transitive subgroup of

$$\{\Pi_{r,s} \mid r, s \in \mathbb{Z}, \gcd(r, p) = 1\},$$

where for each $r, s \in \mathbb{Z}$ with $\gcd(r, n) = 1$, $\Pi_{r,s}$ is the permutation of the roots α_i defined by $\Pi_{r,s}(\alpha_i) = \alpha_{ri+s}$, where subscripts are considered mod p.

The utility of the Galois group is that it encodes information on the extension to which it refers. For instance, we have the following facts, that are very useful when one computes Galois groups.

Proposition 1.1.49. *Let L/K be in the conditions of Theorem 1.1.47. Then, G embeds into A_n if and only if its discriminant is the square of some element in K.*

Recall that the discriminant of a polynomial $f \in K[x]$ is defined as

$$\mathrm{disc}(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2,$$

where $\alpha_1, \ldots, \alpha_n$ are the roots of f.

A more important illustration of the above mentioned phenomenon is that the subgroups of a Galois group are in bijective correspondence with the intermediate fields of the extension to which it refers. This result is commonly known as the fundamental theorem of Galois theory.

Definition 1.1.50. *Let L/K be a Galois extension with group G and let H be a subgroup of G. The subfield of L fixed by H is defined as*

$$L^H = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}.$$

We will also denote the fixed subfield L^H as $\mathrm{Fix}(L, H)$, or simply $\mathrm{Fix}(H)$ when L is implicit in the context.

It is routine to check that a fixed subfield is actually a field.

Theorem 1.1.51 (Fundamental theorem of Galois theory)**.** *Let L/K be a finite Galois extension. The following statements hold:*

1. *There is a bijective inclusion-reversing correspondence*

$$\begin{array}{ccc} \{\textit{Subgroups of } \mathrm{Gal}(L/K)\} & \longrightarrow & \{\textit{Intermediate fields of } L/K\} \\ H & \longmapsto & L^H \\ \mathrm{Gal}(L/E) & \longleftarrow & E \end{array}$$

2. *Given an intermediate field E of L/K, E/K is Galois if and only if $\mathrm{Gal}(L/E)$ is a normal subgroup of $\mathrm{Gal}(L/K)$. In that case, the map*

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(E/K) \\ \sigma & \longmapsto & \sigma\,|_E \end{array}$$

induces a group isomorphism $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/E) \cong \mathrm{Gal}(E/K)$.

1.9 Infinite Galois theory

The fundamental theorem of Galois theory does not necessarily hold for Galois extensions that are not finite: even though the notions of fixed fields and Galois group make perfect sense for infinite extensions, there may be subgroups of the Galois group that do not correspond to any intermediate field. Nevertheless, it is possible to generalize the theorem to arbitrary Galois extensions by means of endowing the Galois group with a topology, so that it becomes a topological group.

Let us briefly review the notions of topological and profinite group.

Definition 1.1.52. *A topological group is a group G together with a topology on G in such a way that the multiplication map $(\sigma, \tau) \in G \times G \longmapsto \sigma\tau \in G$ and the inverse map $\sigma \in G \longmapsto \sigma^{-1} \in G$ are continuous.*

There is a natural notion for homomorphisms between these objects. Namely, if G and G' are topological groups, a map $f\colon G \longrightarrow G'$ is a homomorphism of topological groups if f is a homomorphism of groups and a continuous map with respect to the topologies on G and G'. We will say that f is an isomorphism of topological groups if it is an isomorphism of groups and a homeomorphism.

Definition 1.1.53. *A profinite group is a topological group G which is compact, Hausdorff and such that the identity 1_G admits a system of open neighbourhoods that are normal subgroups of G.*

Proposition 1.1.54. *For a topological group G, the following statements are equivalent:*

1. *G is profinite.*

2. *G is compact, Hausdorff and totally disconnected.*

3. *G is the projective limit of finite groups.*

For the benefit of the reader, we recall briefly the notion of projective limit of groups.

Definition 1.1.55. *Let $(I, \leq)$ be a directed poset (i.e, $\leq$ is a pre-order and every finite subset of I has an upper bound). Let $(G_i)_{i\in I}$ be a family of groups and suppose that for each $i, j \in I$ with $i \leq j$ there is a morphism $f_{ij}\colon G_j \longrightarrow G_i$.*

1. *We say that $\{G_i, f_{ij}\}_{i,j\in I}$ is a projective system if $f_{ii} = \mathrm{Id}_{G_{ii}}$ and $f_{ik} = f_{ij} \circ f_{jk}$ for all $i, j, k \in I$ with $i \leq j \leq k$.*

2. *The projective limit of a projective system $\{G_i, f_{ij}\}_{i,j\in I}$ is defined as the group*

$$\varprojlim_{i\in I} G_i := \{(a_i)_{i\in I} \in \prod_{i\in I} G_i \mid f_{ij}(a_j) = a_i \text{ for all } i, j \in I \text{ with } i \leq j\}.$$

Thus, Proposition 1.1.54 shows that a finite group is necessarily profinite.

Now, let L/K be a Galois extension with group G. We shall endow G with a natural topology, called the Krull topology. For a detailed exposition, see [Neu99, Chapter IV, §1]. Let us write $\mathcal{F}$ for the family of intermediate fields E of L/K such that E/K is a finite Galois subextension of L/K.

Definition 1.1.56. *The Krull topology on G is defined as the topology of G for which a basis of open neighbourhoods of an element $\sigma \in G$ is formed by the left cosets*

$$\sigma\mathrm{Gal}(L/E), \quad E \in \mathcal{F}.$$

A Galois group G endowed with the Krull topology is a topological group. What is more, it is a profinite group. This will follow from the following result, in which we express G as a projective limit of finite groups.

Theorem 1.1.57. *Let L/K be a Galois extension.*

1. *The set $\mathcal{F}$ together with the restriction maps $\pi_{L,L'}\colon \mathrm{Gal}(L'/K) \longrightarrow \mathrm{Gal}(L/K)$, where $L, L' \in \mathcal{F}$ and $L \subseteq L'$, form a projective system.*

2. *There is an isomorphism of topological groups $\mathrm{Gal}(L/K) \cong \varprojlim_{E\in\mathcal{F}} \mathrm{Gal}(E/K)$.*

The correspondence theorem for arbitrary Galois extensions is as follows.

Theorem 1.1.58. *Let L/K be a Galois extension.*

1. *There is a bijective inclusion-reversing correspondence*

$$\begin{array}{ccc} \{\text{Closed subgroups of } \mathrm{Gal}(L/K)\} & \longrightarrow & \{\text{Intermediate fields of } L/K\} \\ H & \longmapsto & L^H \\ \mathrm{Gal}(L/E) & \longleftarrow & E \end{array}$$

   Under this correspondence, the closed subgroups of $\mathrm{Gal}(L/K)$ that are also open correspond to the finite subextensions of L/K.

2. *Given an intermediate field E of L/K, E/K is Galois if and only if $\mathrm{Gal}(L/E)$ is a normal subgroup of $\mathrm{Gal}(L/K)$. In that case, the map*

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(E/K) \\ \sigma & \longmapsto & \sigma\,|_E \end{array}$$

   induces an isomorphism of topological groups $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/E) \cong \mathrm{Gal}(E/K)$.

1.10 Exercises

1. Let K be a field with $\mathrm{char}(K) = 0$. Let L and M be finite extensions of K and M/K is Galois.

   (a) Prove that LM/L is Galois and that there is an embedding $\mathrm{Gal}(LM/L) \hookrightarrow \mathrm{Gal}(M/K)$, which becomes an isomorphism if $L \cap M = K$.

   (b) Suppose that L/K is also Galois. Show that LM/K is Galois and that there is an embedding $\mathrm{Gal}(LM/K) \hookrightarrow \mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K)$, which becomes an isomorphism if $L \cap M = K$.

2. Let L be the splitting field of the polynomial $f(x) = x^4 + 6x^2 - 3$ over $\mathbb{Q}$. Determine completely the lattice of intermediate fields of $L/\mathbb{Q}$ and the lattice of subgroups of $\mathrm{Gal}(L/\mathbb{Q})$.

   Note: L is also the splitting field of the polynomial $x^4 - 3x^2 + 3$ over $\mathbb{Q}$.

3. Let L/K be a Galois extension with group G.

   (a) Show that G endowed with the Krull topology is a topological group.

   (b) Prove that the Krull topology on G is discrete if and only if L/K is finite. Deduce that the fundamental theorem of Galois theory at the infinite case is a generalization of the one for the finite case.

4. For each $m \in \mathbb{Z}_{>0}$, write L_m for the m-th cyclotomic field; that is, $L_m := \mathbb{Q}(\zeta_m)$, where ζ_m is a primitive m-th root of unity. In addition, for a prime number p, let $L_{p^\infty} = \bigcup_{n \in \mathbb{Z}_{>0}} L_{p^n}$ be the union of all the fields L_{p^n} (which is a field because $L_{p^n} \subset L_{p^{n+1}}$ for all $n \in \mathbb{Z}_{>0}$).

   (a) Prove that $L_m/\mathbb{Q}$ is Galois and that $\mathrm{Gal}(L_m/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.

   Note: You do not need to prove the result that all the conjugates of ζ_m are ζ_m^k for $1 \leq k \leq m$ and $\gcd(k, m) = 1$.

   (b) Show that for each intermediate field E of $L_{p^\infty}/\mathbb{Q}$ such that $E/\mathbb{Q}$ is finite, there is some $n \in \mathbb{Z}_{>0}$ such that $E \subseteq L_{p^n}$. Deduce that if in addition $E/\mathbb{Q}$ is Galois, then it is abelian.

   (c) Prove that $L_{p^\infty}/\mathbb{Q}$ is Galois and that $\mathrm{Gal}(L_{p^\infty}/\mathbb{Q}) \cong (\mathbb{Z}_p)^\times$, the multiplicative group of the ring of p-adic integers.

   Note: You are allowed to use the definition of $\mathbb{Z}_p$ as a projective limit.

2 Hopf algebras and their actions on modules

In this section we will introduce the notion of Hopf algebra. It is a versatile object that appears in several areas of mathematics. Our interest in them is due to their connection with group theory. Throughout this section, R will be a commutative ring with unity $1 \equiv 1_R$ and unadorned tensor products will be taken over R.

2.1 Basic definitions

Definition 1.2.1. *An R-**Hopf algebra** is a 6-uple $(H, m_H, u_H, \Delta_H, \varepsilon_H, S_H)$ where:*

1. *H is an R-module.*
2. *$m_H \colon H \otimes H \longrightarrow H$ and $u_H \colon R \longrightarrow H$ are R-linear maps that satisfy:*
   (a) **(Associative property)** *Given $a, b, c \in H$,*
   $$m_H \circ (m_H \otimes Id_H)(a \otimes b \otimes c) = m_H \circ (Id_H \otimes m_H)(a \otimes b \otimes c).$$
   Equivalently, the following diagram is commutative:
   $$\begin{array}{ccc} H \otimes H \otimes H & \xrightarrow{Id_H \otimes m_H} & H \otimes H \\ \downarrow{\scriptstyle m_H \otimes Id_H} & & \downarrow{\scriptstyle m_H} \\ H \otimes H & \xrightarrow{m_H} & H \end{array}$$
   (b) **(Unit properties)** *Given $a \in H$ and $r \in R$,*
   $$m_H \circ (u_H \otimes \mathrm{Id}_H)(r \otimes a) = r\,a = m_H \circ (\mathrm{Id}_H \otimes u_H)(a \otimes r).$$
   Equivalently, the following diagrams are commutative:
   $$\begin{array}{ccc} H \otimes R & \xrightarrow{Id_H \otimes u_H} & H \otimes H \\ \downarrow{\scriptstyle s_2} & \swarrow{\scriptstyle m_H} & \uparrow{\scriptstyle u_H \otimes Id_H} \\ H & \xleftarrow[s_1]{} & R \otimes H \end{array}$$
   where $s_1 \colon R \otimes H \longrightarrow H$ and $s_2 \colon H \otimes R \longrightarrow H$ are defined by $s_1(r \otimes a) = r\,a = s_2(a \otimes r)$.

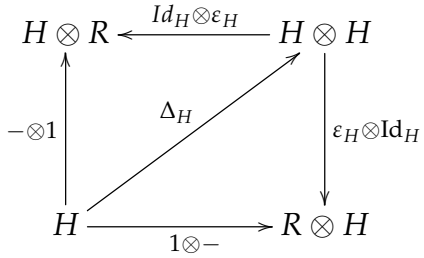
   *The map m_H is called **multiplication map**, and u_H is called **unit map**.*

3. *$\Delta_H \colon H \longrightarrow H \otimes H$ and $\varepsilon_H \colon H \longrightarrow R$ are R-linear maps that satisfy:*
   (a) **(Coassociative property)** *For all $h \in H$,*
   $$(Id_H \otimes \Delta_H)\Delta_H(h) = (\Delta_H \otimes Id_H)\Delta_H(h).$$
   Equivalently, there is a commutative diagram:
   $$\begin{array}{ccc} H \otimes H \otimes H & \xleftarrow{\mathrm{Id}_H \otimes \Delta_H} & H \otimes H \\ \uparrow{\scriptstyle \Delta_H \otimes \mathrm{Id}_H} & & \uparrow{\scriptstyle \Delta_H} \\ H \otimes H & \xleftarrow{\Delta_H} & H \end{array}$$

(b) **(Counit properties)** *For all $h \in H$,*

$$(\varepsilon_H \otimes Id_H)\Delta_H(h) = 1 \otimes h,$$
$$(Id_H \otimes \varepsilon_H)\Delta_H(h) = h \otimes 1.$$

Equivalently, the following diagrams are commutative:



*The map Δ_H is called **comultiplication map** and ε_H is called **counit map** or **augmentation**.*

4. *Δ_H and ε_H are ring homomorphisms, where H is endowed with the ring structure induced by the maps m_H and u_H, and $H \otimes H$ is endowed with the ring structure induced by the one at H.*

5. *$S_H \colon H \longrightarrow H$ is an R-linear map, called **coinverse map** or **antipode** satisfying the following property:*

$$m_H \circ (\mathrm{Id}_H \otimes S_H) \circ \Delta_H(h) = \varepsilon_H(h)\, 1_H = m_H \circ (S_H \otimes Id_H) \circ \Delta_H(h),\ h \in H.$$

If 1 and 2 hold, we say that (H, m_H, ε_H) is an R-algebra.
If 1 and 3 hold, we say that $(H, \Delta_H, \varepsilon_H)$ is an R-coalgebra.
If 1-4 hold, we say that $(H, m_H, u_H, \Delta_H, \varepsilon_H)$ is an R-bialgebra.

We will usually refer to an R-Hopf algebra $(H, m_H, u_H, \Delta_H, \varepsilon_H, S_H)$ just as H, leaving implicit the R-Hopf algebra operations.

Let H be an R-Hopf algebra. The R-module structure of H will be called the underlying module of the R-Hopf algebra H. On the other hand, the operation

$$ab := m_H(a \otimes b), \quad a, b \in H$$

endows H with a ring structure, called the underlying ring of the R-Hopf algebra H. This is the ring structure at H mentioned at 4. Since we have assumed that R is a ring with unity, the underlying ring of an R-Hopf algebra has always a unity, namely $1_H = u_H(1_R)$. Indeed,

$$1_H a = u_H(1_R)a = m_H(u_H(1_R) \otimes a) = m_H(u_H \otimes \mathrm{Id}_H)(1_R \otimes a) = 1_R a = a,$$

and similarly $a1_H = a$.

Definition 1.2.2. *Let M be an R-module. The **twist map** of M is the map $\tau \colon M \otimes M \longrightarrow M \otimes M$ defined by*

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

for every $a, b \in M$.

Definition 1.2.3. *Let H be an R-Hopf algebra.*

1. *We say that H is **commutative** if $m_H \circ \tau = m_H$. Equivalently, the underlying ring structure of H is commutative.*

2. *We say that H is **cocommutative** if $\tau \circ \Delta_H = \Delta_H$.*

2.2 First examples

Example 1.2.4. A commutative ring R with unity is an R-Hopf algebra over itself, called the trivial Hopf algebra.

Example 1.2.5 ([Und15], Example 3.1.4)**.** Let $H = R[x,y]/\langle xy - 1\rangle$. This can be naturally endowed with R-algebra structure. Define $\Delta_H \colon H \longrightarrow H \otimes H$ by

$$\Delta_H(x) = x \otimes x, \quad \Delta_H(y) = y \otimes y,$$

$\varepsilon_H \colon H \longrightarrow R$ by

$$\varepsilon_H(x) = 1, \quad \varepsilon_H(y) = 1$$

and $S_H \colon H \longrightarrow H$ by

$$S_H(x) = y, \quad S_H(y) = x.$$

Then H is a commutative and cocommutative R-Hopf algebra.

The example of Hopf algebra that is of our interest is the following.

Definition 1.2.6. *Let G be a group. The R-**group algebra** of G with coefficients in R, denoted $R[G]$, is the set*

$$R[G] = \Big\{ \sum_{g \in G} a_g g \,|\, a_g \in R,\ a_g = 0 \text{ for all but finitely many } g \in G \Big\}.$$

If the group G is finite, the last condition is vacuous. Note that $R[G]$ is free as an R-module, and a basis is formed by the elements of G. This is a very useful fact: it means that any R-linear notion or result referring to $R[G]$ can be reduced to stating or proving it for the elements of G. The same holds for tensor products of group algebras.

Proposition 1.2.7. *Let G be a finite group. Then $R[G]$ is an R-Hopf algebra with the following operations:*

1. *Multiplication map defined by $m_{R[G]}(g \otimes h) = gh$ for every $g, h \in G$ and unit map given by $u_{R[G]}(r) = r1_G$.*

2. *Comultiplication given by $\Delta_{R[G]}(g) = g \otimes g$ for every $g \in G$ and counit given by $\varepsilon_{R[G]}(g) = 1$ for every $g \in G$.*

3. *Antipode $S_{R[G]} \colon R[G] \longrightarrow R[G]$ defined by $S_{R[G]}(g) = g^{-1}$ for all $g \in G$ and extended by R-linearity.*

Proposition 1.2.8. *Let G be a group.*

1. *$R[G]$ is commutative if and only if G is abelian.*

2. *$R[G]$ is cocommutative.*

3. *If G is finite, $R[G]$ is a free R-module with rank $|G|$.*

The proof of these two results is a routine check that is left to the reader.

If $R = K$ is a field, Proposition 3 is the statement that $K[G]$ is a K-vector space with dimension $|G|$.

2.3 Homomorphisms of Hopf algebras

We have defined a Hopf algebra as a structure composed by more simple structures. In the same way, the notion of a homomorphism of a Hopf algebras arises naturally as a homomorphism between these structures.

Definition 1.2.9. *An R-Hopf algebra homomorphism between two R-Hopf algebras H, H' is a map $f : H \longrightarrow H'$ such that:*

1. *f is an R-linear map between the underlying R-module structures of H and H'.*

2. *f is a homomorphism between the underlying ring structures of H and H', that is:*

   (a) $f \circ m_H = m_{H'} \circ (f \otimes f)$.

   (b) $f \circ u_H = u_{H'}$.

3. *f preserves the comultiplication and the counit of H, meaning that:*

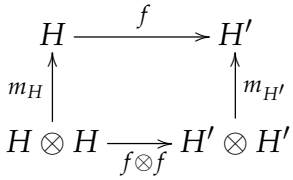
   (a) $\Delta_{H'} \circ f = (f \otimes f) \circ \Delta_H$.

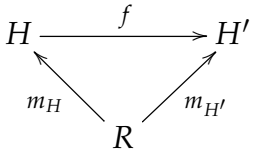
   (b) $\varepsilon_H = \varepsilon_{H'} \circ f$.

4. *f preserves the antipode of H, meaning that $f \circ S_H = S_{H'} \circ f$.*

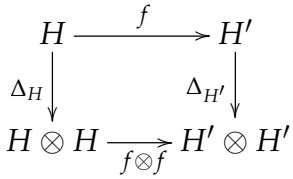
If f satisfies 1 and 2, we say that f is a homomorphism of R-algebras.
If f satisfies 1 and 3, f is said to be a homomorphism of R-coalgebras.
If f satisfies 1-3, we will say that f is a homomorphism of R-bialgebras.
In all these cases, H and H' can be required to be just R-algebras, R-coalgebras or R-bialgebras, respectively.

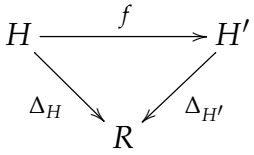
The conditions 2a and 2b are equivalent to the commutativity of these diagrams:





Likewise, the conditions 3a and 3b are equivalent to the commutativity of these other diagrams:





As for the condition 4, it is equivalent to the commutativity of this diagram:

$$\begin{array}{ccc} H & \xrightarrow{f} & H' \\ {\scriptstyle S_H}\downarrow & & \downarrow{\scriptstyle S_{H'}} \\ H & \xrightarrow[f]{} & H' \end{array}$$

We use the terminology of R-Hopf algebra monomorphisms, epimorphisms, endomorphisms and automorphisms in the usual way.

Definition 1.2.10. *We say that two R-Hopf algebras H and H' are isomorphic if there is some isomorphism of R-Hopf algebras $f\colon H \longrightarrow H'$.*

2.4 Sub-Hopf algebras

It is usual, when an algebraic structure is introduced, that we consider its substructures. In this section, we shall view the notion of R-sub-Hopf algebra of an R-Hopf algebra. Fix an R-Hopf algebra H. Following the pattern viewed in other algebraic structures (groups, rings, vector spaces, etc), we may think of an R-sub-Hopf algebra of H as a subset $B \subseteq H$ inheriting the Hopf algebra structure of H. This would mean that we can restrict the Hopf algebra operations of H successfully so that they endow B with Hopf algebra structure. However, there is a technical difficulty at this point, and is related with the presence of the tensor product in the Hopf algebra operations. Namely, if $B \subseteq H$, the canonical inclusion $i\colon B \hookrightarrow H$ induces the map

$$\begin{array}{rccc} i \otimes i\colon & B \otimes B & \longrightarrow & H \otimes H, \\ & s \otimes s & \longrightarrow & i(s) \otimes i(s), \end{array}$$

but in general $i \otimes i$ is not injective. Thus, for those cases in which indeed $i \otimes i$ is not injective, it does not make sense to wonder whether the multiplication map $m_H\colon H \otimes H \longrightarrow H$ of H *restricts* to B, since $B \otimes B$ is not a subset of $H \otimes H$. Likewise, it does not make sense to ask if the image of B by the comultiplication map $\Delta_H\colon H \longrightarrow H \otimes H$ lies in $B \otimes B$.

Definition 1.2.11. *Let H be an R-Hopf algebra and let B be an R-submodule of H. Let $i\colon B \longrightarrow H$ be the canonical inclusion and suppose that $i \otimes i$ is injective. We say that B is an R-sub-Hopf algebra of H if:*

1. *$m_H(B \otimes B) \subset B$ and $1_H \in B$.*
2. *$\Delta_H(B) \subset B \otimes B$.*
3. *$S_H(B) \subset B$.*

In that case, the Hopf algebra operations of B are obtained by restricting those of H. Namely:

- *Multiplication map: $m_B \coloneqq m_H\,|_{B\otimes B}\colon B \otimes B \longrightarrow B$.*
- *Unit map $u_B \coloneqq u_H\colon R \longrightarrow B$.*

- *Comultiplication map:* $\Delta_B \coloneqq \Delta_H|_B \colon B \longrightarrow B \otimes B$.
- *Counit map:* $\varepsilon_B \coloneqq \varepsilon_H|_B \colon B \longrightarrow R$.
- *Coinverse map:* $S_B \coloneqq S_H|_B \colon B \longrightarrow B$.

The injectivity of $i \otimes i$ is not restrictive at all. We can regard $i \otimes i$ as the composition

$$B \otimes B \xrightarrow{i \otimes \mathrm{Id}_B} H \otimes B \xrightarrow{\mathrm{Id}_H \otimes i} H \otimes H$$

If B and H are flat as R-modules, both $i \otimes \mathrm{Id}_B$ and $\mathrm{Id}_H \otimes i$ are injective, and hence so is $i \otimes i$. In particular, this holds when R is a field, which will be our typical situation.

We finish the section with an example of computation of sub-Hopf algebras of a group algebra over a field.

Theorem 1.2.12. *Let K be a field and let G be a finite group. The K-sub-Hopf algebras of $K[G]$ are of the form $K[H]$, with H a subgroup of G.*

Proof. It is clear that any K-group algebra $K[H]$ with H subgroup of G is a K-sub-Hopf algebra of $K[G]$.

Let B be a K-sub-Hopf algebra of $K[G]$. We must check that B is of the form $K[H]$ for some subgroup H of G. Since B is a K-sub-Hopf algebra of $K[G]$, in particular, B is a K-sub-vector space of $K[G]$. We know that $G = \{g_1, \cdots, g_n\}$ is a K-basis of $K[G]$. Let $m = \dim(B)$ and let $k = n - m$. By basic linear algebra, we deduce that B can be described by k equations

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = 0 \\ \cdots \\ a_{k1}x_1 + \cdots + a_{kn}x_n = 0 \end{cases}$$

with respect to the basis $\{g_{m+1}, \cdots, g_n, g_1, \cdots, g_m\}$. Let us consider the matrix

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{k1} & \cdots & a_{kn} \end{pmatrix}.$$

By Gauss method, A is congruent by rows to a matrix of the form

$$\begin{pmatrix} 1 & \cdots & 0 & -\lambda_{m+1}^{(1)} & \cdots & -\lambda_{m+1}^{(n)} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 1 & -\lambda_n^{(1)} & \cdots & -\lambda_n^{(n)} \end{pmatrix}.$$

Then, B has a basis of the form

$$\begin{cases} v_1 = g_1 + \sum_{i=m+1}^{n} \lambda_i^{(1)} g_i \\ \cdots \\ v_m = g_m + \sum_{i=m+1}^{n} \lambda_i^{(m)} g_i \end{cases}.$$

Since B is K-sub-coalgebra, $\Delta_B(v_j) \in B \otimes_K S$ for all $j \in \{1, \dots, m\}$. Let us find the coordinates of $\Delta_B(v_j)$ with respect to the basis $\{v_i \otimes v_j\}_{1 \leq i \leq m, 1 \leq j \leq m}$ of $B \otimes_K S$. We have

$$\begin{cases} \Delta_B(v_1) = g_1 \otimes g_1 + \sum_{i=m+1}^{n} \lambda_i^{(1)} g_i \otimes g_i \\ \dots \\ \Delta_B(v_m) = g_m \otimes g_m + \sum_{i=m+1}^{n} \lambda_i^{(m)} g_i \otimes g_i \end{cases}$$

and then for $1 \leq i, j \leq m$,

$$v_i \otimes v_j = g_i \otimes g_j + \sum_{k=m+1}^{n} (\lambda_k^{(j)} g_i \otimes g_k + \lambda_k^{(i)} g_k \otimes g_j) + \sum_{k,l=m+1}^{n} \lambda_k^{(i)} \lambda_l^{(j)} g_k \otimes g_l.$$

Now, for each $1 \leq i, j \leq m$, $g_i \otimes g_j$ only appears once in the expression of $v_i \otimes v_j$. If $\Delta_C(v_j) = \sum_{k,l=1}^{m} c_{kl} v_k \otimes v_l$, since the elements $g_k \otimes g_l$ are linearly independent in $K[G] \otimes K[G]$, we deduce that $c_{kl} = 0$ for all $k, l \neq j$ and $c_{jj} = 1$. Thus, $\Delta(v_j) = v_j \otimes v_j$. That is,

$$g_i \otimes g_j + \sum_{i=m+1}^{n} \lambda_i^j = g_j \otimes g_j + \sum_{k=m+1}^{n} \lambda_k^{(j)} (g_k \otimes g_k + g_k \otimes g_j) + \sum_{k,l=m+1}^{n} \lambda_k^{(j)} \lambda_l^{(j)} g_k \otimes g_l.$$

Since $g_j \otimes g_i$ does not appear in the leftside member and it does in the rightside one with coefficient $\lambda_i^{(j)}$, $\lambda_i^{(j)} = 0$ for all $i \in \{m+1, \dots, n\}$. Since j is arbitrary, we deduce that $v_i = g_i$ for all $i \in \{1, \dots, m\}$.

Let $H = \{g_1, \dots, g_m\}$. We have just checked that H is a K-basis of B, whence $B = K[H]$. Since B is a K-subalgebra of $K[G]$, H is a subgroup of G. □

Remark 1.2.13. Theorem 1.2.12 will follow directly from a correspondence involving Hopf algebras from the next chapter.

2.5 Sweedler's notation

When doing computations in which R-coalgebras are involved, we will denote elements at the image of the comultiplication in an especial way so as to work with them easily. This is the **Sweedler notation**. We shall work with Hopf algebras just because it is our situation, but the following applies in the same way for R-coalgebras. Let H be an R-Hopf algebra, and let $h \in H$. We write

$$\Delta_H(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)}. \tag{1.2}$$

Note that $h_{(1)}$ and $h_{(2)}$ are just symbolic labels that do not refer to any particular element of H. We know that an element of $H \otimes H$ is a sum of elements of the form $h_1 \otimes h_2$ for $h_1, h_2 \in C$, and this expression refers to any sum of elements of such form that equals $\Delta_H(h)$.

As an immediate application, the counit properties at Definition 1.2.1 3b translate into

$$\sum_{(h)} \varepsilon_H(h_{(1)}) h_{(2)} = h = \sum_{(h)} h_{(1)} \varepsilon_H(h_{(2)}). \tag{1.3}$$

On the other hand, the coassociative property gives

$$\sum_{(h)} h_{(1)} \otimes h_{(2)_{(1)}} \otimes h_{(2)_{(2)}} = \sum_{(h)} h_{(1)_{(1)}} \otimes h_{(1)_{(2)}} \otimes h_{(2)}.$$

We denote this element by

$$\Delta_2(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)} \otimes h_{(3)}.$$

At the same time, we can apply to this element any of the three maps which is the tensor product of twice Id_H and Δ_H, and by coassociativity, all of them will give the same element, denoted

$$\Delta_3(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)} \otimes h_{(3)} \otimes h_{(4)}.$$

Iterating this procedure, we write

$$\Delta_{n-1}(h) = \sum_{(h)} h_{(1)} \otimes \cdots \otimes h_{(n)}$$

for the unique element obtained by iterating coassociativity n times.

2.6 Grouplike elements

On a Hopf algebra we have distinguished elements that can be seen in a certain way as analogues of elements of groups, the so-called grouplike elements.

Definition 1.2.14. *Let H be an R-Hopf algebra. We say that a non-zero element $h \in H$ is **grouplike** if $\Delta_H(h) = h \otimes h$.*

Example 1.2.15. Let G be a finite group. By definition of the comultiplication $\Delta_{R[G]}$ of the R-group algebra $R[G]$, the elements of G are grouplike elements of $R[G]$.

Proposition 1.2.16. *Let H be an R-Hopf algebra and suppose that the only idempotents of R are 0 and 1. If $h \in H$ is grouplike, then $\varepsilon_H(h) = 1$.*

Proof. Since h is grouplike, we have that $\Delta_H(h) = h \otimes h$, and (1.3) translates into $h = \varepsilon_H(h)h$. Applying ε_H yields

$$\varepsilon_H(h) = \varepsilon_H(\varepsilon_H(h)h) = \varepsilon_H(h)\varepsilon_H(h),$$

that is, $\varepsilon_H(h)$ is idempotent of R. Our hypothesis in R gives $\varepsilon_H(h) \in \{0, 1\}$, and since $h \neq 0$, necessarily $\varepsilon_H(h) = 1$. □

Remark 1.2.17. Some authors add the condition that $\varepsilon_H(h) = 1$ to the definition of h being grouplike, and they label our grouplike elements as *semi-grouplike*. If R is a field, the only idempotents of R are of course 0 and 1.

Write $G(H)$ for the set of grouplike elements of an R-Hopf algebra H.

Theorem 1.2.18. *If R has no zero divosors, $G(H)$ is linearly independent over R.*

Proof. This proof comes from [Und15, Proposition 1.2.18], where the result is proved under the assumption that R is a field.

If $G(H) = \emptyset$, then $G(H)$ is R-linearly independent. If $G(H)$ contains just one element, this element is necessarily non-zero, so $G(H)$ is R-linearly independent. Thus we can assume that $G(H)$ contains at least two elements.

Let us suppose that $G(H)$ is R-linearly dependent. Since $|G(H)| \geq 2$, $G(H)$ contains some R-linearly independent subset. Let m be the largest integer such that $G(H)$ contains an R-linearly independent subset $S = \{h_i\}_{i=1}^m$ with cardinal m. Let $h \in G(H) - S$. Then there are scalars $r_i \in R$ such that

$$h = \sum_{i=1}^{m} r_i h_i.$$

Applying the comultiplication, since $h_i \in G(H)$, we have

$$\Delta_H(h) = \sum_{i=1}^{m} r_i h_i \otimes h_i.$$

But, since $h \in G(H)$, we also get

$$\Delta_H(h) = h \otimes h = \sum_{i,j=1}^{m} r_i r_j h_i \otimes h_j.$$

Hence,

$$\sum_{i=1}^{m} r_i h_i \otimes h_i = \sum_{i,j=1}^{m} r_i r_j h_i \otimes h_j.$$

Since S is an R-linearly independent subset of H by definition, $\{h_i \otimes h_j\}_{i,j=1}^m$ is an R-linearly independent subset of $H \otimes H$. Therefore $r_i r_j = 0$ whenever $i \neq j$ and $r_i^2 = r_i$ for every $1 \leq i \leq m$. Since $h \neq 0$, there is some $1 \leq i \leq m$ is such that $r_i \neq 0$. Since R has no zero divisors and $r_i(r_i - 1) = 0$, necessarily $r_i = 1$. Moreover $r_j = 0$ for any other j. We conclude that $h = h_i \in S$, which contradicts our choice of h. □

In Example 1.2.15 we saw that the elements of a group G are grouplike elements of the R-group algebra $R[G]$. If R has no zero divisors, we can use Theorem 1.2.18 to prove that the elements of G are actually *all* the grouplike elements of $R[G]$.

Corollary 1.2.19. *Let G be a finite group. If R has no zero divisors, then $G(R[G]) = G$.*

Proof. By Example 1.2.15, the elements of G belong to $G(R[G])$, so $G \subseteq G(R[G])$. But by Theorem 1.2.18, $|G(R[G])| \leq \mathrm{rk}_R(R[G]) = |G|$. Then the equality follows. □

In particular, the grouplike elements of an R-group algebra form a group. This is actually a general fact for grouplike elements of a Hopf algebra.

Proposition 1.2.20 ([Chi00], (1.6))**.** *$G(H)$ is a group with the product of H.*

Proof. First, since Δ_H is an R-algebra homomorphism and the unit of $H \otimes H$ is $1 \otimes 1$, $\Delta_H(1) = 1 \otimes 1$. Then $1 \in G(H)$, so $G(H)$ is not empty.

Let $h_1, h_2 \in G(H)$. Then,

$$\begin{aligned}\Delta_H(h_1\, h_2) &= \Delta_H(m_H(h_1 \otimes h_2)) \\ &= m_{H\otimes H}(\Delta_H(h_1) \otimes \Delta_H(h_2)) \\ &= m_{H\otimes H}((h_1 \otimes h_1) \otimes (h_2 \otimes h_2)) \\ &= (h_1\, h_2) \otimes (h_1\, h_2),\end{aligned}$$

which proves that $h_1\, h_2 \in G(H)$.

Given $h \in G(H)$,

$$\begin{aligned}h\, S_H(h) = m_H(h \otimes S_H(h)) = m_H(Id_H \otimes S_H)(h \otimes h) = \\ = m_H(Id_H \otimes S_H)\Delta_H(h) \quad , \\ = \epsilon_H(h)\, 1_H = 1_H\end{aligned}$$

and similarly, $\sigma_H(h)\, h = 1_H$. So it is enough to prove that $S_H(h) \in G(H)$. We have that $h\, S_H(h) = 1_H$, so

$$\begin{aligned}1_H \otimes 1_H &= \Delta_H(m_H(Id_H \otimes S_H)(h \otimes h)) \\ &= m_{H\otimes H}(\Delta_H(h) \otimes \Delta_H(S_H(h))) \\ &= m_{H\otimes H}((h \otimes h) \otimes \Delta_H(S_H(h))) = (h \otimes h)\, \Delta_H(S_H(h)).\end{aligned}$$

By the uniqueness of the inverse in the algebra $H \otimes H$, $\Delta_H(S_H(h)) = S_H(h) \otimes S_H(h)$, so $S_H(h) \in G(H)$ as we wanted. □

From Corollary 1.2.19 it also follows that the grouplike elements of R-group algebras $R[G]$ with G finite form an R-basis. Under the assumption that R has no zero divisors, they are the only finitely generated and free R-Hopf algebras with this behaviour.

Corollary 1.2.21. *Suppose that R has no zero divisors and let H be a finitely generated and free R-Hopf algebra admitting an R-basis G formed by grouplike elements. Then $G = G(H)$ and $H = R[G]$.*

Proof. By hypothesis, $G \subseteq G(H)$ and G is an R-basis of H. We know from Theorem 1.2.18 that $G(H)$ is R-linearly independent, so necessarily $G = G(H)$. In particular, G is a group, so it makes sense to consider the R-group algebra $R[G]$. Since G is an R-basis of H, we can regard H as the R-span of the elements of G. Moreover, multiplication is closed for elements of N, so $H = R[G]$ follows. □

2.7 Duality

Recall that the dual of an R-module M, denoted M^*, is the set

$$\mathrm{Hom}_R(M, R) = \{f \colon M \longrightarrow R \mid f \text{ } R\text{-linear}\}.$$

Note that $\mathrm{Hom}_R(M, R)$ becomes also an R-module when it is endowed with pointwise multiplication by R. Moreover, an R-linear map $\varphi \colon M \longrightarrow M'$ gives rise to a map $\varphi^* \colon M'^* \longrightarrow M^*$ defined by $\varphi^*(g)(m) = g(\varphi(m))$, where $m \in M$ and $g \in M'^*$. Thus, we have a contravariant functor at the category of R-modules, which we call the **duality functor**.

2.7.1 Finite R-modules and projective coordinate sytems

If R is a field and M is a finite dimensional R-vector space, then it is well known that for every R-basis $\{m_i\}_{i=1}^n$ of M there is an R-basis $\{f_i\}_{i=1}^n$ of M^*, called the dual basis, such that $f_i(m_j) = \delta_{ij}$ for every $1 \leq i, j \leq n$, where δ_{ij} is the Kronecker delta. However, we want to keep a broader perspective, since it is often useful to consider dual modules over rings. The analogue over rings to finite dimensional vector spaces over fields are finitely generated and projective modules. We will refer to such modules as finite. Namely:

Definition 1.2.22. *Let M be an R-module.*

1. *We say that M is finitely generated if there is a finite subset $\{m_i\}_{i=1}^n \subset M$ such that $M = \sum_{i=1}^n Rm_i$.*
2. *We say that M is projective if it is a direct summand of a free R-module.*
3. *We say that M is finite if it is finitely generated and projective.*

The analogy between finite dimensional vector spaces and finite modules lies in the following result:

Proposition 1.2.23. *An R-module M is finite if and only if there are $n \in \mathbb{Z}_{\geq 1}$ and elements $m_1, \ldots, m_n \in M$, $f_1, \ldots, f_n \in M^*$ such that for each $m \in M$ we have*

$$m = \sum_{i=1}^{n} f_i(m) m_i.$$

Definition 1.2.24. *Let M be a finite R-module. A set $\{m_i, f_i\}_{i=1}^n$ as in Proposition 1.2.23 is called a **projective coordinate system** for M.*

When R is a field, finite R-modules are actually finite-dimensional R-vector spaces, and the union of a basis together with its dual is a projective coordinate system.

Remark 1.2.25. Free modules of finite rank are finite, but the converse in general does not hold. The existence of a projective coordinate system is coherent with this fact, because the expression of m with respect to the elements m_i may not be unique.

Remark 1.2.26. If $\{m_i, f_i\}_{i=1}^n$ is a projective coordinate system for a finite R-module M, we can also write elements of M^* with respect to the f_i. Indeed, given $m \in M$, we know that $m = \sum_{i=1}^n f_i(m) m_i$. Applying f at both sides, we obtain $f(m) = \sum_{i=1}^n f(m_i) f_i(m)$. Since m is arbitrary, this means that

$$f = \sum_{i=1}^{n} f(m_i) f_i.$$

Proposition 1.2.27. *If M is a finite R-module, then so is M^*. Moreover, there is a canonical isomorphism $M \cong M^{**}$ as R-modules.*

Proof. Suppose that M is a finite R-module. Then M is a direct summand of a free R-module of finite rank n, that is, there is an R-module N such that $R^n = M \oplus N$. Now, applying the duality functor, we have that $R^n = M^* \oplus N^*$, so M^* is finitely generated and projective.

Let us define

$$\begin{array}{rccl} \eta\colon & M & \longrightarrow & M^{**}, \\ & m & \longrightarrow & \eta(m)\colon M^* \to R,\ f \mapsto f(m), \end{array}$$

which is clearly a canonical morphism of R-modules. Let us prove that it is bijective. Since M is finite, it admits a projective coordinate system $\{h_i, f_i\}_{i=1}^n$. Let us consider the map

$$\begin{array}{rccl} \mu\colon & M^{**} & \longrightarrow & M, \\ & \varphi & \longmapsto & \sum_{i=1}^n \varphi(f_i) m_i. \end{array}$$

This is clearly R-linear. Now, for every $\varphi \in M^{**}$ and $f \in M^*$,

$$\eta \circ \mu(\varphi)(f) = f(\mu(\varphi)) = f\Big(\sum_{i=1}^n \varphi(f_i) m_i\Big) = \varphi\Big(\sum_{i=1}^n f(m_i) f_i\Big) = \varphi(f),$$

the last equality due to Remark 1.2.26. On the other hand, given $m \in M$ and $f \in M^*$,

$$\mu \circ \eta(m) = \sum_{i=1}^n \eta(m)(f_i) m_i = \sum_{i=1}^n f_i(m) m_i = m.$$

□

Remark 1.2.28. The isomorphism η being canonical means that its definition does not depend on any choice; we can say that it is written the same for any finite R-module M. In particular, if M is free of finite rank, the definition of η does not depend on the choice of bases. In this case, we have that M is isomorphic as an R-module with M^*, because they have the same rank. However, this isomorphism is not canonical, in the sense that it depends on the choice of bases: if we change bases, the definition of the isomorphism also changes.

After Proposition 1.2.27, we often identify $H = H^{**}$ by identifying any element $h \in H$ with its image $\eta(h) \in H^{**}$.

Corollary 1.2.29. *Let M be a finite R-module. If $\{h_i, f_i\}_{i=1}^n$ is a projective coordinate system for M, then $\{f_i, h_i\}_{i=1}^n$ is a projective coordinate system for M^*.*

When we take $m \in M$ and $f \in M^*$, $f(m)$ stands for the map f evaluated at the element m. But identifying m with its image in M^{**}, $f(m)$ coincides with $m(f)$, which means the map $m\colon M^* \longrightarrow M^*$ evaluated at the element $f \in M^*$. In the contexts where both expressions arise, we will unify these two points of view by using the map

$$\langle \cdot, \cdot \rangle\colon M^* \otimes M \longrightarrow R, \quad \langle f, h \rangle = f(h).$$

Under this convention,

$$m = \sum_{i=1}^n \langle f_i, m \rangle m_i, \quad m \in M,$$

$$f = \sum_{i=1}^{n} \langle f, m_i \rangle f_i, \quad f \in M^*.$$

Let us study how the duality functor behaves with respect to the tensor product. Namely, for two R-modules M and N, we are interested in the relation between $M^* \otimes N^*$ and $(M \otimes N)^*$. There is an important remark: if $f \in M^*$ and $g \in N^*$, $f \otimes g$ can stand for the tensor product of f and g, which is an element of $M^* \otimes N^*$, or the R-linear map $M \otimes N \longrightarrow R$ defined by $m \otimes n \mapsto f(m)g(n)$, which is an element of $(M \otimes N)^*$. However, both objects can be identified, as by the universal property of the tensor product, given f and g there is a unique R-linear map as above (see [Und15, Proposition 1.1.7]). Actually, we have been using implicitly this fact each time we considered a tensor product of R-linear maps. Now, let $\Phi \colon M^* \otimes N^* \longrightarrow (M \otimes N)^*$ be the map defined by $\Phi(f \otimes g)(m \otimes n) = f(m)g(n)$ (and extended by R-linearity), i.e, it carries the first interpretation of $f \otimes g$ to the second one.

Proposition 1.2.30. *Let M and N be R-modules. Let $\Phi \colon M^* \otimes N^* \longrightarrow (M \otimes N)^*$ defined by*

$$\Phi(f \otimes g)(m \otimes n) = f(m)g(n), \quad f \in M^*, g \in N^*, m \in M, n \in N$$

and extended by R-linearity.

1. *If R has no zero divisors, Φ is injective.*

2. *If either M or N is finite as an R-module, then Φ is bijective.*

Proof.

1. Let $f \otimes g \in \mathrm{Ker}(\Phi)$, so $f(m)g(n) = 0$ for all $m \in M$ and all $n \in N$. If $f = 0$, we have finished. Otherwise, if $f \neq 0$, there is some $m \in M$ such that $f(m) \neq 0$. Since R has no zero divisors, $g(n) = 0$ for all $n \in N$, so $g = 0$. Then $f = 0$ or $g = 0$, proving that $f \otimes g = 0$.

2. Suppose that M is finite as an R-module and pick a projective coordinate system $\{m_i, f_i\}_{i=1}^n$ for M. Let $\Psi \colon (M \otimes N)^* \longrightarrow M^* \otimes N^*$ be the map defined by $\Psi(\varphi) = \sum_{i=1}^n f_i \otimes \varphi(m_i \otimes -)$. It is straightforward to check the R-linearity of Ψ. We prove that it is the inverse of Φ, from which it will follow the statement. Given $f \in M^*$ and $g \in N^*$,

$$\begin{aligned} \Psi \circ \Phi(f \otimes g) &= \sum_{i=1}^{n} f_i \otimes \Phi(f \otimes g)(m_i \otimes -) \\ &= \sum_{i=1}^{n} f_i \otimes \langle f, m_i \rangle g \\ &= \sum_{i=1}^{n} \langle f, m_i \rangle f_i \otimes g \\ &= f \otimes g, \end{aligned}$$

where the last equality follows from Remark 1.2.26. Conversely, given $\varphi \in$

$(M \otimes N)^*$, $m \in M$ and $n \in N$,

$$\begin{aligned}\Phi \circ \Psi(\varphi)(m \otimes n) &= \sum_{i=1}^{n} \langle f_i, m \rangle \varphi(m_i \otimes n) \\ &= \varphi\Big(\sum_{i=1}^{n} \langle f_i, m \rangle m_i \otimes n \Big) \\ &= \varphi(m \otimes n).\end{aligned}$$

Since m and n are arbitrary, it follows that $\Phi \circ \Psi(\varphi) = \varphi$.

□

In particular, Φ is bijective when R is a field and M, N are finite-dimensional R-vector spaces.

2.7.2 Duals of Hopf algebras

Let us apply the notions related with duality to the context of Hopf algebras.

Looking at Definition 1.2.1, one can regard the notions of algebra and coalgebra as duals: the diagram at 2a for the associative property is obtained from reversing arrows at the diagram 3a for the coassociative property. The same phenomenon can be observed with the diagrams 2b and 3b for the unit and counit properties respectively. This intuition is materialized in the result that the dual of an R-coalgebra is an R-algebra.

Proposition 1.2.31 ([Und15], Proposition 1.3.1)**.** *If C is an R-coalgebra, then C^* is an R-algebra with multiplication map $m_{C^*} : C^* \otimes C^* \longrightarrow C^*$ defined by*

$$m_{C^*}(f \otimes g) := (f \otimes g) \circ \Delta_C, \quad f, g \in C^*$$

and unit map $u_{C^*} : R \longrightarrow C^*$ given by

$$u_{C^*}(r)(c) = r\varepsilon_C(c), \quad r \in R,\ c \in C$$

Proof. Let us prove that m_{C^*} satisfies the associative property. For $f, g, h \in C^*$ and $c \in C$, we have:

$$\begin{aligned}m_{C^*} \circ (\mathrm{Id}_{C^*} \otimes m_{C^*})(f \otimes g \otimes h)(c) &= m_{C^*}(f \otimes \Delta_{C^*}(g \otimes h))(c) \\ &= (f \otimes \Delta_{C^*}(g \otimes h)) \circ \Delta_C(c) \\ &= \sum_{(c)} f(c_{(1)}) \otimes \Delta_{C^*}(g \otimes h))(c_{(2)}) \\ &= \sum_{(c)} f(c_{(1)}) \otimes ((g \otimes h) \circ \Delta_C(c_{(2)})) \\ &= \sum_{(c)} f(c_{(1)}) \otimes g(c_{(2)}) \otimes h(c_{(3)}).\end{aligned}$$

Likewise,

$$\begin{aligned} m_{C^*} \circ (m_{C^*} \otimes \mathrm{Id}_{C^*})(f \otimes g \otimes h)(c) &= m_{C^*}(\Delta_{C^*}(f \otimes g) \otimes h)(c) \\ &= (\Delta_{C^*}(f \otimes g) \otimes h) \circ \Delta_C(c) \\ &= \sum_{(c)} \Delta_{C^*}(f \otimes g))(c_{(1)}) \otimes h(c_{(2)}) \\ &= \sum_{(c)} ((f \otimes g) \circ \Delta_C(c_{(1)})) \otimes h(c_{(2)}) \\ &= \sum_{(c)} f(c_{(1)}) \otimes g(c_{(2)}) \otimes h(c_{(3)}). \end{aligned}$$

Since we have arrived in the same expression, the first members at each chain of equalities coincide, which proves that the associative property holds.

As for the unit property, given $r \in R$, $f \in C^*$ and $c \in C$, we have

$$\begin{aligned} m_{C^*} \circ (\mathrm{Id}_{C^*} \otimes u_{C^*})(f \otimes r)(c) &= m_{C^*}(f \otimes u_{C^*}(r))(c) \\ &= (f \otimes u_{C^*}(r)) \circ \Delta_C(c) \\ &= \sum_{(c)} f(c_{(1)}) r \varepsilon_C(c_{(2)}) \\ &= r \sum_{(c)} f(c_{(1)}) \varepsilon_C(c_{(2)}) \\ &= r \sum_{(c)} f(\varepsilon_C(c_{(2)}) c_{(1)}) \\ &= rf\Big(\sum_{(c)} \varepsilon_C(c_{(2)}) c_{(1)} \Big) \\ &= rf(c). \end{aligned}$$

In the same way, we prove that $m_{C^*} \circ (u_{C^*} \otimes \mathrm{Id}_{C^*})(r \otimes f)(c) = rf(c)$ for every $r \in R$, $f \in C^*$ and $c \in C$. Hence the unit property is satisfied. This finishes the proof. □

Remark 1.2.32. If we appy the duality functor at the counit map ε_C we obtain the unit map u_{C^*} at Proposition 1.2.31. Indeed, $\varepsilon_C^*\colon R^* \longrightarrow C^*$ is defined by $\varepsilon_C^*(f)(c) = f \circ \varepsilon_C(c)$. Note that $R^* = \mathrm{End}_R(R)$, whose only elements $f \in R^*$ are homotheties with factor $f(1_R)$, and then R^* identifies trivially with R by $f \mapsto f(1)$. Then $\varepsilon_C^*\colon R \longrightarrow C^*$ is defined by $\varepsilon_C^*(r)(c) = r\varepsilon_C(c) = u_{C^*}(r)(c)$. Sine r and c are arbitrary, $\varepsilon_C^* = u_{C^*}$.

As for the relation between m_{C^*} and the dual Δ_C^* of the comultiplication map Δ_C, the matter is more subtle, as the map $C^* \otimes C^* \longrightarrow (C \otimes C)^*$ need not be injective (even though Proposition 1.2.31 is still valid in that case). However, following Proposition 1.2.30, there is injectivity when R has no zero divisors or C is finite as an R-module.In that case, applying the duality functor to the comultiplication $\Delta_C\colon C \longrightarrow C \otimes C$ yields the map

$$\Delta_C^*\colon (C \otimes C)^* \longrightarrow C^*$$

defined as $\Delta_C^*(\varphi) = \varphi \circ \Delta_C$, and we can consider the restriction $\Delta_C^* \,|_{C^* \otimes C^*}$, which is just the multiplication map m_{C^*}.

Remark 1.2.33. Let C be an R-coalgebra and consider the R-algebra structure on C^* from Proposition 1.2.31. Then, the identity element for the multiplication on C^* is the counit map ε_C of C. Indeed, given $f \in C^*$ and $c \in C$, we have

$$\begin{aligned} m_{C^*}(f \otimes \varepsilon_C)(c) &= (f \otimes \varepsilon_C)\Delta_C(c) \\ &= \sum_{(c)} \varepsilon_C(c_{(2)}) f(c_{(1)}) \\ &= f\Big(\sum_{(c)} \varepsilon_C(c_{(2)}) c_{(1)}\Big) \\ &= f(c), \end{aligned}$$

so $m_{C^*}(f \otimes \varepsilon_C) = f$. Similarly, one proves that $m_{C^*}(\varepsilon_C \otimes f) = f$.

After Proposition 1.2.31, one may expect that if A is an R-algebra, then A^* is an R-coalgebra. However, this is not always the case (see [Und15, Example 1.3.2] for a counterexample). Instead, we will that it holds when A is finite as an R-module (if R is a field, this is just assuming that A is of finite dimension).

Let us think on what happens when one applies the duality functor to the multiplication map $m_A \colon A \otimes A \longrightarrow A$. We obtain a map $m_A^* \colon A^* \longrightarrow (A \otimes A)^*$. Again by Proposition 1.2.30, we have that $(A \otimes A)^* \cong A^* \otimes A^*$ because A is finite, and identifying both, we obtain a map $m_A^* \colon A^* \longrightarrow A^* \otimes A^*$. For $f \in A^*$, we can consider $m_A^*(f)$ as an element of $(A \otimes A)^*$, and then, for $a, b \in A$, $m_A^*(f)(a \otimes b) = f(m_A(a \otimes b))$. Therefore, thanks to the hypothesis that A is finite as an R-module, the image of m_A^* lies in $A^* \otimes A^*$.

On the other hand, if one dualizes the unit map $u_A \colon R \longrightarrow A$, we obtain a map $u_A^* \colon A^* \longrightarrow R^*$ defined by $u_{A^*}(f)(r) = f(u_A(r))$. Identifying $R^* = R$, we obtain that $u_A^* \colon A^* \longrightarrow R$ is defined by $u_{A^*}(f) = f(1_A)$.

In the following we shall see that the maps m_A^* and u_A^* serve as comultiplication and counit maps for A^*, respectively.

Proposition 1.2.34 ([Und15], Proposition 1.3.9)**.** *If A is an R-algebra that is finite as an R-module, then A^* is an R-coalgebra with comultiplication map $\Delta_{A^*} \colon A^* \longrightarrow A^* \otimes A^*$ defined as*

$$\Delta_{A^*}(f)(a \otimes b) = f \circ m_A(a \otimes b), \quad a, b \in A,$$

and counit map $\varepsilon_{A^*} \colon A^* \longrightarrow R$ given by

$$\varepsilon_{A^*}(f) = f(1_A).$$

Proof. Let us check the coassociative property. For $f \in A^*$ and $a, b, c \in A$, we claim that

$$(\mathrm{Id}_{A^*} \otimes \Delta_{A^*}) \circ \Delta_{A^*}(f) = \Delta_{A^*}(f) \circ (\mathrm{Id}_A \otimes m_A).$$

Indeed, let us write

$$\Delta_{A^*}(f) = \sum_{i=1}^{s} \alpha_i \otimes \beta_i, \quad \alpha_i, \beta_i \in A^*$$

(note that we are not allowed to use Sweedler's notation as long as we do not know that Δ_{A^*} is a comultiplication). Then, given $a, b, c \in A$

$$\begin{aligned}(\mathrm{Id}_{A^*} \otimes \Delta_{A^*}) \circ \Delta_{A^*}(f)(a \otimes b \otimes c) &= \sum_{i=1}^{s} \alpha_i \otimes \Delta_{A^*}(\beta_i)(a \otimes b \otimes c) \\ &= \sum_{i=1}^{s} \langle \alpha_i, a \rangle \beta_i \circ m_A(b \otimes c) \\ &= \sum_{i=1}^{s} (\alpha_i \otimes \beta_i)(\mathrm{Id}_A \otimes m_A)(a \otimes b \otimes c) \\ &= \Delta_{A^*}(f) \circ (\mathrm{Id}_A \otimes m_A)(a \otimes b \otimes c),\end{aligned}$$

as claimed. Hence

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

Likewise, it is proved that

$$(\Delta_{A^*} \otimes \mathrm{Id}_{A^*}) \circ \Delta_{A^*}(f)(a \otimes b \otimes c) = (ab)c.$$

Since A is an R-algebra, the associative property gives that $(ab)c = a(bc)$, implying coassociativity.

Finally, we check the counit property. Given $f \in A^*$, $r \in R$ and $a \in A$, we have

$$\begin{aligned}(\varepsilon_{A^*} \otimes \mathrm{Id}_{A^*}) \circ \Delta_{A^*}(f)(r \otimes a) &= \Delta_{A^*}(u_A \otimes \mathrm{Id}_A)(r \otimes a) \\ &= f \circ m_A(u_A \otimes \mathrm{Id}_A)(r \otimes a) \\ &= f(m_A(r1_A \otimes a) \\ &= f(ra) \\ &= rf(a) \\ &= (1 \otimes f)(r \otimes a),\end{aligned}$$

so $(\varepsilon_{A^*} \otimes \mathrm{Id}_{A^*})(f) = 1 \otimes f$, and similarly, $(\mathrm{Id}_{A^*} \otimes \varepsilon_{A^*})(f) = f \otimes 1$. □

In the end, we see that the category of R-Hopf algebras is invariant under the duality functor.

Proposition 1.2.35. *Let H be a finite R-Hopf algebra. Then H^* is an R-Hopf algebra.*

Proof. We follow the proof at [Und15, Proposition 3.1.12].

By Proposition 1.2.31, H^* is an R-algebra with multiplication $m_{H^*} := \Delta_H^* \,|_{H^* \otimes H^*}$ and unit $u_{H^*} := \varepsilon_H^*$. On the other hand, since H is finite as an R-module, Proposition 1.2.34 gives that H^* is an R-coalgebra with comultiplication $\Delta_{H^*}(f) = f \circ m_H$ and counit $\varepsilon_{H^*}(f) = f(1_H)$. Now, it is straightforward to check that Δ_{H^*} and ε_{H^*} are ring homomorphisms, proving that H^* is an R-bialgebra. Let us consider the

dual $S_H^*\colon H^* \longrightarrow H^*$ of the antipode $S_H\colon H \longrightarrow H$. Given $f \in H^*$ and $a \in H$, we have

$$\begin{aligned}(m_{H^*} \circ (\mathrm{Id}_{H^*} \otimes S_H^*) \circ \Delta_{H^*}(f))(a) &= (\mathrm{Id}_{H^*} \otimes S_H^*)(\Delta_{H^*}(f)(\Delta_H(a))) \\ &= \Delta_{H^*}(f)((\mathrm{Id}_H \otimes S_H) \circ \Delta_H(a)) \\ &= f(m_H \circ (\mathrm{Id}_H \otimes S_H) \circ \Delta_H(a)) \\ &= f(\varepsilon_H(a)1_H) \\ &= \varepsilon_H(a)f(1_H) \\ &= \varepsilon_{H^*}(f)\varepsilon_H(a) \\ &= \varepsilon_{H^*}(f)1_{H^*}(a).\end{aligned}$$

Likewise,

$$(m_{H^*} \circ (S_H^* \otimes \mathrm{Id}_{H^*}) \circ \Delta_{H^*}(f))(a) = \varepsilon_{H^*}(f)1_{H^*}(a).$$

Then $S_{H^*} := S_H^*$ works as an antipode and H^* is an R-Hopf algebra. □

Proposition 1.2.36. *Let H be an R-Hopf algebra which is finite as an R-module. Then H^{**} is an R-Hopf algebra and $H \cong H^{**}$ as R-Hopf algebras.*

Proof. That H^{**} is an R-Hopf algebra follows directly from Proposition 1.2.35. On the other hand, from the proof of Proposition 1.2.27, we know that there is an isomorphism $\eta\colon H \longrightarrow H^{**}$ of R-modules defined by $\eta(h)(f) = f(h)$. It is enough to check that this is an isomorphism of R-Hopf algebras.

- Given $h, h' \in H$ and $f \in H^*$,

$$\begin{aligned}(m_{H^{**}}(\eta \otimes \eta)(h \otimes h'))(f) &= (\eta(h) \otimes \eta(h'))\Delta_{H^*}(f) \\ &= (\eta(h) \otimes \eta(h'))\Big(\sum_{(f)} f_{(1)} \otimes f_{(2)}\Big) \\ &= \sum_{(f)} \eta(h)(f_{(1)})\eta(h')(f_{(2)}) \\ &= \sum_{(f)} f_{(1)}(h)f_{(2)}(h') \\ &= \sum_{(f)} f_{(1)} \otimes f_{(2)}(h \otimes h') \\ &= \Delta_{H^*}(f)(h \otimes h') \\ &= f \circ m_H(h \otimes h') \\ &= f(m_H(h \otimes h')) \\ &= \eta(m_H(h \otimes h'))(f).\end{aligned}$$

  Then $m_{H^{**}} \circ (\eta \otimes \eta)(h \otimes h') = \eta \circ m_H(h \otimes h')$ for every $h \otimes h'$, whence $m_{H^{**}} \circ (\eta \otimes \eta) = \eta \circ m_H$.

- Given $r \in R$ and $f \in H^*$,

$$\begin{aligned}\eta \circ u_H(r)(f) &= r\eta(1_H)(f) \\ &= rf(1_H) \\ &= r\varepsilon_{H^*}(f) \\ &= u_{H^{**}}(r)(f).\end{aligned}$$

  Then $\eta \circ u_H = u_{H^{**}}$.

- Note that since $H^{**} \subset (H^* \otimes H^*)^*$, elements of H^{**} can be seen as R-linear maps $H^* \otimes H^* \longrightarrow R$. Now, given $h \in H$ and $f, g \in H^*$,

$$\begin{aligned}(\Delta_{H^{**}} \circ \eta(h))(f \otimes g) &= \eta(h) \circ m_{H^*}(f \otimes g) \\ &= \eta(h)((f \otimes g) \circ \Delta_H) \\ &= (f \otimes g)\Delta_H(h) \\ &= \sum_{(h)} f(h_{(1)}) \otimes g(h_{(2)}) \\ &= \sum_{(h)} \eta(h_{(1)})(f) \otimes \eta(h_{(2)})(g) \\ &= (\eta \otimes \eta)\Delta_H(h)(f \otimes g).\end{aligned}$$

  It follows that $\Delta_{H^{**}} \circ \eta = (\eta \otimes \eta)\Delta_H$.

- Given $h \in H$,

$$\varepsilon_{H^{**}} \circ \eta(h) = \eta(h)(1_{H^*}) = 1_{H^*}(h) = \varepsilon_H(h).$$

  Then, $\varepsilon_{H^{**}} \circ \eta = \varepsilon_H$.

- Given $h \in H$ and $f \in H^*$,

$$S_{H^{**}} \circ \eta(h) = \eta(h) \circ S_{H^*}(f) = S_{H^*}(f)(h) = f \circ S_H(h) = \eta \circ S_H(h)(f).$$

  Then $S_{H^{**}} \circ \eta = S_H$.

□

Corollary 1.2.37. *Let H be a finite R-module. Then H is an R-Hopf algebra if and only if so is H^*.*

Proof. The left-to-right implication is Proposition 1.2.35. Conversely, assume that H^* is an R-Hopf algebra. Again by Proposition 1.2.35, we have that H^{**} is an R-Hopf algebra. Now, we induce on H an R-Hopf algebra structure by means of the isomorphism of R-modules $\eta\colon H \longrightarrow H^{**}$. Namely, we define on H the following operations:

- Multiplication map: $m_H := \eta^{-1} \circ m_{H^{**}} \circ (\eta \otimes \eta)$.
- Unit map: $u_H := \eta^{-1} \circ \eta_{H^{**}}$.
- Comultiplication map: $\Delta_H := (\eta^{-1} \otimes \eta^{-1}) \circ \Delta_{H^{**}} \circ \eta$.
- Counit map: $\varepsilon_H := \varepsilon_{H^{**}} \circ \eta$.
- Coinverse map: $S_H := \eta^{-1} \circ S_{H^{**}} \circ \eta$.

Since the previous definitions are equivalent to the axioms for a Hopf algebra homomorphism (see Definition 1.2.9), it is automatic that H is an R-Hopf algebra with these operations. But by Proposition 1.2.36, this Hopf algebra structure on H is the one such that its bidual is the one at H^{**}, and hence its dual is the one at H^*. □

2.8 Modules and comodules

Let us fix an R-Hopf algebra H. Suppose that we have an R-module A which in addition is an H-module. This means that we have an external product of H on A, or equivalently, an action $H \times A \longrightarrow A$, that preserves the additive structure of S. If in addition we want H to act R-linearly on A, that is, the action is preserved by external multiplication by R, we should impose that the map above is R-bilinear. Equivalently, we can think of it as an R-linear map $H \otimes A \longrightarrow A$, which will be our usual way to consider R-linear actions.

We need to consider R-linear actions of R-Hopf algebras that are in addition well behaved with respect to the Hopf algebra operations. This leads to the notion of left H-module.

Definition 1.2.38. *Let A be an R-module and let H be an R-Hopf algebra. We say that A is a **left H-module** if there is an R-linear map $\alpha\colon H \otimes A \longrightarrow A$ such that:*

1. **(Associative property)** $\alpha \circ (\mathrm{Id}_H \otimes \alpha) = \alpha \circ (m_H \otimes \mathrm{Id}_A)$, *that is, the following diagram is commutative:*

$$\begin{array}{ccc} H \otimes H \otimes A & \xrightarrow{m_H \otimes \mathrm{Id}_A} & H \otimes A \\ \downarrow{\scriptstyle \mathrm{Id}_H \otimes \alpha} & & \downarrow{\scriptstyle \alpha} \\ H \otimes A & \xrightarrow{\alpha} & H \end{array}$$

2. **(Unit property)** $\alpha \circ (u_H \otimes \mathrm{Id}_A)(r \otimes a) = ra$ *for every $r \in R$ and $a \in A$, that is, the following diagram is commutative:*

$$\begin{array}{ccc} R \otimes A & & \\ \downarrow{\scriptstyle u_H \otimes \mathrm{Id}_A} & \searrow^{\mathfrak{s}} & \\ H \otimes A & \xrightarrow{\alpha} & A \end{array}$$

where $\mathfrak{s}\colon R \otimes A \longrightarrow A$ is the R-linear action of R on A induced by u_A.

We will also say that A is a left H-module via α.

Remark 1.2.39. The notion of left H-module at Definition 1.2.38 is **not** the usual notion of left module over a ring, that is, an abelian group receiving the external product of a ring of scalars that preserves addition. The mere existence of an R-linear map $\alpha\colon H \otimes A \longrightarrow A$ yields that A is a left module over the underlying ring structure of H in that sense. Instead, our ground ring is required to be an R-Hopf algebra and we impose that the associative and unit properties at Definition 1.2.38 are satisfied. In fact, there is no need of the coalgebra structure and the antipode, so we can actually define the notion of left S-module, for an R-algebra S, in the same way.

If A is a left H-module, we usually refer to $\alpha\colon H\otimes A\longrightarrow A$ as an R-linear action or module map. We may use the label α_A for the action of A when other left H-modules are present in the context. Given $h\in H$ and $a\in A$, we will usually denote $h\cdot a := \alpha(h\otimes a)$. Under this notation, the associative property means that

$$(hh')\cdot a = h\cdot(h'\cdot a),\quad h,h'\in H,\, a\in A,$$

while the unit property translates into

$$(r1_H)\cdot a = ra,\quad r\in R,\, a\in A.$$

Example 1.2.40.

1. The ground ring R has itself left H-module structure by means of
$$h\cdot r = \varepsilon_H(h)r,\quad h\in H, r\in R.$$
2. Let A be a left H-module. Then, $A\otimes A$ is also a left H-module with respect to
$$h\cdot(a\otimes b) := \sum_{(h)}(h_{(1)}\cdot a)\otimes(h_{(2)}\cdot b),\quad h\in H,\, a,b\in A.$$
3. An R-Hopf algebra H is a left H-module with the multiplication m_H as R-linear action.

Definition 1.2.41. *Let H be an R-Hopf algebra and let A and A' be left H-modules. We say that an R-module homomorphism $f\colon A\longrightarrow A'$ is a left H-module homomorphism if $f\circ\alpha_A = \alpha_{A'}\circ(\mathrm{Id}_H\otimes f)$, that is, the following diagram commutes:*

$$\begin{array}{ccc} A & \xrightarrow{\quad f\quad} & A' \\ {\scriptstyle\alpha_A}\uparrow & & \uparrow{\scriptstyle\alpha_{A'}} \\ H\otimes A & \xrightarrow{\mathrm{Id}_H\otimes f} & H\otimes A' \end{array}$$

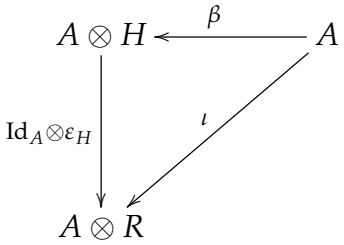
While in the notion of left H-module we have an action consisting on an R-linear map $\alpha\colon H\otimes A\longrightarrow A$ compatible with the Hopf algebra operations, we can dualize this notion to the one of right H-comodule.

Definition 1.2.42. *Let A be an R-module. We say that A is a **right H-comodule** if there is an R-module homomorphism $\beta\colon A\longrightarrow A\otimes H$ such that:*

1. **(Coassociative property)** $(\beta\otimes\mathrm{Id}_H)\circ\beta = (\mathrm{Id}_A\otimes\Delta_H)\circ\beta$, *that is, the following diagram is commutative:*

$$\begin{array}{ccc} A\otimes H\otimes H & \xleftarrow{\beta\otimes\mathrm{Id}_H} & A\otimes H \\ \uparrow{\scriptstyle\mathrm{Id}_A\otimes\Delta_H} & & \uparrow{\scriptstyle\beta} \\ A\otimes H & \xleftarrow{\quad\beta\quad} & A \end{array}$$

2. **(Counit property)** $(\mathrm{Id}_A \otimes \varepsilon_H) \circ \beta$ *is the trivial* R*-linear map* $\iota\colon A \longrightarrow A \otimes R$*, that is, the following diagram is commutative:*



We will also say that A *is a right* H*-comodule via* β*.*

Remark 1.2.43. As in the case of left H-modules, for the notion of right H-comodule, the requirement of H to be an R-Hopf algebra is not needed, so that right C-comodules are defined in the same way for an R-coalgebra C.

We will usually call the map $\beta\colon A \longrightarrow A \otimes H$ an R-linear coaction or comodule map. We have also a Sweedler notation for this map. Namely, if $a \in A$, we will write

$$\beta(a) = \sum_{(a)} a_{(0)} \otimes a_{(1)}, \quad a_{(0)} \in A,\, a_{(1)} \in H. \tag{1.4}$$

Again, when we are working also with other right H-comodules, we may denote β_A for the comodule map of A.

Example 1.2.44. *1. The ring* R *can be seen as a right* H*-comodule with coaction*

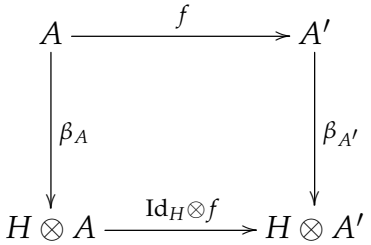
$$\beta_R(r) = r \otimes u_H(1_R), \quad r \in R.$$

2. *If* A *is a right* H*-comodule, then so is* $A \otimes A$ *with coaction*

$$\beta_{A\otimes A}(a \otimes b) = \sum_{(a),(b)} a_{(0)} \otimes b_{(0)} \otimes m_H(a_{(1)} \otimes b_{(1)}), \quad a, b \in A.$$

3. *An* R*-Hopf algebra* H *is a right* H*-comodule with the comultiplication* Δ_H *as coaction.*

Definition 1.2.45. *Let* A *and* A' *be right* H*-comodules. We say that an* R*-linear map* $f\colon A \longrightarrow A'$ *is a right* H*-comodule homomorphism if* $\beta_{A'} \circ f = (f \otimes \mathrm{Id}_H) \circ \beta_A$*, that is, the following diagram commutes:*



Now, suppose that the R-Hopf algebra H is finite. Recall that the dual H^* is also an R-Hopf algebra which is finite as an R-module (in short, we will refer to H as a finite R-Hopf algebra). If we fix a projective coordinate system for H, we can induce a right H^*-comodule structure from a left H-module structure and viceversa, and both operations are inverse to each other.

Proposition 1.2.46. *Let H be a finite R-Hopf algebra and let $\{h_i, f_i\}_{i=1}^n$ be a projective coordinate system for H.*

1. *If A is a right H-comodule, then it is a left H^*-module with action $H^* \otimes A \longrightarrow A$ defined by*
$$f \cdot a := \sum_{(a)} a_{(0)} \langle f, a_{(1)} \rangle, \quad f \in H^*, a \in A.$$

2. *If A is a left H-module, then it is a right H^*-comodule with coaction given by the map*
$$\begin{array}{rccc} \beta\colon & A & \longrightarrow & A \otimes H^*, \\ & a & \longmapsto & \sum_{i=1}^n (h_i \cdot a) \otimes f_i. \end{array}$$

Proof. 1. We prove the validity of the conditions 1 and 2 at Definition 1.2.38.

We first check 1. The coassociative property for β means that

$$\sum_{(a)} \beta(a_{(0)}) \otimes a_{(1)} = \sum_{(a)} a_{(0)} \otimes \Delta_H(a_{(1)}), \quad a_{(0)} \in A, a_{(1)} \in H.$$

Writing down the Sweedler notation for $\beta(a_{(0)})$, we have

$$\sum_{(a)} a_{(0)} \otimes a_{(1)} \otimes a_{(2)} = \sum_{(a)} a_{(0)} \otimes \Delta_H(a_{(1)}).$$

Given $f, f' \in H^*$ and $a \in A$, we obtain

$$\begin{aligned} (ff') \cdot a &= \sum_{(a)} a_{(0)} \langle ff', a_{(1)} \rangle \\ &= \sum_{(a)} a_{(0)} m_{H^*}(f \otimes f')(a_{(1)}) \\ &= \sum_{(a)} a_{(0)} (f \otimes f') \circ \Delta_H(a_{(1)}) \\ &= \sum_{(a)} a_{(0)} \langle f, a_{(1)} \rangle \langle f', a_{(2)} \rangle \\ &= f \cdot \Big(\sum_{(a)} a_{(0)} \langle f', a_{(1)} \rangle \Big) \\ &= f \cdot (f' \cdot a), \end{aligned}$$

as we wanted.

Next, we check 2. For $r \in R$ and $a \in A$, we have

$$(r1_{H^*}) \cdot a = \sum_{(a)} a_{(0)} \langle r1_{H^*}, a_{(1)} \rangle = r \sum_{(a)} a_{(0)} \varepsilon_H(a_{(1)}) = a.$$

2. We shall check that the conditions 1 and 2 at Definition 1.2.42 are satisfied.

Given $a \in A$, we have that

$$(\beta \otimes \mathrm{Id}_{H^*}) \circ \beta(a) = (\beta \otimes 1) \left(\sum_{i=1}^n (h_i \cdot a) \otimes f_i \right) = \sum_{i,j=1}^n (h_j \cdot (h_i \cdot a)) \otimes f_j \otimes f_i,$$

$$(\mathrm{Id}_A \otimes \Delta_{H^*}) \circ \beta(a) = (1 \otimes \Delta_{H^*}) \left(\sum_{i=1}^{n} (h_i \cdot a) \otimes f_i \right) = \sum_{i=1}^{n} (h_i \cdot a) \otimes \left(\sum_{(f_i)} f_{i(1)} \otimes f_{i(2)} \right).$$

Next, we evaluate at an element $h \otimes h' \in H \otimes H$, obtaining that

$$\begin{aligned}
(\beta \otimes \mathrm{Id}_{H^*}) \circ \beta(a)(h \otimes h') &= \sum_{i,j=1}^{n} (h_j \cdot (h_i \cdot a)) \langle f_j \otimes f_i, h \otimes h' \rangle \\
&= \sum_{i,j=1}^{n} (h_j \cdot (h_i \cdot a)) \langle f_j, h \rangle \langle f_i, h' \rangle \\
&= \sum_{j=1}^{n} \langle f_j, h' \rangle h_j \cdot \left(\sum_{i=1}^{n} \langle f_i, h' \rangle (h_i \cdot a) \right) \\
&= h \cdot (h' \cdot a),
\end{aligned}$$

$$\begin{aligned}
(\mathrm{Id}_A \otimes \Delta_{H^*}) \circ \beta(a)(h \otimes h') &= \sum_{i=1}^{n} (h_i \cdot a) \left(\sum_{(f_i)} \langle f_{i(1)} \otimes f_{i(2)}, h \otimes h' \rangle \right) \\
&= \sum_{i=1}^{n} (h_i \cdot a) \left(\sum_{(f_i)} \langle f_{i(1)}, h \rangle \langle f_{i(2)}, h' \rangle \right) \\
&= \sum_{i=1}^{n} (h_i \cdot a) \, \Delta_{H^*}(f_i)(h \otimes h') \\
&= \sum_{i=1}^{n} (h_i \cdot a) \langle f_i, h\, h' \rangle \\
&= (h\, h') \cdot a.
\end{aligned}$$

Since A is a left H-module, we have that $h \cdot (h' \cdot a) = (h\, h') \cdot a$, so we conclude that $(\beta \otimes \mathrm{Id}_{H^*}) \circ \beta = (\mathrm{Id}_A \otimes \Delta_{H^*}) \circ \beta$.

Finally, for $a \in A$ we have

$$\begin{aligned}
(\mathrm{Id}_A \otimes \varepsilon_{H^*}) \circ \beta(a) &= \sum_{i=1}^{n} h_i \cdot a \otimes \varepsilon_{H^*}(f_i) \\
&= \sum_{i=1}^{n} h_i \cdot a \otimes f_i(1_H) \\
&= \Big(\sum_{i=1}^{n} f_i(1_H) h_i \Big) \cdot a \otimes 1_R \\
&= (1_H \cdot a) \otimes 1_R \\
&= a \otimes 1_R
\end{aligned} \tag{1.5}$$

□

We check that the notions left H-module and right H-comodule are dual to each other, in the sense that left H-module is equivalent to right H^*-comodule.

Proposition 1.2.47. *Let H be a finite R-Hopf algebra and let A be an R-module. Then, A is a left H-module if and only if it is a right H^*-comodule. Furthermore, if it is the case, the H-module and H^*-comodule structures on A are induced as in Proposition 1.2.46 by each other.*

Proof. The equivalence has been proved already. Let us consider the left H-module structure $H \otimes A \longrightarrow A$ on A. Then, the induced right H^*-comodule structure is given by

$$\beta(a) = \sum_{i=1}^{n} (h_i \cdot a) \otimes f_i, \quad a \in A.$$

This coaction induces a left H-module structure given by

$$h(a) = \sum_{(a)} a_{(0)} \langle h, a_{(1)} \rangle.$$

By the definition of β,

$$h(a) = \sum_{i=1}^{n} (h_i \cdot a) \langle h, f_i \rangle = \left(\sum_{i=1}^{n} \langle f_i, h \rangle \, h_i \right) \cdot a = h \cdot a$$

for every $a \in A$, so we recover the original left H-module structure on A.

Now, we consider the right H^*-comodule structure $\beta \colon A \longrightarrow A \otimes H^*$ on A. The induced left H-module structure is given by

$$h(a) = \sum_{(a)} a_{(0)} \langle h, a_{(1)} \rangle.$$

This action induces a right H^*-comodule structure given by

$$\begin{aligned} \beta'(a) &= \sum_{i=1}^{n} h_i(a) \otimes f_i \\ &= \sum_{i=1}^{n} \left(\sum_{(a)} a_{(0)} \langle h_i, a_{(1)} \rangle \right) \otimes f_i \\ &= \sum_{(a)} a_{(0)} \left(\sum_{i=1}^{n} \langle a_{(1)}, h_i \rangle \otimes f_i \right) \\ &= \sum_{(a)} a_{(0)} \otimes a_{(1)} \\ &= \beta(a), \end{aligned}$$

which is just the original right H^*-comodule structure. □

2.9 Module and comodule algebras

In Section 2.8, A has been assumed to be an R-module with either module or comodule structures over an R-Hopf algebra H, but no assumption on the inner structure of A has been imposed. Now, let us suppose that A is in addition an

R-algebra, so that it is endowed with multiplication and unit maps satisfying the associative and unit properties. If A is a left H-module (resp. right H-comodule), it admits an R-linear action (resp. coaction) which is well behaved with respect to the algebra (resp. coalgebra) operations of H. The notions of left module algebra and right comodule algebra arise when some compatibility conditions are imposed between the Hopf algebra operations and the multiplication and unit maps of A.

Definition 1.2.48. *Let A be an R-algebra. We say that A is a left H-module algebra if it is a left H-module and the following conditions are satisfied:*

1. *Given $h \in H$ and $a, b \in A$,*
$$h \cdot (ab) = \sum_{(h)} (h_{(1)} \cdot a)(h_{(2)} \cdot b).$$

2. *For every $h \in H$,*
$$h \cdot 1_A = \varepsilon_H(h) 1_A.$$

There is an equivalent definition in terms of the multiplication and the unit maps of the R-algebra A.

Proposition 1.2.49. *Let H be an R-Hopf algebra and let A be an R-algebra which is also a left H-module with action denoted by $\cdot$. Then, A is a left H-module algebra if and only if $m_A \colon A \otimes A \longrightarrow A$ and $u_A \colon R \longrightarrow A$ are left H-module homomorphisms.*

Proof. First, we check that m_A is a left H-module homomorphism if and only if the condition 1 at Definition 1.2.48 holds. Let $h \in H$, $a, b \in A$ and note that

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

$$h \cdot m_A(a \otimes a') = h \cdot (ab).$$

Thus, $h \cdot (ab) = \sum_{(h)} (h_{(1)} \cdot a)\, (h_{(2)} \cdot b)$ if and only if $m_A(h(a \otimes b)) = h \cdot m_A(a \otimes b)$ and we are done.

It remains to check that the u_A is a left H-module homomorphism if and only if the condition 2 at Definition 1.2.48 is satisfied. Assume that u_A is a left H-module homomorphism. Given $h \in H$,

$$h \cdot 1_A = h \cdot u_A(1_R) = u_A(h \cdot 1_R) = u_A(\epsilon_H(h)\, 1_R) = \epsilon_H(h)\, 1_A.$$

Conversely, if 2 is satisfied, given $h \in H$ and $r \in R$,

$$u_A(h \cdot r) = u_A(\varepsilon_H(h) r) = \varepsilon_H(h)\, u_A(r) = (h \cdot 1_A)\, u_A(r) = h \cdot u_A(r).$$

□

Based on the equivalent definition of the left H-module algebra notion at Proposition 1.2.49, we establish the one of right H-comodule algebra.

Definition 1.2.50. *Let H be an R-Hopf algebra and let A be an R-algebra. We say that A is a **right H-comodule algebra** if it admits right H-comodule structure and the maps m_A, u_A are right H-comodule homomorphisms.*

As in the module algebra case, there is an equivalent definition.

Proposition 1.2.51. *Let H be an R-Hopf algebra and let A be an R-algebra. Then, A is a right H-comodule algebra if and only if the coaction β is a homomorphism of R-algebras.*

Proof. Given $a, b \in A$, we have that $\beta \circ m_A(a \otimes b) = \beta(a\,b)$ and

$$\begin{aligned}(m_A \otimes \mathrm{Id}_H) \circ \beta_{A\otimes A}(a \otimes b) &= (m_A \otimes \mathrm{Id}_H) \left(\sum_{(a),(b)} a_{(0)} \otimes b_{(0)} \otimes (a_{(1)}\, b_{(1)}) \right) \\ &= \sum_{(a),(b)} a_{(0)}\, b_{(0)} \otimes a_{(1)}\, b_{(1)} \\ &= \left(\sum_{(a)} a_{(0)} \otimes a_{(1)} \right) \left(\sum_{(b)} b_{(0)} \otimes b_{(1)} \right) \\ &= \beta(a)\,\beta(b),\end{aligned}$$

so m_A is an homomorphism of right H-comodules if and only if $\beta(a\,b) = \beta(a)\,\beta(b)$ for every $a, b \in A$.

On the other hand, we have that $\beta \circ u_A(r) = \beta(r\,1_A) = r\,\beta(1_A)$ and

$$(u_A \otimes \mathrm{Id}_H) \circ \beta_R(r) = (u_A \otimes \mathrm{Id}_H)(r \otimes u_H(1_R)) = u_A(r) \otimes 1_H = r\,1_A \otimes 1_H.$$

Thus, u_A is an homomorphism of H-comodules if and only if $\beta(1_A) = 1_A \otimes 1_H$.

Then, A is a H-comodule algebra if and only if $\beta(a\,b) = \beta(a)\,\beta(b)$ for every $a, b \in A$ and $\beta(1_A) = 1_A \otimes 1_H$, that is, β is a homomorphism of R-algebras. □

We can complete Proposition 1.2.47 to the following.

Proposition 1.2.52. *Let H be a finite R-Hopf algebra and let A be an R-algebra. Then A is a left H-module algebra if and only if it is a right H^*-comodule algebra.*

Proof. Assume that A is a right H^*-comodule algebra with coaction $\beta\colon A \longrightarrow A \otimes H^*$. Consider the left H-module structure on A as in Proposition 1.2.46, that is,

$$h \cdot a := \sum_{(a)} a_{(0)}\, \langle h, a_{(1)} \rangle, \quad h \in H,\ a \in A.$$

By Proposition 1.2.51, β is a homomorphism of R-algebras. This means that for every $a, b \in A$,

$$\beta(ab) = \sum_{(a,b)} a_{(0)} b_{(0)} \otimes a_{(1)} b_{(1)}.$$

Now, given $f \in H^*$ and $a, b \in A$, we have

$$\begin{aligned}h \cdot (ab) &= \sum_{(a,b)} a_{(0)} b_{(0)} \langle h, a_{(1)} b_{(1)} \rangle \\ &= \sum_{(a,b)} a_{(0)} b_{(0)} \sum_{(f)} \langle h_{(1)}, a_{(1)} \rangle \langle h_{(2)}, b_{(1)} \rangle \\ &= \sum_{(h)} \sum_{(a,b)} a_{(0)} \langle h_{(1)}, a_{(1)} \rangle b_{(0)} \langle h_{(2)}, b_{(1)} \rangle \\ &= \sum_{(h)} \Big(\sum_{(a)} a_{(0)} \langle h_{(1)}, a_{(1)} \rangle \Big) \Big(\sum_{(b)} b_{(0)} \langle h_{(2)}, b_{(1)} \rangle \Big) \\ &= \sum_{(h)} (h \cdot a)(h \cdot b).\end{aligned}$$

On the other hand, since $\beta(1_A) = 1_A \otimes 1_{H^*}$, for every $h \in H$ we have

$$h \cdot 1_A = \langle h, 1_{H^*} \rangle 1_A = \varepsilon_H(h) 1_A.$$

Suppose that A is a left H-module algebra. By Proposition 1.2.46, we have that m_A and u_A are left H-module homomorphisms. We know from Proposition 1.2.47 that A is a right H^*-comodule with coaction

$$\beta(a) = \sum_{i=1}^{n} (h_i \cdot a) \otimes f_i.$$

Let us check that A is a right H^*-comodule algebra. By Proposition 1.2.51, it is enough to check that β is a homomorphism of R-algebras. First, let us define a map

$$\begin{array}{rccl} \Phi\colon & A \otimes H^* & \longrightarrow & \mathrm{Hom}_R(H, A), \\ & a \otimes f & \longrightarrow & h \mapsto a\langle f, h \rangle. \end{array}$$

This is clearly an R-linear map, and it is bijective because it has inverse

$$\begin{array}{rccl} \Psi\colon & \mathrm{Hom}_R(H, A) & \longrightarrow & A \otimes H^*, \\ & \varphi & \longmapsto & \sum_{i=1}^{n} \varphi(h_i) \otimes f_i. \end{array}$$

Indeed, given $a \otimes f \in A \otimes H^*$, we have

$$\begin{aligned} \Psi \circ \Phi(a \otimes f) &= \sum_{i=1}^{n} \Phi(a \otimes f)(h_i) \otimes f_i \\ &= \sum_{i=1}^{n} a\langle f, h_i \rangle \otimes f_i \\ &= a \otimes \Big(\sum_{i=1}^{n} \langle f, h_i \rangle f_i \Big) \\ &= a \otimes f, \end{aligned}$$

and conversely, for any $\varphi \in \mathrm{Hom}_R(H, A)$ and $h \in H$,

$$\begin{aligned} \Phi \circ \Psi(\varphi)(h) &= \Phi\Big(\sum_{i=1}^{n} \varphi(h_i) \otimes f_i \Big)(h) \\ &= \sum_{i=1}^{n} \varphi(h_i) \langle f_i, h \rangle \\ &= \varphi\Big(\sum_{i=1}^{n} \langle f_i, h \rangle h_i \Big) \\ &= \varphi(h). \end{aligned}$$

Since h is arbitrary, we conclude that $\Phi \circ \Psi(\varphi) = \varphi$.

Let us check that β is a homomorphism of R-algebras. Given $a, b \in A$, we shall prove that $\Phi(\beta(ab)) = \Phi(\beta(a)\beta(b))$. From the bijectivity of Φ, it will follow that $\beta(ab) = \beta(a)\beta(b)$.

First, we have

$$\beta(ab) = \sum_{i=1}^{n} h_i \cdot (ab) \otimes f_i.$$

Thus, given $h \in H$,

$$\Phi(\beta(ab))(h) = \sum_{i=1}^{n} h_i \cdot (ab)\langle f_i, h\rangle.$$

Since $\langle f_i, h\rangle \in R$,

$$\sum_{i=1}^{n} h_i \cdot (ab)\langle f_i, h\rangle = \Big(\sum_{i=1}^{n} \langle f_i, h\rangle h_i\Big) \cdot (ab) = h \cdot (ab).$$

From this, we have that

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

because A is a left H-module algebra. Now, writing elements of h with respect to $\{h_i, f_i\}_{i=1}^{n}$, we obtain

$$\sum_{(h)} (h_{(1)} \cdot a)(h_{(2)} \cdot b) = \sum_{(h)} \Big(\sum_{i=1}^{n} \langle f_i, h_{(1)}\rangle h_i\Big) \cdot a \Big(\sum_{j=1}^{n} \langle f_j, h_{(2)}\rangle h_j\Big) \cdot b.$$

Again, since the expressions in brackets belong to R, we have

$$\begin{aligned}
\sum_{(h)} \Big(\sum_{i=1}^{n} \langle f_i, h_{(1)}\rangle h_i\Big) \cdot a \Big(\sum_{j=1}^{n} \langle f_j, h_{(2)}\rangle h_j\Big) \cdot b &= \sum_{(h)} \Big(\sum_{i=1}^{n} (h_i \cdot a)\langle f_i, h_{(1)}\rangle\Big)\Big(\sum_{j=1}^{n} (h_j \cdot b)\langle f_j, h_{(2)}\rangle\Big) \\
&= \sum_{(h)} \sum_{i,j=1}^{n} (h_i \cdot a)(h_j \cdot b)\langle f_i, h_{(1)}\rangle\langle f_j, h_{(2)}\rangle \\
&= \sum_{i,j=1}^{n} (h_i \cdot a)(h_j \cdot b) \sum_{(h)} \langle f_i, h_{(1)}\rangle\langle f_j, h_{(2)}\rangle
\end{aligned}$$

Note that

$$\begin{aligned}
\sum_{(h)} \langle f_i, h_{(1)}\rangle\langle f_j, h_{(2)}\rangle &= (f_i \otimes f_j)\Big(\sum_{(h)} h_{(1)} \otimes h_{(2)}\Big) \\
&= (f_i \otimes f_j)\Delta_H(h) \\
&= m_{H^*}(f_i \otimes f_j)(h) \\
&= \langle f_i f_j, h\rangle.
\end{aligned}$$

Therefore,

$$\sum_{i,j=1}^{n} (h_i \cdot a)(h_j \cdot b) \sum_{(h)} \langle f_i, h_{(1)}\rangle\langle f_j, h_{(2)}\rangle = \sum_{i,j=1}^{n} (h_i \cdot a)(h_j \cdot b)\langle f_i f_j, h\rangle.$$

Since

$$\beta(a)\beta(b) = \sum_{i,j=1}^{n} (h_i \cdot a)(h_j \cdot b) \otimes f_i f_j,$$

we see that

$$\sum_{i,j=1}^{n} (h_i \cdot a)(h_j \cdot b)\langle f_i f_j, h\rangle = \Phi(\beta(a)\beta(b))(h).$$

Going through the chain of equalities, we conclude that

$$\Phi(\beta(ab))(h) = \Phi(\beta(a)\beta(b))(h),$$

for every $h \in H$, from which the desired equality follows. □

Bibliography

[Chi00] L. N. Childs. *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory*. 1st ed. Mathematical Surveys and Monographs 80. American Mathematical Society, 2000. ISBN: 0-8218-2131-8.

[Neu99] J. Neukirch. *Algebraic Number Theory*. Springer, 1999.

[Und15] R. Underwood. *Fundamentals of Hopf Algebras*. Universitext. Springer, 2015.