Hopf-Galois theory and applications to number theory

Daniel Gil Muñoz

Charles University
&
Università di Pisa

Cornelius Greither

Universität der Bundeswehr München

These notes are a support material for the PhD course *Hopf-Galois theory and applications to number theory* delivered by the author and Cornelius Greither at the University of Pisa during Fall 2025.

September 2025

Contents

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

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

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 $\{\mathrm{min.poly.}(\alpha, K) \mid \alpha \in S\}$ 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.

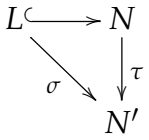
1. Every quadratic extension L/K is normal. Indeed, there is $n \in K$ such that $L = K(\sqrt{n})$, and given an embedding $\sigma\colon L \longrightarrow \overline{L}$, we have $\sigma(\sqrt{n}) = -\sqrt{n}$, so $\sigma(L) = L$.
2. Let $\alpha = \sqrt[3]{2}$ be the real root of $x^3 - 2$. Then $\mathbb{Q}(\alpha)/\mathbb{Q}$ 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 $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/E) \cong \mathrm{Gal}(E/K)$.

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 $s_1(r \otimes a) = r\,a = s_2(a \otimes r)$.

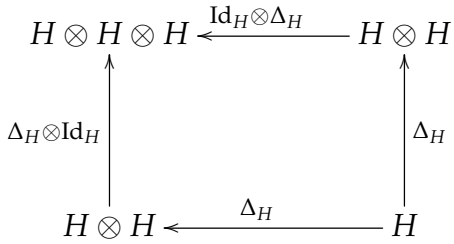
   *The map m_H is called **multiplication map**, and u_H is called **unit map**.*

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:

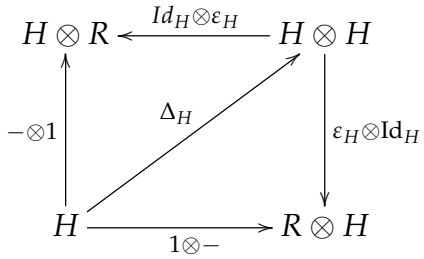


(b) **(Counit properties)** *For all $h \in H$,*

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

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

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

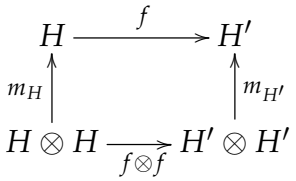
We have defined a Hopf algebra as a structure composed by more simple structures. In the same way, the notion of a homomorphism of a Hopf algebras arises naturally as a homomorphism between these structures.

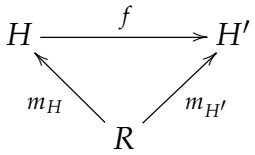
Definition 1.2.9. *An R-Hopf algebra homomorphism between two R-Hopf algebras H, H' is a map $f\colon H \longrightarrow H'$ such that:*

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 $f \circ S_H = S_{H'} \circ f$.*

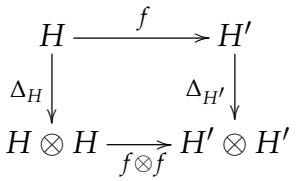
If f satisfies 1 and 2, we say that f is a homomorphism of R-algebras.
If f satisfies 1 and 3, f is said to be a homomorphism of R-coalgebras.
If f satisfies 1-3, we will say that f is a homomorphism of R-bialgebras.
In all these cases, H and H' can be required to be just R-algebras, R-coalgebras or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

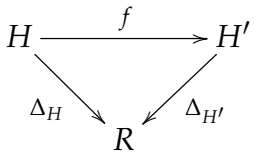
The conditions 2a and 2b are equivalent to the commutativity of these diagrams:



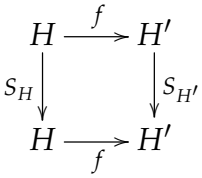


Likewise, the conditions 3a and 3b are equivalent to the commutativity of these other diagrams:





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



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:* $m_B \coloneqq m_H \mid_{B\otimes B}\colon B \otimes B \longrightarrow B$.
- *Unit map* $u_B \coloneqq u_H\colon R \longrightarrow B$.
- *Comultiplication map:* $\Delta_B \coloneqq \Delta_H \mid_B\colon B \longrightarrow B \otimes B$.
- *Counit map:* $\varepsilon_B \coloneqq \varepsilon_H \mid_B\colon B \longrightarrow R$.
- *Coinverse map:* $S_B \coloneqq S_H \mid_B\colon B \longrightarrow B$.

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 $j \in \{1, \ldots, m\}$. 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

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

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 $i \in \{m+1, \ldots, n\}$. Since j is arbitrary, we deduce that $v_i = g_i$ for all $i \in \{1, \ldots, m\}$.

Let $H = \{g_1, \ldots, g_m\}$. 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 $f \otimes g \in \operatorname{Ker}(\Phi)$, 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: $m_H \coloneqq \eta^{-1} \circ m_{H^{**}} \circ (\eta \otimes \eta)$.
- Unit map: $u_H \coloneqq \eta^{-1} \circ \eta_{H^{**}}$.
- Comultiplication map: $\Delta_H \coloneqq (\eta^{-1} \otimes \eta^{-1}) \circ \Delta_{H^{**}} \circ \eta$.
- Counit map: $\varepsilon_H \coloneqq \varepsilon_{H^{**}} \circ \eta$.
- Coinverse map: $S_H \coloneqq \eta^{-1} \circ S_{H^{**}} \circ \eta$.

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.

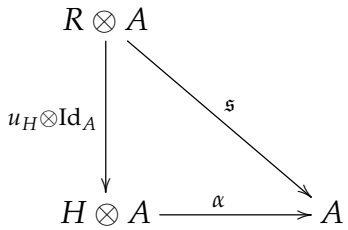
We need to consider R-linear actions of R-Hopf algebras that are in addition well behaved with respect to the Hopf algebra operations. This leads to the notion of left H-module.

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:*



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

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

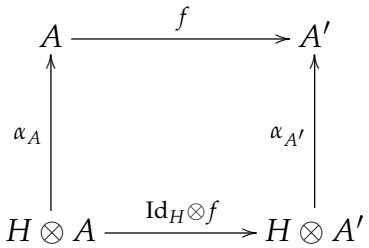
while the unit property translates into

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

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:*



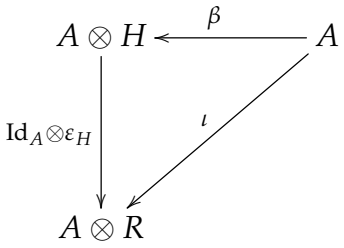
While in the notion of left H-module we have an action consisting on an R-linear map $\alpha\colon H \otimes A \longrightarrow A$ compatible with the Hopf algebra operations, we can dualize this notion to the one of right H-comodule.

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:*

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

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:*

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & A' \\ \downarrow{\scriptstyle \beta_A} & & \downarrow{\scriptstyle \beta_{A'}} \\ H \otimes A & \xrightarrow{\mathrm{Id}_H \otimes f} & H \otimes A' \end{array}$$

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

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

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

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

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

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

Therefore,

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

Since

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

we see that

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

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. □

3 Exercises

3.1 Exercises on Section 1

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.

3.2 Exercises on Section 2

1. Let G be a group. Prove that the R-group algebra $R[G]$ is an R-Hopf algebra.

2. Let H and H' be R-Hopf algebras. Prove that $H \otimes H'$ is an R-Hopf algebra with the following operations:

   - Multiplication map: $m_{H\otimes H'} \colon (H \otimes H') \otimes (H \otimes H') \longrightarrow H \otimes H'$, $m_{H\otimes H'}((a \otimes b) \otimes (c \otimes d)) = m_H(a \otimes c) \otimes m_{H'}(b \otimes d)$.
   - Unit map: $u_{H\otimes H'} \colon R \longrightarrow H \otimes H'$, $u_{H\otimes H'}(r) = r1_H \otimes 1_{H'}$.
   - Comultiplication map: $\Delta_{H\otimes H'} = (\mathrm{Id_H} \otimes \tau \otimes \mathrm{Id}_{H'}) \circ (\Delta_H \otimes \Delta_{H'}) \colon H \otimes H' \longrightarrow (H \otimes H') \otimes (H \otimes H')$, where $\tau \colon H \otimes H' \longrightarrow H' \otimes H$ is defined by $\tau(a \otimes b) = b \otimes a$.
   - Counit map: $\varepsilon_{H\otimes H'} \colon H \otimes H' \longrightarrow R$, $\varepsilon_{H\otimes H'}(a \otimes b) = \varepsilon_H(a)\varepsilon_{H'}(b)$.

- Coinverse map: $S_{H\otimes H'}\colon H\otimes H' \longrightarrow H\otimes H'$, $S_{H\otimes H'}(a\otimes b) = S_H(a)\otimes S_{H'}(b)$.

3. Let G and H be finite groups. Prove that $R[G\times H]$ and $R[G]\otimes R[H]$ are isomorphic as R-Hopf algebras.

4. Let A be an R-algebra and let C be an R-coalgebra. Given $f, g \in \mathrm{Hom}_R(C, A)$, the **convolution** of f and g is defined as

$$f * g \coloneqq m_A \circ (f\otimes g)\circ \Delta_C.$$

Prove that $(\mathrm{Hom}_R(C,A), *)$ is a monoid (that is, it is associative and admits an identity element).

Hint: It may help write down the definition of $f * g$ in terms of the Sweedler notation for the comultiplication.

5. Let H be an R-Hopf algebra. Prove that the antipode S_H is an anti-homomorphism of R-algebras, that is, $S_H(ab) = S_H(b)S_H(a)$ for all $a, b \in H$ and $S_H(1_H) = 1_H$.

Hint: Use the uniqueness of the inverse of m_H, regarded as an element of the monoid $\mathrm{Hom}_R(H\otimes H, H)$ with the convolution.

6. Let H and H' be R-Hopf algebras, and let $f\colon H \longrightarrow H'$ be a homomorphism of R-bialgebras. Prove that f is a homomorphism of R-Hopf algebras.

Hint: Use the uniqueness of the inverse of f, regarded as an element of the monoid $\mathrm{Hom}_R(H, H')$ with the convolution.

7. Let $f\colon H \longrightarrow H'$ be a homomorphism of R-Hopf algebras.

   (a) Prove that $f(G(H)) \subseteq G(H')$.

   (b) Show that $|f(G(H))|$ divides $\gcd(|G(H)|, |G(H')|)$.

8. Let H be a finite R-Hopf algebra.

   (a) Show that H is a left H-module with the multiplication $m_H\colon H\otimes H \longrightarrow H$ as action. Write down the induced right H^*-comodule structure for H.

   (b) Show that H^* is a right H^*-comodule with the comultiplication $\Delta_{H^*}\colon H^* \longrightarrow H^*\otimes H^*$ as coaction. Write down the induced left H-module structure for H^*.

9. Let H be a finite R-Hopf algebra and let A be a left H-module algebra. Let $\{h_i, f_i\}_{i=1}^n$ be a projective coordinate system for H and let $\Psi\colon \mathrm{Hom}_R(H, A) \longrightarrow A\otimes H^*$ be the map defined by

$$\Psi(\varphi) = \sum_{i=1}^{n} \varphi(h_i)\otimes f_i, \quad \varphi \in \mathrm{Hom}_R(H, A).$$

Endow $\mathrm{Hom}_R(H, A)$ with the convolution product from Exercise 4. Prove that for every $f, g \in \mathrm{Hom}_R(H, A)$,

$$\Psi(\varphi * \psi) = \Psi(\varphi)\Psi(\psi).$$

Hint: Let $\Phi\colon A\otimes H^* \longrightarrow \mathrm{Hom}_R(H, A)$ be the inverse of Φ. Try to prove that $\varphi * \psi = \Phi(\Psi(\varphi)\Psi(\psi))$.

Chapter 2

Hopf-Galois theory and the Greither-Pareigis correspondence

1 Hopf-Galois extensions and Hopf-Galois objects

In this section we will introduce Hopf-Galois structures from two viewpoints: via module algebras, and via comodule algebras. Given a Hopf-Galois structure, there is a method of turning sub-Hopf algebras (quotient Hopf algebras respectively) into subalgebras of the algebra which carries a Hopf-Galois structure. This is in a way a generalization of the classical correspondence in Galois theory of fields, but it is in a sense weaker, as not all subalgebras are reached by this process in general. We will soon describe this method, but for a proof of some main properties we will need a better understanding of algebras (via Γ-sets), an so some arguments have to be postponed

Let K be any base field. All algebras over K are assumed finite-dimensional over K unless said otherwise; the algebras bearing a Hopf-Galois structure will be assumed to be commutative. Hom groups and tensor products without subscript are taken over K.

Let H be a K-Hopf algebra. Recall that the defining map $\alpha_A : H \otimes A \longrightarrow A$ of a module algebra A makes H act on A, by the simple rule $h \cdot x = \alpha_A(h \otimes x)$ for $h \in H, x \in A$. The defining map $\beta_A : A \longrightarrow A \otimes H^*$ looks as follows in Sweedler notation: $\beta_A(x) = \sum_{(x)} x_{(0)} \otimes x_{(1)}$, where $x \in A$, and the factors $x_{(0)}$ and $x_{(1)}$ indicate elements of A and H^* respectively (see (1.4)).

There are two standard types of canonical isomorphisms for any triple X, Y, Z of K-vector spaces:

$$\mathrm{Hom}(X \otimes Y, Z) \cong \mathrm{Hom}(X, \mathrm{Hom}(Y, Z)) \text{ (Hom-Tensor adjunction)}$$

and

$$\mathrm{Hom}(X, Y \otimes Z) \cong \mathrm{Hom}(X, Y) \otimes Z.$$

This gives (recall that $H^* = \mathrm{Hom}(H, K)$ and $A = K \otimes A$):

$$\begin{aligned} \mathrm{Hom}(H \otimes A, A) &\cong \mathrm{Hom}(A, \mathrm{Hom}(H, A)) \\ &\cong \mathrm{Hom}(A, \mathrm{Hom}(H, K \otimes A)) \\ &\cong \mathrm{Hom}(A, \mathrm{Hom}(H, K) \otimes A) \\ &= \mathrm{Hom}(A, A \otimes H^*). \end{aligned}$$

The twist in the last step is necessary, not for the existence of the isomorphism, but to make it behave, with respect to module and comodule structures.

Definition 2.1.1. *Let H be a K-Hopf algebra and A a left H-module algebra. Consider the map $j : A \otimes H \longrightarrow \mathrm{End}(A) = \mathrm{Hom}(A, A)$ defined by $j(x \otimes h)(y) = x \cdot h(y)$. In other words: $j(x \otimes h)$ is the action of h on A, followed by left multiplication with the element x. Then A is said to be an H-Hopf-Galois (or H-Galois) extension if the map j is bijective.*

We remark that if j is bijective and n, m denote the K-dimensions of A and H respectively, then we get an equality $nm = dim(A \otimes H) = dim(\mathrm{End}(A)) = n^2$ and hence $n = m$.

The prime example is the Hopf algebra $K[G]$, where G is any finite group, for any $g \in G$ we have $\Delta_{K[G]}(g) = g \otimes g$, the antipode $S_{K[G]}$ sends g to its inverse, and $\varepsilon_{K[G]}(g) = 1$. Assume L/K is G-Galois. Then L becomes an H-module algebra by defining $\alpha_L(g \otimes x) = g(x)$; the action of the Galois group is simply encoded as a map $K[G] \otimes L \longrightarrow L$. We check that L is indeed a module algebra: let $x, y \in L$ and $g \in G$. Then $g(xy) = g(x)g(y)$, and on the other hand

$$\Delta_{K[G]}(g)(x \otimes y) = (g \otimes g)(x \otimes y) = g(x) \otimes g(y),$$

which contracts to $g(x)g(y)$ under multiplication. The condition concerning the unit map is obviously satisfied.

Dedekind has already showed that the elements of G, considered as elements of $\mathrm{End}(L)$, are linearly independent, if we make $\mathrm{End}(L)$ into an L-vector space, vie left multiplication by elements of L. But this is exactly saying that the map j is injective. So for reasons of dimension, j is bijective.

Let us discuss H^* and the comodule-algebra structure $\beta_L : L \longrightarrow L \otimes H^*$ in detail, to get a clear picture in this classical setting. A basis for H^* is given by the elements e_g ($g \in G$), where $e_g : K[G] \longrightarrow K$ is extraction of the g-th coefficient: $e_g(\sum_{h \in G} r_h h) = r_g$. We calculate the structure maps. First, since every $k \in G$ satisfies $\Delta_{H^*}(k) = k \otimes k$, we get $(e_g \cdot e_h)(k) = e_g(k)e_h(k)$ for all $g, h, k \in G$; this is 1 if $g = h = k$ and 0 otherwise. Therefore $e_g e_h$ is e_g if $g = h$ and 0 otherwise. Elements e with $e^2 = e$ are commonly called idempotents.

Now for the diagonal map of the dual; it is given by $\Delta_{H^*}(e_g)(h \otimes k) = e_g(hk)$. This is 1 if $hk = g$ and 0 otherwise, so $\Delta_{H^*}(e_g)$ is the sum of all $e_h \otimes e_k$ such that $hk = g$. We leave it to the readers to determine the augmentation and the antipode of H^*.

The dual H^* can be described more simply as the set of maps $\mathrm{Maps}(G, K)$, also written K^G; a G-tuple $(r_g)_{g \in G}$ is simply the map on G sending g to r_g. In other terms, the tuple $(r_g)_{g \in G}$ is $\sum_g r_g e_g$, and the idempotent e_g corresponds to the tuple having exactly one 1 at position g and zeros otherwise. From this one also sees that $L \otimes H^*$ likewise identifies with L^G (the set of maps from G to L). We may now elucidate the comodule structure.

The general rule for getting β_A from α_A uses a "dual basis" $\{h_i, \phi_i\}_i$ (see Definition 1.2.24) for the pair (H, H^*), and says $\beta(x) = \sum_i m(h_i \otimes x) \otimes \phi_i = \sum_i h_i(x) \otimes \phi_i$. (Recall that the rule going the other way is even simpler). In our case we already have a beautiful dual basis: the elements $g \in G$ for H, and the idempotents e_g for H^*. Thus:

$$\beta(x) = \sum_{g \in G} g(x) \otimes e_g.$$

If we look at the identification $L \otimes K^G = L^G$, the last sum is simply the map $G \longrightarrow L$ taking the value $g(x)$ at g; in other words, the tuple $(g(x))_{g\in G}$.

We need another definition.

Definition 2.1.2. *Let J be another K-Hopf algebra, and A be a J-comodule algebra via $\beta = \beta_A : A \longrightarrow A \otimes J$. We define a map $\gamma : A \otimes A \longrightarrow A \otimes J$ via $\gamma(x \otimes y) = (x \otimes 1)\beta(y)$. (So it is identity on the lefthand tensor factor, and restricted to the righthand tensor factor of its source, it is β.) Then A is called a right H-object if the map γ is bijective.*

Let us show that in the above example, the map $L \longrightarrow L \otimes H^* = L^G$ gives an H^*-Galois object. Let $\{x_1, \ldots, x_n\}$ be a K-basis of L. Injectivity of $\gamma : L \otimes L \longrightarrow L^G$ means that the elements $\beta(x_i)$ are not only K-linearly independent, but even over L. Let us show this. We need that the n row vectors $(g(x_i))_g$ are L-linearly independent. It is equivalent to say that the square matrix $M = \big(g(x_i)\big)_{i,g}$ has maximal rank. But now we look at the columns $\big(g(x_i)\big)_i$ of M. They are L-independent iff the elements g of G are L-independent considered as maps $L \longrightarrow L$. And this is known, again thanks to Dedekind.

Before proceeding, let us present another important class of Hopf-Galois extensions/objects.

Definition 2.1.3. *Let n be a fixed positive integer; a K-algebra A is called **fully n-graded** if*

$$A = \bigoplus_{i\in\mathbb{Z}/n\mathbb{Z}} A_i, \quad \dim_K(A_i) = 1 \quad \forall i$$

and for all $i, j \in \mathbb{Z}/n\mathbb{Z}$, the multiplication of A induces an isomorphism $A_i \otimes A_j \longrightarrow A_{i+j}$. In simpler terms, if $A_i = Kx_i$, then $x_i x_j = u_{i,j} x_{i+j}$ where $u_{i+j} \in K$ is not zero.

Example 2.1.4. Assume $u \in K$, α is a root of $x^n - u$, and the latter polynomial is irreducible. Put $A = K(\alpha)$ (a field), and $A_i = K\alpha^i$.

Now let C be another cyclic group of order n, written multiplicatively, with generator c. We will show that any fully n-graded algebra A is an H-Galois extension with $H = K^C$ and an H^*-Galois object with $H^* = (K^C)^* = K[C]$. Let us begin with the latter. The map $\beta : A \longrightarrow A \otimes H^* = A[C]$ is defined as follows: Put $\beta x = x \otimes c^i$ if $x \in A_i$ (one says: x is homogeneous of degree i), and extend by linearity. Coassociativity is easy: take $x \in A_i$. Then $(1 \otimes \Delta)\beta(x) = x \otimes c^i \otimes c^i$, and $\beta \otimes 1$ applied to $\beta(x) = x \otimes c^i$ gives the same. Let us also check that the induced map γ is bijective. Take a basis x_i of every A_i. Then γ maps $x_j \otimes x_i$ to $x_j x_i \otimes c^i$, and the "fully graded" condition ensures that these elements generate all of $A[C]$. This makes γ surjective, hence bijective.

Let us quickly describe the corresponding H-Galois structure on the fully n-graded algebra A; details left to reader. Recall that $H = K^C$ has a K-basis $(e_0, e_1, \ldots e_{n-1})$ of idempotents, each e_i acting on $K[C]$ as extraction of the coefficient at c^i. One can then check that $e_i \in H$ acts on A as projection to the direct summand A_i. – We note in passing that one can prove a converse: indeed A is an H^*-Galois object (or as we will see: equivalently, an H-Galois extension) only if A is fully graded and the structures arise exactly as described.

We will now show that our definitions of Hopf-Galois extension/object behave well in general when we switch the side. In the concrete examples above, we checked it or at least mentioned it.

Proposition 2.1.5. *Let H be a K-Hopf algebra, and $\alpha : H \otimes A \longrightarrow A$, $\beta : A \longrightarrow A \otimes H^*$ be (co)module algebra structures that correspond to each other. Then A is an H-Galois extension if and only if A is an H^*-Galois object.*

Proof. The only real point is that the map j (attached to α) is bijective if and only if the map γ (attached to β) is bijective. Ensuring this equivalence is a bit technical, and we omit some details. Recall that the algebra A is assumed to be commutative.

We start by exhibiting two canonical K-linear maps. Both are isomorphisms; we will not check this (it can be done by picking bases for example). They are:

$$\eta : A \otimes H \longrightarrow \mathrm{Hom}_A(A \otimes H^*, A), \quad \eta(a \otimes h)(b \otimes \phi) = \phi(h) \cdot ab,$$

and

$$\delta : \mathrm{Hom}_K(A, A) = \mathrm{End}(A) \longrightarrow \mathrm{Hom}_A(A \otimes A, A), \quad \delta(f)(a \otimes b) = af(b).$$

Recall our two maps $j : A \otimes H \longrightarrow \mathrm{End}(A)$ and $\gamma : A \otimes A \longrightarrow A \otimes H^*$, given by $j(a \otimes h)(b) = ah(b)$ and $\gamma(a \otimes b) = (a \otimes 1) \cdot \beta(b)$. The map γ gives rise to another map $\gamma^* = \mathrm{Hom}_A(\gamma, A)$ going from $\mathrm{Hom}_A(A \otimes H^*, A)$ to $\mathrm{Hom}_A(A \otimes A, A)$. We consider the following diagram:

$$\begin{array}{ccc} A \otimes H & \xrightarrow{\quad j \quad} & \mathrm{End}(A) \\ \downarrow \eta & & \downarrow \delta \\ \mathrm{Hom}_A(A \otimes H^*, A) & \xrightarrow{\gamma^*} & \mathrm{Hom}_A(A \otimes A, A). \end{array}$$

If we can prove that this square commutes, then we are done: given that the vertical maps are bijective, the upper horizontal map will be bijective if and only if the lower one is.

As a preparation we calculate: $\gamma^*(f)(a \otimes b) = f(\gamma(a \otimes b)) = f((a \otimes 1) \cdot \beta(b)) = f(\sum_{(b)} ab_{(0)} \otimes b_{(1)})$. Now we take an element $a \otimes h$ in the upper left hand module and chase it two ways. We have $j(a \otimes h)(b) = ah(b)$, so

$$\delta j(a \otimes h)(c \otimes b) = c\, j(h \otimes a)(b) = ca\, h(b).$$

Now for the other way round the square (f being replaced by $\eta(a \otimes h)$):

$$\gamma^* \eta(a \otimes h)(c \otimes b) = \eta(a \otimes h)(\sum_{(b)} cb_{(0)} \otimes b_{(1)}) = a \sum_{(b)} cb_{(0)} \otimes h(b_{(1)}) = ac\, h(b).$$

This concludes the argument. □

Now we turn to a version of the classical Galois correspondence. For a G-Galois extension L/K, we can associate to every subgroup $U < G$ an intermediate field $\mathrm{Fix}(U) = \mathrm{Fix}(L, U) = \{x \in L : \sigma(x) = x \ \forall \sigma \in U\}$, and it is known that we obtain an inclusion-reversing bijection between the set (lattice) of all subgroups of G and the set (lattice) of all fields between K and L (see Theorem 1.1.51). In the Hopf setting, there will be two versions again, on the module side and on the comodule side. It will be important to see that these two ways of viewing the correspondence are equivalent. We say already here that in general the new correspondence will not

be perfect - we will not get all intermediate algebras between K and A, not even if $A = L$ is a field.

If L/K is G-Galois, it is a H-Galois extension with $H = K[G]$ as seen before. For any subgroup $U < G$ we have the sub-Hopf algebra $H' = K[U]$ in H, and the fixed field $E = \mathrm{Fix}(U)$ can be described as

$$E = \{x \in L : h(x) = \varepsilon(h)(x)\ \forall h \in H'\}.$$

In other words, E is the subalgebra annihilated by the augmentation kernel of the sub-Hopf algebra H'. This lends itself to a generalization. We note already here: If J and J' denote the duals of H and H' respectively, then $J = K^G$, $J' = K^U$, and the induced surjective homomorphism $J \longrightarrow J'$ of Hopf algebras, call it g, is simply restricting a G-tuple to an U-tuple. We will come back to this.

Definition 2.1.6. *Let A be an H-Galois extension, and $H' \subset H$ an arbitrary K-sub-Hopf algebra. The fixed algebra* $\mathrm{Fix}(A, H') = \mathrm{Fix}(H')$ *is defined as the set* $\{x \in A : h(x) = \varepsilon(h)(x)\ \forall h \in H'\}$. *Note that we use the simpler notation $h(x)$ instead of $\alpha_A(h \otimes x)$.*

It is obvious that $\mathrm{Fix}(H')$ is a subspace of A.

This construction reduces to the usual "fixed field" operation in the classical case, as seen above.

Example 2.1.7. Let us review the fully graded situation for another example. We take A to be a fully n-graded K-algebra, with its structure of H-Galois extension, where $H = K^C$, and C is cyclic of order n generated by c. If m is a divisor of n, and C' cyclic of order m, then there is a canonical surjective group homomorphism $C \longrightarrow C'$, mapping c to $\overline{c}$ (a generator of C'). This gives a sub-Hopf algebra $H' \subset H$, consisting of the tuples (r_i) whose i-entry $r_i \in K$ depends only on i modulo m, not just modulo n. We look at elements $a = \sum_i a_i \in A$, where $a_i \in A_i$, and we ask when such an element is annihilated by all $h - \varepsilon(h)$ with $h \in H'$. Let $0 \leq k < n$ not be divisible by m. Then there is an m-periodic tuple r having $r_0 = 0$ and $r_k = 1$. Applying it to a, we get zero only if $a_k = 0$. So we find that $\mathrm{Fix}(H')$ consists exactly of those a which have nothing in all degrees k that are not divisible by m; and this is the fully n/m-graded algebra $\sum_{0 \leq i < n; m|i} A_i = A_0 \oplus A_m \oplus A_{2m} \oplus \ldots$.

Let us now describe the Fix construction on the comodule side, starting with a motivating example. We will conclude this section by a proof that we get the same outcome of the Fix construction on both sides.

Consider $A = L$ a field Galois extension of K with group N. Then L is a J-object, with $J = K^N = \mathrm{Maps}(N, K)$; the map β sends $x \in L$ to the tuple $(\sigma(x))_{\sigma \in N}$. Let N' be any subgroup of N. This gives a surjective homomorphism $g : J \longrightarrow J' = K^{N'}$, simply by restricting tuples. We then have two maps $f_1, f_2 : L \longrightarrow L \otimes J = L^{N'}$. The first is β followed by $L \otimes g$, so x goes to $(\tau(x))_{\tau \in N'}$. The map f_2 sends $x \in L$ to $(x, \ldots, x)$, that is, the N'-tuple which has all entries equal to x.

Then it is pretty obvious that $f_1(x) = f_2(x)$ if and only if x is fixed under the subgroup N'; in other words, the so-called equalizer $\{x \in L : f_1(x) = f_2(x)\}$ of the two maps f_1 and f_2 is the fixed field of N' inside L. We now generalize this construction.

Let A be a Hopf-Galois object for the Hopf algebra J, and let $g : J \longrightarrow J'$ be any surjective homomorphism of K-Hopf algebras. Let $u = u_{J'}$ be the unit map of the

algebra J', that is, the map $K \longrightarrow J'$ that sends $r \in K$ to $r \cdot 1_{J'}$. (One might consider u as an inclusion, but in the example $J' = K^{N'}$ this would be a bit unnatural as we will see.) We define $\mathrm{Fix}(g) \subset A$ to be the equalizer of the two maps

$$\begin{aligned} A \longrightarrow A \otimes J \quad &\longrightarrow \quad A \otimes J', \quad x \longmapsto (id_A \otimes g)\beta(x); \\ A \longrightarrow A \otimes J \quad &\longrightarrow \quad A \otimes J', \quad x \longmapsto (id_A \otimes u\varepsilon)\beta(x). \end{aligned}$$

Let us check that this reproduces taking a fixed field, in the particular case just discussed: Here $g : K^N \longrightarrow K^{N'}$ is the restriction map. The first map in the display just above specializes to the map f_1. We look at $u\varepsilon$: As $u : K \longrightarrow K^{N'}$ is the diagonal, sending x to $(x, \ldots, x)$, we get that $u\varepsilon$: sends an N-tuple y to the N'-tuple all of whose entries are y_e (the e-entry of y). Hence the second map in the display specializes to f_2, as desired.

The proof of the following result has no particular difficulties (use the definitions) and is omitted.

Proposition 2.1.8. *1. If A is an H-Hopf-Galois extension and H' a sub-Hopf algebra of H, then the set* $\mathrm{Fix}(A)$ *is a subalgebra of A.*

2. If A is a J-Hopf-Galois object and $g : J \longrightarrow J'$ a surjection of Hopf algebras, then the set $\mathrm{Fix}(g)$ *is a subalgebra of A.*

The operators Fix enjoy more properties. They are injective in the sense that different sub-Hopf algebras (quotient Hopf-algebras) lead to different (co)fixed algebras, and one can also predict the dimension of the fixed algebra. To prove these statements, we need more technique, so this is deferred. For the moment, we "only" prove compatibility of the Fix operators on the two sides. We consider the usual situation: A is a H-Hopf-Galois extension via $\alpha : H \otimes A \longrightarrow A$, and the corresponding structure of A as an $H^* = J$-Galois object is $\beta : A \longrightarrow A \otimes J$. Let H' be a sub-Hopf algebra of H. Dualizing the inclusion $H' \to H$ gives a surjective Hopf algebra map $J \longrightarrow J' = (H')^*$, which will be denoted g.

Theorem 2.1.9. *With these notations and assumptions, the fixed algebra* $\mathrm{Fix}(H') \subset A$ *agrees with the cofixed algebra* $\mathrm{Fix}(g)$.

Proof. Recall the transition rule: if $\beta(x) = \sum_{(x)} x_{(0)} \otimes x_{(1)}$ with $x_{(1)} \in J$, then for $v \in H$, we have $u(x) = \sum_{(x)} x_{(0)} \cdot x_{(1)}(v)$. Let us assume $x \in \mathrm{Fix}(g)$, so $\sum_{(x)} x_{(0)} \otimes g(x_{(1)}) = \sum_{(x)} x_{(0)} \otimes u_J\varepsilon_J(x_{(1)})$, where the structural maps i_J, ε_J belong to J. Then $i_J(1)$ applied to $v \in H$ is the scalar $\varepsilon_H(v)$. We get for $v \in H'$ (the g may be inserted because v is not just in H but in H'):

$$\begin{aligned} v(x) &= \sum_{(x)} x_{(0)} \cdot x_{(1)}(v) \\ &= \sum_{(x)} x_{(0)} \cdot g(x_{(1)})(v) \\ &= \sum_{(x)} x_{(0)} \cdot i_J\varepsilon_J(x_{(1)})(v) \\ &= \sum_{(x)} x_{(0)} \cdot \varepsilon_H(v)\varepsilon_J(x_{(1)}) \\ &= \varepsilon_H(v) \cdot x, \end{aligned}$$

so x is indeed in $\mathrm{Fix}(H')$.

For the other direction, assume that x is in $\mathrm{Fix}(H')$. We choose dual bases (u_i, h_i) (with $i = 1, \ldots, n$) for H and J such that the following hold. h_1 is the unit element of J (that is, $h_1 = \varepsilon_H$); $u_1 = 1_H$; $u_1, \ldots, u_k$ are a basis of H' and all of them but u_1 are in the kernel of augmentation; and $h_{k+1}, \ldots, h_n$ are a basis of the kernel of $g : J \longrightarrow J'$. In particular, $(u_i, \overline{h_i})_{1 \le i \le k}$ is a dual basis for the pair H', J'. By the general transition rule from modules to comodules, we have $\beta(x) = \sum_{i=1}^{n} u_i(x) \otimes h_i$. Hence we obtain (denoting the map $g : J \longrightarrow H'$ simply by overbar)

$$(1 \otimes g)\beta(x) = \sum_{i=1}^{n} u_i(x) \otimes \overline{h_i}.$$

We now use that for $i > k$ the term $\overline{h_i}$ vanishes, that $u_1(x) = x$, and $u_i(x) = 0$ for $i = 2, \ldots k$ since x is H'-fixed; so the RHS in the preceding equation is simply $x \otimes \overline{h_1}$. On the other hand, $u_J \varepsilon_J$ annihilates all h_i with $i > 1$, so we likewise obtain $(1 \otimes u_J \varepsilon_J)(\sum_i u_i(x) \otimes h_i = 1 \cdot x \otimes u_J \varepsilon_J(h_1) = x \otimes h_1$. Therefore x is cofixed under g, as desired. □

2 Hopf-Galois structures on separable extensions

2.1 Describing (Hopf) algebras via Γ-sets

Our goal in this section is a description of finite-dimensional commutative algebras A over a fixed base field K by a simpler object, almost combinatorial in nature. A description of (finite-dimensional) commutative K-Hopf algebras will also emerge almost for free. This technique will allow to prove some missing facts about (co)fixed algebras in a Hopf-Galois situation, and it is an easy way towards Greither-Pareigis (GP) theory, which will be treated in the next section. We will assume for simplicity that our base field is of characteristic zero (or a finite field), so that all field extensions are separable. (It would be sufficient to assume that all algebras that we use are "separable", but then we would have to define what that means.)

Every field K has an algebraic closure $\overline{K}$, which can be thought of as a filtered union of finite (in particular algebraic) field extensions L/K. In every concrete situation it would be enough to work with one such extension L/K. But very often that field L needs to be changed (e.g. enlarged) in a longer argument, and it is a hindrance to fix such an L too early. The situation is similar to polynomials: one needs the full polynomial ring a priori, and bounds on degrees of polynomials often tend to obscure theoretical arguments that are otherwise clear. The price to pay is that $\Gamma = \Gamma_K$, the automorphism group of $\overline{K}/K$, is (almost always) infinite. But this group bears a very nice topology, called profinite. It suffices to know the following facts: The open subgroups U are exactly the fixed groups of finite extensions L/K, and they have finite index, equal to $[L : K]$, in Γ; every open subgroup contains another subgroup V still of finite index which is normal in Γ, and then $G = \Gamma/V$ is the Galois group of the fixed field $\mathrm{Fix}(V)/K$. The group Γ will act on various finite sets , and all actions will be continous in the following sense: for every $s \in S$, the so-called stabilizer $\Gamma_s = \{\gamma \in \Gamma : \gamma s = s\}$ is open. Then the intersection of all stabilizers is again open, contains an open normal subgroup V, and "in reality" the action is then via the finite group $G = \Gamma/V$.

After these preliminaries, let us repeat what a Γ-set S is: it is a set together with a map $\Gamma \times S \longrightarrow S$ denoted by a dot in the middle or by nothing, such that some obvious axioms are satisfied: $e_\Gamma s = s$, and $\beta(\gamma s) = (\beta\gamma)s$ for all $s \in S$, $\beta, \gamma \in \Gamma$. We also say: The group Γ operates on the set S. The stabilizer of an element has already be defined; it is always a subgroup. A typical example is the set $S = \{1, \ldots, n\}$, acted upon by the symmetric group of order $n!$.

Another example is the linear group $\mathrm{GL}(n, K)$ action (via left multiplication by matrices) on the column space K^n.

We offer some more remarks about group operations, for later use.

(1) The notion of morphism between two Γ-sets is so obvious that we do not have to write it down.

(2) If $s_0 \in S$, then $\Gamma s_0 = \{\gamma s : \gamma \in \Gamma\}$ is a Γ-subset of S, and it does not contain any nonempty smaller Γ-subset. Such subsets are called orbits. Every Γ-set S is the disjoint union of its orbits in an essentially unique way.

(3) For any subgroup $\Delta < \Gamma$, the set of cosets $\gamma\Delta$, $\gamma \in \Gamma$, is a Γ-set, via the operation $\rho(\gamma\Delta) = (\rho\gamma)\Delta$. It is written Γ/Δ (careful: this need not be a group unless Δ is normal), and it has only one orbit.

(4) Every orbit in a Γ-set is isomorphic to the Γ-set Γ/V, where V is defined to be the stabilizer of a chosen element.

Let $\mathcal{A}_K$ be the class (or category) of all commutative finite-dimensional K-algebras without nilpotent elements, and let $\mathcal{S}_\Gamma$ be the category of all finite Γ-sets (with continuous action, always), where Γ is short for Γ_K. Our goal is to establish inverse bijections (more precisely equivalences of categories) $\Phi : \mathcal{A}_K \longrightarrow \mathcal{S}_\Gamma$ and Ψ going the other way, and to see what happens to Hopf algebras under this correspondence. We need a minimum of algebraic informaton on algebras.

Proposition 2.2.1. *Let A be a finite-dimensional commutative K-algebra. If A has no nonzero nilpotent elements, then A is isomorphic to a finite product of fields L_i with $[L_i : K] < \infty$. (The reverse implication is also true, and obvious.)*

Proof. (a) We first argue that A has only finitely many maximal ideals. Indeed let $(\mathfrak{m}_i)_{i\in\mathbb{N}}$ be an infinite list of distinct maximal ideals. If we take $x_i \in \mathfrak{m}_i \setminus \mathfrak{m}_{s+1}$ for all $i \leq s$, then the product $x_1 \cdots x_s$ is in the intersection $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_s$ but not in $\mathfrak{m}_{s+1}$. Hence the intersection $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_{s+1}$ is properly smaller than $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_s$, which means that we have a properly descending infinite chain of ideals, which is of course impossible.

(b) Every prime ideal $\mathfrak{p}$ of A is maximal. Indeed if $\mathfrak{p}$ is prime, the factor ring $A/\mathfrak{p}$ is still finite-dimensional over K and has no zero-divisors. It is well known that this forces $A/\mathfrak{p}$ to be a field. That is, the ideal $\mathfrak{p}$ was maximal.

(c) The set of nilpotent elements in A is equal to the intersection of all prime ideals. This is a standard fact with a standard proof, which will be omitted here.

(d) Now let $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$ be the complete list of the maximal ideals of A. This is also the list of all prime ideals, so the intersection of the $\mathfrak{m}_i$ is zero, by part (c)

and our hypothesis. By the Chinese Remainder Theorem we get $A \cong A/0 \cong \prod_{i=1}^{t} A/\mathfrak{m}_i$, and it suffices to put $L_i = A/\mathfrak{m}_i$.

□

We now define the map (functor) $\Phi : \mathcal{A}_K \longrightarrow \mathcal{S}_\Gamma$ by setting

$$\Phi(A) = \mathrm{Alg}_K(A, \overline{K}).$$

Here $\mathrm{Alg}_K(A, \overline{K})$ denotes the set of K-algebra homomorphisms (= K-linear ring homomorphisms) from A to $\overline{K}$. We make Γ act on $\Phi(A)$ by the formula $\gamma \cdot \phi = \gamma\phi : A \longrightarrow \overline{K}$, for all $\phi \in \mathrm{Alg}_K(A, \overline{K})$ and $\gamma \in \Gamma$. Recall that Γ is the automorphism group of the field $\overline{K}$ over K, so the composition $\gamma\phi$ makes sense.

It is easily seen that $\Phi(A_1 \times A_2)$ is the disjoint union of $\Phi(A_1)$ and $\Phi(A_2)$ (a homomorphism ϕ must map exactly one of the idempotents $(1,0)$ and $(0,1)$ to 1, and the other one to 0). If $A = L$ is a field finite over K, then the action of Γ on $\Phi(L)$ really happens through $G = \mathrm{Gal}(M/K) = \Gamma/\mathrm{Fix}(M)$, where M is any normal field extension of K which is again finite-dimensional. We also note that the cardinal of $\Phi(A)$ is the K-dimension of A, as is easily seen by reduction to the case that $A = L$ is a field.

Example 2.2.2. Let $K = \mathbb{Q}$ and $A = \mathbb{Q}(i)$. This is already a normal field extension. The set $\Phi(A)$ has two elements f_0 and f_1; one of them is the inclusion in $\overline{\mathbb{Q}}$, the other is complex conjugation. More generally, if $A = L = K(\alpha)$ where $p(x)$ is the minimal polynomial of α, then $\Phi(L)$ corresponds to the set $\{\alpha, \alpha_2, \ldots, \alpha_{deg(p)}\}$ of roots of $p(x)$ in the algebraic closure, just by looking at the image of α under f. This also shows that the cardinal of $\Phi(L)$ equals $[L : K]$; because of the compatibility with products, we have $|\Phi(A)| = \dim_K(A)$ in general.

Let us now define $\Psi : \mathcal{S}_\Gamma \longrightarrow \mathcal{A}_K$. Generally $\mathrm{Maps}(X, Y)$ denotes the set of mappings from X to Y (this was also written Y^X earlier). If both sets are Γ-sets, then we let $\mathrm{Maps}_\Gamma(X, Y) = \{f : X \longrightarrow Y | f(\gamma x) = \gamma f(x)\ \forall x \in X\ \forall \gamma \in \Gamma\}$. Define

$$\Psi(S) = \mathrm{Maps}_\Gamma(S, \overline{K}).$$

Via pointwise operations, $\Psi(S)$ becomes a commutative ring, and also a K-vector space; we will see its dimension is $|S|$. This K-algebra obviously has no nilpotents, so it is in $\mathcal{A}_K$.

The two operators are inverse to each other. We will show this and in the process gain a better understanding. Assume S is an orbit. Then $S \cong \Gamma/U$ with an open subgroup U. Let L be the fixed field of U. Then $[L : K] = [\Gamma : U]$. We claim $\Phi(L)$ identifies with S. Indeed via restriction, Γ surjects onto $\mathrm{Alg}(L, \bar{K}$, and $\gamma, \delta \in \Gamma$ become the same there iff their restrictions to L agree as maps; this in turn is equivalent with $\gamma^{-1}\delta$ being identity on L, that is, $\gamma^{-1}\delta \in U$, and this is finally the same as saying $\gamma U = \delta U$. On the other hand we claim that $\Psi(\Gamma/U)$ identifies with L. Indeed, for every $f \in \mathrm{Maps}_\Gamma(\Gamma/U, \bar{K}$, the element $x = f(e_\Gamma U$ bust be fixed under U, hence in L; on the other hand, f is determined by x, given that $f(\gamma U)$ must be $\gamma(x)$, and any $x \in L$ may take this role.

So we see that Φ and Ψ define inverse bijections between (finite) Γsets which are orbits on the one side, and K-algebras which are field on the other side. Now any Γ-set is the disjoint union of its orbits, and any algebra A is the product of fields. So

the claim about Φ and Ψ also hold for the larger domains where they are defined, given that our operators turn disjoint unions into cartesian products In passing we have also proved: $|\Phi(A)|$ equals the K-dimension of A.

We give some examples:

Example 2.2.3. Recall that for any open subgroup H (of finite index) in Γ, we saw that the fixed field L of H inside $\overline{K}$ corresponds to the Γ-set Γ/H.

Example 2.2.4. Let I be any finite set with trivial Γ-action (which means $\gamma i = i$ for all $\gamma \in \Gamma$, $i \in I$). What are then the Γ-invariant maps f from I to $\overline{K}$? All values of f must again be fixed under Γ, and the fixed field of Γ is the ground field K, so we get $\Psi(I) = \mathrm{Maps}(I, K) = K^I$ the direct product of copies of K, indexed by I. A special case of this is: The "trivial" algebra K corresponds to the one-point set. (Of course the operation on that set cannot be other than trivial.)

Example 2.2.5. Fix an integer $n > 1$, and choose a primitive n-th root ζ_n of unity in $\overline{K}$. We define the cyclotomic character $\omega : \Gamma \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ by $\gamma(\zeta_n) = \zeta_n^{\omega(\gamma)}$. Using this we make $\mathbb{Z}/n\mathbb{Z}$ into a Γ-set, which will actually be considered as a Γ-group later on: we denote reduction mod n by an overbar and define

$$\gamma \cdot \overline{a} = \overline{\omega(\gamma)a}, \quad \overline{a} \in \mathbb{Z}/n\mathbb{Z}.$$

Denote by C_n a multiplicatively written cyclic group of order n, and pick a generator σ. Let $A = K[C_n]$ be the group ring; we have $A \cong K[x]/(x^n - 1)$ with σ mapping to $\overline{x}$.

We claim that $\Phi(A)$ is $\mathbb{Z}/n\mathbb{Z}$ with the cyclotomic Γ-action just defined. Indeed, the algebra homomorphisms from A to $\overline{K}$ are completely determined by the image of σ, and this can be any power of ζ_n. Thus, let $\phi_a : A \longrightarrow \overline{K}$ be the homomorphism that sends σ to ζ_n^a. If we apply γ, we get the homomorphism that sends σ to $\gamma(\zeta_n^a) = \zeta_n^{\omega(\gamma)a}$. Identifying ζ_n^a with $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ we get the claim.

Example 2.2.6. We have seen that Φ turns direct products of algebras into disjoint unions of sets. It is natural to ask: What corresponds to the direct product of sets on the algebra side? The answer is simple, nice and important: $\Phi(A \otimes B)$ can be naturally identified with $\Phi(A) \times \Phi(B)$, since every algebra homomorphism starting from $A \otimes B$ is uniquely characterized by what it does on $A = A \otimes 1$, and on $B = 1 \otimes B$.

At the end of this section, let us reconsider Hopf algebras in the light of this correspondence. We have not yet commented on the obvious fact that Φ and Ψ are not only defined on objects but also on maps (the technical details can safely be left to our readers); and both of the correspondence reverse the direction of the maps. Otherwise everything is preserved. Now a K-Hopf algebra H is just a K-algebra, with three extra algebra maps, which are (in order of decreasing complexity): the comultiplication $\Delta_H : H \longrightarrow H \otimes H$, the antipode $s_H : H \longrightarrow H$, and the augmentation $\varepsilon_H : H \longrightarrow K$. These maps must also obey certain axioms, coded as diagrams. The nice thing is now that we can mechanically translate all these things in the category of Γ-sets. Let $S = \Phi(H)$. Then:

- Δ_H gives $m_S : S \times S \longrightarrow S$;

- s_H gives $i_S : S \longrightarrow S$;
- $\varepsilon_H : H \longrightarrow K$ gives a map from the one-element set to S, that is: a distinguished element e_S of S.

From the nature of the diagrams it becomes clear without further effort that the Hopf axioms translate into saying that S is a group under m_S, with neutral element e_S and inverse map i_S. Furthermore, all maps on S etcetera are Γ-invariant. Let us define a Γ-group N to be a group N which is also a Γ-set, with the obvious compatibility condition that multiplication and formation of inverses commute with the Γ action and e_N is Γ-fixed. (This is actually a consequence.) We obtain:

Theorem 2.2.7. *There are inverse bijective correspondences Φ' and Ψ' between the category $\mathcal{H}_K$ of finite-dimensional commutative K-Hopf algebras on the one hand, and the category $\mathcal{G}_\Gamma$ of finite Γ-groups on the other. As before, the correspondences reverse all arrows; the product of Γ-groups corresponds to the tensor product of Hopf algebras.*

We give a few examples.

Example 2.2.8. Let us resume Example 2.2.4, assuming that the finite set I is a group (still with trivial Γ-action). Then $\Psi(I) = K^I$ becomes a Hopf algebra; let us look at the details, and we will recognize an old acquaintance . For $i \in I$ let $e_i \in K^I$ be the idempotent having 1 at position i and zero everywhere else; then $(e_i)_{i\in I}$ is a K-basis of K^I. From the definition of Ψ one can easily check the following:

$$\begin{aligned} \Delta e_i &= \sum_{j*k=i} e_j \otimes e_k; \\ s(e_i) &= e_{i^{-1}}; \\ \varepsilon(e_i) &= \delta_{i,1}. \quad \text{Kronecker's delta; 1 is the neutral element of } I \end{aligned}$$

Example 2.2.9. We go back to Example 2.2.5. We have the Hopf algebra $H = K[C_n]$ with $\Delta_H(\sigma) = \sigma \otimes \sigma$, $S_H(\sigma) = \sigma^{-1}$, and $\varepsilon_H(\sigma) = 1$. Recall that $S = \Phi(H) = \{\phi_0, \ldots, \phi_{n-1}\}$ where $\phi_i(\sigma) = \zeta_n^i$. We want to determine the group structure of S, which as a set was in canonical bijection with $\mathbb{Z}/n\mathbb{Z}$, so we expect that bijection to be also a group homomorphism. This is indeed the case: The product $\phi_i\phi_j$ in S is given by the composition

$$H \longrightarrow H \otimes H \longrightarrow \overline{K},$$

with the last map being $h \otimes h' \longmapsto \phi_i(h)\phi_j(h')$. Evaluated on σ, we get $\sigma \otimes \sigma$ and then $\phi_i(\sigma)\phi_j(\sigma)$, which is $\phi_{i+j}(\sigma)$. So indeed $\phi_i\phi_j = \phi_{i+j}$. This suffices to pin down the group structure. Recall that we already determined the Γ-action; one should spend a moment checking directly that the action is compatible with the group structure, as it has to be.

2.2 Translating Hopf-Galois structures and the Fix construction

We have a good understanding of algebras and Hopf algebras, via our correspondence. It will not be a surprise that the correspondence also applies to Hopf-Galois situations. Let us note two things: the resulting description is really simple, much

simpler than the original one (this is perhaps not surprising), and the coalgebra version (Hopf-Galois objects) is much more suitable for the translation than the algebra version (which is perhaps surprising at first).

Recall what it means that A is an H-Hopf-Galois object: we have a sort of diagonal $\beta\colon A \longrightarrow A \otimes H$ which is co-associative and co-unitary, and the induced map

$$\gamma : A \otimes A \longrightarrow A \otimes H, \quad a \otimes b \longmapsto (a \otimes 1) \cdot \beta(b)$$

is an isomorphism. (Equivalently, A is an H^*-Hopf-Galois extension, but this will be in the background for the moment.) We proceed to translate this into the language of Γ-sets. Let A correspond to the Γ-set S, and let H correspond to the Γ-group N.

Then β translates into a map $m = m_{S,N} : S \times N \longrightarrow S$. The axioms of coassociativity and co-unitarity are equivalent then to saying that m defines a (right) action of the group N on S, so S is a right N-set. (Recall that S is a left Γ-set.) We now ask ourselves what the bijectivity of γ means in terms of sets; the answer will be nice. As a preparation we need:

Definition 2.2.10. *Let Π be a group acting on a set X from the right. (Left actions can be treated similarly.) Then the action is transitive, if for any two $x, y \in Y$ there is $\pi \in \Pi$ with $x\pi = y$. The action is called simply transitive, when this π always exists, and is unique.*

Remark 2.2.11. The action is transitive iff X is an orbit, that is, isomorphic to $U\backslash\Omega$ for some subgroup U. The action is moreover simply transitive iff that subgroup is trivial. In other words: A set X with a simply transitive action of a group Ω is basically a copy of the group, only that in X we do not have a distinguished element, like the unit element in Ω.

Proposition 2.2.12. *With the above notation, the map γ is bijective if and only if the resulting action of N on S (on the right) is simply transitive.*

Proof. One mechanically translates γ into a map $q : S \times N \longrightarrow S \times S$, given by $q(s, \nu) = (s, s\nu)$. The bijectivity of q is then equivalent to the simple transitivity of the action of N on S. □

This situation is only possible if S and N have the same cardinality. We already know that these cardinalities are equal to the respective K-dimensions of K and H. So we recover the fact that a Hopf-Galois situation is only possible if the algebra and the Hopf algebra have the same dimension.

To complete the picture we revisit the Galois correspondence, that is, fixed and co-fixed subalgebras. As mentioned before, it is simpler to work with the comodule side. So assume that the algebra A is a J-Hopf-Galois object, and $g : J \longrightarrow J'$ is a surjective homomorphism of Hopf algebras. Let $S = \Phi(A)$, $N = \Phi(J)$, and $N' = \Phi(J')$. Then S has an action of N from the right which is simply transitive, and N' embeds as a subgroup of N (we consider this as an inclusion). Let $B = \mathrm{Fix}(g) \subset A$ be the co-fixed algebra; we want to understand $T = \Phi(B)$.

To do this we just have to translate the construction. As a set or vectorspace, B was defined as a difference kernel of two maps δ_0 and δ_1. That is, B is the largest subalgebra of A such that composing the inclusion $\iota : B \longrightarrow A$ with δ_0, and δ_1 respectively, gives the same map. Hence T is the finest surjective image of S such that composing $\Phi\delta_0$ (and $\Phi\delta_1$ respectively) with the surjection $S \longrightarrow T$ gives the same map. In other words, we are looking for the equivalence relation on S generated

by the postulate that $\Phi\delta_0(z)$ and $\Phi\delta_1(z)$ are equivalent, for all z in the domain of definition of the $\Phi\delta_i$, which is $S \times N'$. Now $\Phi\delta_0 : S \times N' \longrightarrow S$ is just the action of N on S, restricted to N'; and $\Phi\delta_1$ is the "no action" map, sending $(s, \nu) \longrightarrow s * 1_N = s$. Thus we are looking for the finest equivalence relation on S that makes s and $s * \nu$ equivalent, for all $\nu \in N'$.

This description is very concrete: T is just "S modulo N'", that is, the set of N'-orbits in S. This set T still has an action of N from the right. The fact that N acts simply transitively gives at once that all N'-orbits have $|N'|$ elements, so $|T| = |N|/|N'|$. We also see that T (or rather the equivalence relation defining it) allows to recover N'. We repeat these insights:

Theorem 2.2.13. *Let the notation be as above. Then we have an equality* $\dim_K(B) = \dim_K(J)/\dim_K(J')$. *Moreover the operator "co-fixed algebra" is injective, in the sense that surjections* $J \longrightarrow J'$ *and* $J \longrightarrow J''$ *that give rise to different subgroups* N', N'' *will also give rise to different co-fixed algebras.*

2.3 Base change

In this short section we take a different look at the (Hopf) algebras defined by Γ-sets, and Γ-groups, respectively. This view is often taken in the literature, and there it comes under the name "faithfully flat descent" or "Galois descent".

The correspondences defined in the preceding section depend on the base field K; in the present section it will be better to include this in the notation, writing Φ_K instead of Φ, and so on. Whenever L is a finite extension of K within $\overline{K}$, the algebraic closure of L is still $\overline{K}$, and $\Gamma_L = \mathrm{Aut}(\overline{K}/L)$ is an open subgroup of Γ_K. (Recall that if L is normal, then $G = \Gamma_K/\Gamma_L$ is the Galois group of L/K.)

We slightly rewrite the definition of Ψ_K. Remember that $\Psi_K(S)$ is the set of all Γ_K-equivariant maps $f : S \longrightarrow \overline{K}$. Actually $\mathrm{Maps}(S, \overline{K})$ is itself a Γ-set, by setting

$$(\gamma f)(s) = \gamma f(\gamma^{-1}s), \quad f : S \longrightarrow \overline{K}, s \in S.$$

When one checks that this does define a Γ_K-action, one will also see that one really needs to take inverses as written. But it is then clear that $\mathrm{Maps}_{\Gamma_K}(S, \overline{K})$ is then exactly the set of all $f \in \mathrm{Maps}(S, \overline{K})$ which are fixed under this new action.

For the next lemma (which is simple but fundamental) we need a harmless bit of notation: if X is any Γ_K-set, and L as above, then $X|L$ is the same set as X, but with restricted action: only Γ_L acts. It may seem unnecessary to indicate this, but the reader will see that it is useful for clarity.

Lemma 2.2.14. *With the above notations, we have for every commutative finite-dimensional K-algebra A the following:*

$$\Phi_L(L \otimes_K A) = \Phi_K(A)|L.$$

Proof. Again this will follow from the defining properties of the tensor product. Let us look at L-algebra homomorphisms $\phi' : L \otimes_K A \longrightarrow \overline{K}$. Then $\phi'(y \otimes a) = y \cdot \phi'(1 \otimes a)$ for all $y \in L$ and $a \in A$, so ϕ' is uniquely determined by its restriction ϕ to $1 \otimes A$, which we identify with A. This already identifies $\Phi_L(L \otimes A)$ with $\Phi_K(A)$ as sets. It is then obvious that the action of Γ_L is the same on both of these sets, now identified, which finishes the argument. □

The following will be formulated for commutative K-algebras, but everything holds also for comm. K-Hopf algebras with the appropriate changes. Consider a Γ-set S and the corresponding algebra A. There exists an open subgroup U of Γ such that H acts trivially on S, and we can even take U normal.

Let M be the fixed field of U; then $U = \Gamma_M$, and $G = \Gamma/U$ is the (finite) Galois group of M/K. By the lemma, $M \otimes A$ is the "trivial" algebra $M^S = \mathrm{Maps}(S, M)$, because the Γ_M-action on $\mathrm{Maps}(S, \overline{K})$ is just given by the action on $\overline{K}$, and the fixed field is M. The factor group G acts on $\mathrm{Maps}(S, M)$ in a way totally similar to the Γ_K-action on $\mathrm{Maps}(S, \overline{K})$: given $g \in G$ and $f : S \longrightarrow M$, we have $(gf)(s) = gf(g^{-1}s)$. Thus G acts by K-algebra automorphisms on $M \otimes A$, and the G-fixed subalgebra is A, for the following reason: Taking Γ_K-invariants at once is the same as first taking Γ_M-invariants and then taking $G = \Gamma_K/\Gamma_M$-invariants. Thus every comm. K-algebra A can be obtained from a "trivial" M-algebra by taking invariants under a suitable $\mathrm{Gal}(M/K)$-action, for a suitable finite Galois extension M/K. This M is also called a trivializing extension for A.

2.4 The so-called Greither-Pareigis correspondence

In this section, actions of Γ will be denoted by a dot $\cdot$ (or nothing), and an action of a Γ-group on a Γ-set will be denoted by $*$. The former is from the left, and the latter usually from the right.

Our classical example is $A = L$ a G-Galois extension of K, with the structure of K^G-Hopf-Galois object given by $\beta(x) = \sum_{g \in G} g(x) \otimes e_g$. The Γ-group N corresponding to K^G is the group G with trivial Γ-action; the Γ-set corresponding to L is $S = G = \Gamma/H$ where H is the group fixing L, with the obvious left Γ-action; and one checks that the action of G (as the group) on G (as the set) is again given by the group structure in G. This time the action is on the right.

Now let us look at a general situation: A is an H-Hopf-Galois object, with A corresponding to the Γ-set S and H corresponding to the Γ-group N. It is intentional that we don't use the letter G here, since we are not assuming that A is a G-Galois extension of K. By translation we get a simply transitive action $* : S \times N \longrightarrow S$. The map $N \longrightarrow \mathrm{Perm}(S)$ which sends ν to $\pi_\nu : S \ni s \longmapsto s * \nu$ is injective, and an anti-homomorphism of groups (if we use the usual composition as the group law in $\mathrm{Perm}(S)$. Thus, giving N and its action on S is the same as giving a simply transitive subgroup $\Pi = \{\pi_\nu : \nu \in N\}$ of $\mathrm{Perm}(S)$.

Let us denote the map $s \mapsto \gamma \cdot s$ (with $s \in S$ and $\gamma \in \Gamma$) by λ_γ. (Later this will indeed be a left multiplication.) The Γ-invariance of $*$ gives the following formula, for $\gamma \in \Gamma$, $\nu \in N$, and $s \in S$:

$$\lambda_\gamma(\pi_\nu(s)) = \pi_{\gamma \cdot \nu}(\lambda_\gamma(s)),$$

that is,

$$\pi_{\gamma \cdot \nu} = \lambda_\gamma \pi_\nu \lambda_\gamma^{-1},$$

or in terms of the group Π (we simply transfer the Γ-action from N to Π):

$$\gamma \cdot \phi = \lambda_\gamma \phi \lambda_\gamma^{-1}, \quad \forall \phi \in \Pi.$$

This shows that in our setting the Γ-action on Π (or N) can be determined from the other data, and moreover that Π as a subgroup of $\mathrm{Perm}(S)$ must be normalized by

all the λ_γ, with $\gamma \in \Gamma$. (If Ω is any group with any subgroup U, then $x \in \Omega$ is said to normalize U iff $xUx^{-1} = U$. The set $N_\Omega(U)$ of all x that normalize U is called the normalizer of U in Ω. It is the biggest subgroup of Ω which contains U as a normal subgroup.)

Now assume $A = L$ is a field. Then the Γ-set S becomes an orbit: it is Γ/Γ' with Γ' the open subgroup fixing L. (We have replaced U by Γ', to conform with the literature.) Then $\lambda_\gamma : \Gamma/\Gamma' \longrightarrow \Gamma/\Gamma'$ is indeed multiplication by γ on the left. We repeat what we have just seen:

Proposition 2.2.15. *Let $S = \Gamma/\Gamma'$ as above and let $\Pi \subset \mathrm{Perm}(S)$ be a simply transitive subgroup. Then the resulting action $* : S \times \Pi \longrightarrow S$ is Γ-equivariant if and only if the Γ-action on Π is given by the formula*

$$\gamma \cdot \pi = \lambda_\gamma \pi \lambda_\gamma^{-1}.$$

In particular Π must be normalized by all the left translations λ_γ.

Let us denote the subgroup of $\mathrm{Perm}(S)$ made up by all the λ_γ by Λ. We reformulate our findings as follows.

Theorem 2.2.16. *Let L/K be a field, finite over K, with fixed group $\Gamma' \subset \Gamma$. Then all instances of "L is a H-Hopf-Galois object" are given by simply transitive subgroups $\Pi \subset \mathrm{Perm}(\Gamma/\Gamma')$ such that Π is normalized by Λ. The Hopf algebra H is given by the group Π and the Γ-action via Λ (by conjugation).*

In the classical example where L/K is Galois with group G, the group Π is made up by all right translations ρ_γ as we have seen. Let us state this again, in different words: $G = \Gamma/\Gamma'$ (which is also S!!), the group G acts on the set G by right multiplication, so $\Pi = G$ acting by right multiplications on G. Here Π is not only normalized by Λ but actually centralized.

Let us revisit another example. Let $K = \mathbb{Q}$, p an odd prime, $a \in \mathbb{Q}$ not a p-th power. Let $\alpha = \sqrt[p]{a}$. Then $L = \mathbb{Q}(\alpha)$ has degree p; put $H = \mathbb{Q}[C$ where C is a cyclic group of order p. We have seen that $L/\mathbb{Q}$ is an H-Galois object. Let Γ' be the fixed group of L and let $\Gamma_0 \subset \Gamma'$ be the fixed group of the normal closure L' of L, which is given by $E = \mathbb{Q}(\alpha, \zeta_p)$. Finally write G for Γ/Γ_0; this is the Galois group of $L'/\mathbb{Q}$. It is instructive (if a bit involved) to determine G explicitly. Let $\sigma \in G$ be described by $\sigma(\alpha) = \zeta_p\alpha$ and $\sigma(\zeta_p) = \zeta_p$. On the other hand $\tau \in G$ is specified by saying that it fixes α and ζ_p to ζ_p^t where t is a chosen primitive root modulo p. Then G is the semidirect product of the cyclic group C of order p generated by σ,which is normal, and the cyclic group G' of order $p-1$ generated by τ. The action of the latter on the former is (only in different notation) the cyclotomic one, and G' is the image of Γ' in G, so $\Gamma/\Gamma' = G/G'$. We can identify G/G' with the set $S = \{0, 1, \ldots, p-1\}$, and the group Π (which is again cyclic of order p, with cyclotomic Γ-action) acts on this by cyclic shifts. Observe that $\tau \in G$ acts on S as multiplication by t. So this does not commute with the action of Π, but the group Π is normalized by τ which is "multiplication by t". In fact, the normalizer of the group Π (which is generated by the cyclic permutation $c : 0 \mapsto 1 \mapsto \cdots \mapsto p-1 \mapsto 0$) is exactly generated by c and τ, as we will prove later.

2.5 Explicit formulas

A variant of a previous example goes as follows (replace the odd prime p by the number 4): Take $a \in \mathbb{Q}$ squarefree, $a \neq \pm 1$. Take $L = \mathbb{Q}(x)$ with $x^4 = a$, and $J = \mathbb{Q}[C_4]$, where C_4 is cyclic of order 4 with chosen generator σ. Then one can show that L has degree 4, and $\beta : L \longrightarrow J \otimes L$, $x \longmapsto x \otimes \sigma$, makes L into a J-Galois object. For $S = \Phi(L)$ we get the set $\{0,1,2,3\}$ with a certain Γ-action, and $N = \mathbb{Z}/4\mathbb{Z}$ with the cyclotomic Γ-action.

On the module side, we have $H = J^* = \mathbb{Q}^{\mathbb{Z}/4\mathbb{Z}}$, which is the product of four copies of $\mathbb{Q}$, indexed by $0,1,2,3$. We have corresponding idempotents $e_0, \ldots, e_3$ (just one 1 and three zeros each), and the action of e_j on L is projection to the one-dimensional subspace $\mathbb{Q}x^j$. The same holds if we perform a base-change, that is we tensor everything with $E = \mathbb{Q}(i)$ over $\mathbb{Q}$; but then we should be careful and write $E \otimes L$ instead of $E(x)$ (even though one can show that these objects are equal, as $E(x)$ has degreee 8 over $\mathbb{Q}$). We define

$$\eta = e_0 + ie_1 - e_2 - ie_3 = (1, i, -1, -i) \in E \otimes H.$$

The following lemma is checked by calculation, using that we know the diagonal map on Hopf algebras of type K^N.

Lemma 2.2.17. *The element η is group-like, that is, $\Delta(\eta) = \eta \otimes \eta$. Note moreover that $\eta^4 = 1$.*

Now we define $c = \frac{1}{2}(\eta + \eta^3)$ and $s = \frac{1}{2i}(\eta - \eta^3)$. In quadruple notation we have $c = (1, 0, -1, 0)$ and $s = (0, 1, 0, -1)$. The action of c on L is certainly not an automorphism; but if restrict the action to the quadratic subfield

$$L_0 = \mathbb{Q} \oplus \mathbb{Q}x^2$$

, then c actually acts as the nontrivial automorphism of L_0 (you should convince yourself of this).

Lemma 2.2.18. 1. *$cs = 0$ and $c^2 + s^2 = 1$.*

2. *$\Delta c = c \otimes c - s \otimes s$ and $\Delta s = s \otimes c + c \otimes s$.*

Remark 2.2.19. These formula explain the choice of the letters; c and s are intended to be reminiscent of cosine and sine.

Proof. 1. The first formula is easy to show from the definitions, and actually obvious if we look at c and s written as quadruples.

2. We have $2\Delta\eta = \eta \otimes \eta + \eta^{-1} \otimes \eta^{-1}$. On the other hand, for $4(c \otimes c - s \otimes s)$ we get the eight-term sum $\eta \otimes \eta + \eta \otimes \eta^{-1} + \eta^{-1} \otimes \eta + \eta^{-1} \otimes \eta^{-1} + \eta \otimes \eta - \eta \otimes \eta^{-1} - \eta^{-1} \otimes \eta + \eta^{-1} \otimes \eta^{-1}$. After simplifying and comparing we obtain the first formula. The second formula is checked similarly.

□

We said that the element $c \in H$ does not act as a (field) automorphism. This is compatible with the fact that it is not group-like. However for $x, y \in L$ we have the

following formulas, which are reminiscent of the addition theorems for cosine and sine:

$$\begin{aligned} c(xy) &= c(x)c(y) - s(x)s(y); \\ s(xy) &= s(x)c(y) + c(x)s(y). \end{aligned}$$

It is open to debate whether these formulas are illuminating. It is certainly possible to perform similar computations in examples of larger dimension, but in our opinion the resulting formulas will not tell us much.

3 First applications of the main theorem

3.1 Almost classical extensions

This notion is inspired by the example $L = \mathbb{Q}(\sqrt[p]{a})$, whose normal closure is $L(\zeta_p)$. Here the group $G = \mathrm{Gal}(L(\zeta_p)/\mathbb{Q})$ can be split as a semidirect product, one factor of which is $\mathrm{Gal}(L(\zeta_p)/L)$. This is in fact a rather special situation. (Of course it arises in a trivial way if L/K is already a Galois extension itself.)

So assume that as always L/K is a finite-dimensional field extension with normal closure $\tilde{L}/K$. Let $G = \mathrm{Gal}(\tilde{L}/K)$, and let $G' < G$ be the subgroup $\mathrm{Gal}(\tilde{L}/L)$. So if Γ' is the subgroup of Γ fixing L, then the set of cosets Γ/Γ' identifies with G/G'. Assume moreover that there is a normal extension M/K inside $\tilde{L}$ such that

$$ML = \tilde{L},\ M \cap L = K.$$

The field M will be called a complement for L in $\tilde{L}$. Let $N < G$ be the group fixing M; this is a normal subgroup with $\mathrm{Gal}(M/K) = G/N$, and the intersection $N \cap G'$ is trivial. Better than that: G is the semidirect product $N \rtimes G'$. In the above example, the field M is $\mathbb{Q}(\zeta_p)$, and G is the semidirect product of two cyclic groups, the one of order $p-1$ acting on the one of order p, which is normal.

Let $P \subset \mathrm{Perm}(G/G')$ be the set (= subgroup) of all left translations λ_ν with $\nu \in N$. Recall $\Lambda = \{\lambda_\gamma : \gamma \in \Gamma\} \subset \mathrm{Perm}(G/G')$.

Proposition 2.3.1. *The group P acts simply transitively on G/G', and it is normalized by Λ. Therefore we obtain a Hopf-Galois object $L \longrightarrow L \otimes H$, where the Hopf algebra H belongs to the abstract group P with Γ-action via Λ.*

Proof. We first show that the action is transitive. It suffices that we can reach every class gU from $U = 1_G\dot{G}'$, by applying an element of P. Indeed we can decompose $g = \nu u$ with $\nu \in N$ and $u \in G'$, and then $\lambda_n u(1_G G') = \nu \cdot 1_G \cdot G') = \nu G' = gG'$. The uniqueness of ν is shown similarly; it follows from the fact that G' and N intersect trivially. Finally, P is normalized by Λ, because $\lambda_g \lambda_\nu \lambda_{g^{-1}} = \lambda_{g\nu g^{-1}}$, and $g\nu g^{-1} \in N$ since N is normal in G. □

Example 2.3.2. We revisit $L = \mathbb{Q}(\sqrt[p]{a})$ with hypotheses as before. Here we may take $M = \mathbb{Q}(\zeta_p)$, which is a normal (even abelian) extension of $\mathbb{Q}$ with degree $p-1$, so $M \cap L = \mathbb{Q}$, and we have already used that $ML = \widetilde{L} = L(\zeta_p)$ is the normal closure of $L/\mathbb{Q}$. The resulting Hopf-Galois structure coming from this "almost classical" setup is the same as the one explained before. Recall that the Γ-action on the cyclic group N of order p is the cyclotomic action.

Example 2.3.3. We take any non-normal cubic extension L/K. Then the Galois group G of $\widetilde{L}/K$ must be a copy of the symmetric group S_3, and $G' < G$ must be generated by a transposition. So we can take N to be the unique subgroup of order 3 in S_3; it is normal as is well known. Let us pin this down: "All cubic extensions are Hopf-Galois" (and even almost classically so).

Motivated by the last example, let us mention that there are extensions L/K which are not Hopf-Galois at all. Indeed there are many, but let us just discuss one class of examples. Let L/K be of degree 5 such that $\widetilde{L}/K$ has Galois group G isomorphic to the alternating group A_5. Then $S = G/G'$ is a 5-element set, on which G acts transitively, and in particular not trivially. So the resulting group homomorphism $\lambda : A_5 \cong G \longrightarrow \mathrm{Perm}(S)$ is a nontrivial homomorphism defined on a simple group, and therefore injective (the kernel is always a normal subgroup). That is, Λ is a copy of A_5 lying in $\mathrm{Perm}(S) \cong S_5$. So Λ is a subgroup of index 2 in S_5, hence normal; hence it contains all 5-cycles (look at the image in the group S_5/Λ of order 2). In fact Λ *is* A_5, but we don't need this. Now assume L/K is Hopf-Galois; this gives a simply transitive subgroup $N < \mathrm{Perm}(S)$ normalized by Λ. But then N has order 5, so it actually lies in Λ. On the other hand the simple group Λ does not normalize any nontrivial subgroup, contradiction.

3.2 The Byott translation

We keep the following setup: $\widetilde{L}$ is the normal closure of the finite extension L/K; the Galois group of $\widetilde{L}/K$ is G; and the subgroup belong to L is $G' < G$. Then G' contains no nontrivial normal subgroup of G, since otherwise $\widetilde{L}$ would not be the minimal normal over-field of L. One may always think of the example where $G = S_n$, and G' is the subgroup of all permutations that fix 1; then $S = G/G'$ identifies with $\{1, \ldots, n\}$; the dimensions are $[L : K] = n$ and $[\widetilde{L} : K] = n!$.

If one wants to exploit GP theory fully, it is hard to find the eligible subgroups $\Pi \subset S = \mathrm{Perm}(G/G')$. Byott's clever idea is to start with Π and look for G instead. Of course this takes some explanation: what is the suitable structure inside of which we may look for G? It is certainly not Π itself, that would be too simple. We begin with some abstract group theory, omitting the proofs of statements which will not really be used. In the following, let X be any group and $f : X \longrightarrow X$ be any bijective map. By $\mathrm{Aut}(X)$ we denote the set of all group automorphisms of X; this is again a group, under composition. For $x \in X$, the map $c_x : X \longrightarrow X$, $y \longmapsto xyx^{-1}$ is in $\mathrm{Aut}(X)$, and called conjugation by x. Recall that λ_v is left translation by an element $v \in X$.

Lemma 2.3.4. *The following are equivalent:*

(i) $f(xy^{-1}z) = f(x)f(y)^{-1}f(z)$, *for all* $x, y, z \in X$.

(ii) f *can be written* $f = \lambda_u \circ \phi$ *for some* $\phi \in \mathrm{Aut}(X)$, $u \in X$.

(iii) f *can be written* $f = \phi \circ \lambda_v$ *for some* $\phi \in \mathrm{Aut}(X)$, $v \in X$.

Proof. Most of the proof is easy and left to the reader. A few hints: Going from (ii) to (iii), ϕ stays the same, but v is not the same as u (what is it, exactly?) The implication (ii) to (i) is a calculation. Let us show how (i) $\implies$ (ii).

First step: The set of bijections f satisying (i) is closed under composition. (Fairly obvious.)

Second step: Every left multiplication λ_d satisfies (i). (Quick calculation.)

Final step: Assume f satisfies (i). Let $d = f(e_X)$ and put $g = \lambda_{d^{-1}} \circ f$. Then g again satisfies (i), and it has the extra property that it maps the neutral element e_X to itself. Putting $y = e_X$ in the equality (i), we get that g is a homomorphism of groups. □

Definition 2.3.5. *The subset of* $\mathrm{Perm}(X)$ *consisting of all* f *that satisfy one of the three conditions of the lemma is called the holomorph* $\mathrm{Hol}(X)$. *As already said, this subset is closed under composition, and in fact it is a subgroup.*

It is easily seen that the decomposition in item (ii) of the lemma is unique. If Λ_X denotes the subgroup of all λ_x, $x \in X$, then Λ_X is normalized by $\mathrm{Aut}(X)$ (see the exercises), and we get a representation of the holomorph as a semidirect product:

$$\mathrm{Hol}(X) = \Lambda_X \rtimes \mathrm{Aut}(X).$$

For later use we need a sharpening of this statement.

Proposition 2.3.6. $\mathrm{Hol}(X)$ *is the exact normalizer of* Λ_X *in* $\mathrm{Perm}(X)$.

Proof. We already know that $\mathrm{Aut}(X)$ normalizes Λ_X, and of course Λ_X normalizes itself. Putting these together we have that $\mathrm{Hol}(X)$ normalizes Λ_X. The point is to show the reverse inclusion. Assume f normalizes Λ_X. As in the proof of the lemma we write $f = \lambda g$, where λ is left multiplication by a suitable element, and g fixes $e = e_X$. Then g also normalizes Λ_X. Let us show that g is an automorphism. For any $x \in X$ there is $x' \in X$ such that $g\lambda_x g^{-1} = \lambda_{x'}$. Evaluating this in e we get $g(x) = x'$, so for all x we have the rule $g\lambda_x g^{-1} = \lambda_{g(x)}$. Now we take $x, y \in X$ and evaluate $w := g\lambda_{xy}g^{-1}$ two ways:

$$w = g\lambda_x g^{-1} g\lambda_y g^{-1} = \lambda_{g(x)}\lambda_{g(y)} = \lambda_{g(x)g(y)};$$

and

$$w = \lambda_{g(xy)}.$$

Evaluating w in e and using both these equalities shows that $g(x)g(y) = g(xy)$ as desired. □

A good example for this is given by the cyclic group $X = C$ of order p; we identify C with $\mathbb{Z}/p\mathbb{Z}$. The left multiplications (rather: additions!) Λ_C are then all the powers (rather: multiples) of the p-cycle $(0\,1\,\ldots\,p-1)$; this is again a copy of $\mathbb{Z}/p\mathbb{Z}$. The automorphisms of C are given as multiplications by integers prime to p; so $\mathrm{Aut}(C)$ is a copy of the unit group $\mathbb{Z}/p\mathbb{Z}^*$. The holomorph of C is a non-abelian group of order $p(p-1)$, and it is the exact normalizer of Λ_C.

Before reading on, please review the main result of GP theory. In the sequel we will write N instead of Π, to conform with the literature. The main idea of Byott is, very roughly: instead of having N permute G/G', we let a copy of G permute N. We set up some notation, and then we formulate and prove Byott's result. We keep the assumption that G is a finite group, G' a subgroup, and G' contains no nontrivial

normal subgroup of G. Moreover we still assume that N is a group of order $|G/G'|$. Define

$$\mathcal{N} = \{\alpha : N \longrightarrow \mathrm{Perm}(G/G') : \alpha(N) \text{ simply transitive}\};$$

and

$$\mathcal{G} = \{\beta : G \longrightarrow \mathrm{Perm}(N) : \beta(G') \text{ is the stabilizer of } e_N\}.$$

Theorem 2.3.7. *1. There is an explicit bijection between the sets $\mathcal{N}$ and $\mathcal{G}$ (described in the proof).*

2. If $\alpha \in \mathcal{N}$ corresponds to $\beta \in \mathcal{G}$ under that bijection, then $\alpha(N)$ is normalized by Λ_G if and only if $\beta(G)$ is contained in $\mathrm{Hol}(N)$.

Before we come to the proof, let us quickly explain why this is so useful: While $\mathrm{Perm}(G/G')$ is in general much larger that G/G', the holomorph $\mathrm{Hol}(N)$, while larger than N, is much smaller, comparatively seen.

Proof. As a small preparation, we observe that any bijection of sets $a : X \longrightarrow X'$ induces another bijection $Ca : \mathrm{Perm}(X) \longrightarrow \mathrm{Perm}(X')$, simply by putting $Ca(\pi) = a \circ \pi \circ a^{-1}$. (You might draw a little diagram for yourself, to visualize this.) – Moreover we will need that the left-multiplication map $\lambda : G \to \mathrm{Perm}(G)$ is injective. Indeed its kernel is normal in G, and contained in G', hence trivial, as said at the beginning of this subsection.

(a) We explain how α turns into β. Let α be given; by assumption it induces a bijection $a : N \longrightarrow G/G'$, via $a(\eta) = \alpha(\eta)(eG')$. Let $\lambda : G \longrightarrow \mathrm{Perm}(G/G')$ be our well-known left translation map, and define

$$\beta = Ca^{-1} \circ \lambda : \quad G \longrightarrow \mathrm{Perm}(G/G') \longrightarrow \mathrm{Perm}(N).$$

Then β is injective, as λ is injective (its kernel is normal in G and contained in G'), and Ca even bijective. The stabilizer of e_N under G (via β) is the stabilizer of eG' under G (via λ), and this is evidently G'. So the new map β is in the set $\mathcal{G}$.

(b) As a technical point, we claim and prove that $Ca^{-1} \circ \alpha : N \longrightarrow \mathrm{Perm}(N)$ is the same as the left translation map λ_N. This comes down to checking the commutativity of the following diagram for $\eta \in N$:

$$\begin{array}{ccc} G/G' & \xrightarrow{\alpha(\eta)} & G/G' \\ {\scriptstyle a}\uparrow & & \uparrow{\scriptstyle a} \\ N & \xrightarrow{\lambda_\eta} & N. \end{array}$$

We start with $\nu \in N$ in the southwest corner. For clarity, denote the class $e_G G'$ by $\bar{e}$. Going up and right, we get $\alpha(\nu)\bar{e}$, and then $\alpha(\eta)\alpha(\nu)\bar{e}$. Going first right and then up, we get $\eta\nu$ and then $\alpha(\eta\nu)\bar{e}$, and this is the same.

(c) Now we explain how β turns into α. Let $\beta : G \longrightarrow \mathrm{Perm}(N)$ be given with the indicated property. Then the orbit of e_N under G must be all of N, since G' is the stabilizer of e_N and the sets N and G/G' have the same cardinality.

This gives rise to a new bijection $b : G/G' \longrightarrow N$ via $gG' \longmapsto \beta(g)e_N$. As above, this induces the bijection $Cb : \mathrm{Perm}(G/G') \longrightarrow \mathrm{Perm}(N)$, and we put $\alpha = Cb^{-1} \circ \lambda_N : \quad N \longrightarrow \mathrm{Perm}(N) \longrightarrow \mathrm{Perm}(G/G')$. Again, we get immediately that the map α is injective. The image $\alpha(N)$ is simply transitive, because Λ_N is a simply transitive subgroup of $\mathrm{Perm}(N)$. Therefore $\alpha \in \mathcal{N}$ as required.

(d) The two constructions, from α to β, are mutually inverse: here we will be a bit shorter, and just say that if α leads to β, then the described bijections a and b are inverses of each other, and this is enough for checking that then β leads back to α.

(e) Now comes the final and central point: the equivalence of the additional property of α with that of β. – Assume first that $\alpha(N)$ is normalized by Λ_G, and β is constructed out of α as explained in step (1) above. Then $Ca^{-1}\alpha(N)$ is normalized by $Ca^{-1}\Lambda_G = \beta(G)$; by (2) we have $Ca^{-1}\alpha(N) = \lambda(N)$, and so $\lambda(N)$ is normalized by $\beta(G)$. By the proposition above (before the theorem), we conclude that $\beta(G) \subset \mathrm{Hol}(N)$. – Now assume that β is given, α is derived from it as explained in (c), and that $\beta(G) \subset \mathrm{Hol}(N)$. This says: $\lambda(N)$ is normalized by $\beta(G)$. Quite similarly as just before, this gives that $Cb^{-1}\lambda(N)$ is normalized by $Cb^{-1}\beta(G)$. The former is $\alpha(N)$ by construction; the latter is $\lambda(G)$, by the same technical argument as in (b) above. This shows the required extra condition on α.

□

Example 2.3.8. Let L/K be Galois in the classical sense. Then $\widetilde{L} = L$; $G = \mathrm{Gal}(L/K)$, and G' is trivial. This situation will be studied a lot later, but for now let us assume that G has order p (a prime number). We claim that there is only one Hopf-Galois structure for L/K. Indeed: in Byott's translation, the "other" group N must also be (cyclic) of order p. Therefore G must embed in $\mathrm{Hol}(N)$, which is known to us: it is the semidirect product of an order p group (which is normal) by a group or order $p-1$. Hence the p-Sylow subgroup of $\mathrm{Hol}(N)$ is normal, and unique, so there is only one choice for G. Thus there is only one choice on the other side (GP theory) as well, and it must be the classical one.

Example 2.3.9. Let $N = C_2 \times C_2$ (the non-cyclic group of order 4, which can also be seen as the two-dimensional $\mathbb{F}_2$-vectorspace). Then $\mathrm{Aut}(N) = \mathrm{GL}_2(\mathbb{F}_2)$ is non-abelian of order 6, and $\mathrm{Hol}(N)$ has order 24. As $\mathrm{Perm}(N)$ has only 24 elements as well, we have $\mathrm{Hol}(N) = \mathrm{Perm}(N)$. If we identify $\mathrm{Perm}(N)$ with S_4 (the details do not matter), any 4-cycle in $\mathrm{Hol}(N)$ generates a simply transitive subgroup G. That is: Every *cyclic* extension L/K of degree 4 admits a Hopf-Galois structure in which the involved group N is (of order 4 of course but) *non-cyclic.*

To finish this section we discuss a larger class of field extensions.

Theorem 2.3.10. *Assume $[L : K]$ is a prime number p, and let $G = \mathrm{Gal}(\widetilde{L}/K)$ as usual. Then L/K admits a Hopf-Galois structure if and only if G is solvable, and the latter happens exactly if G is a semidirect product $C \rtimes \Delta$, where C is of order p and Δ is a cyclic group of order dividing $p-1$.*

Proof. Assume that L/K has a Hopf-Galois structure. The group N such that G embeds into $\mathrm{Hol}(N)$ is also of order p, so $\mathrm{Hol}(N)$ is our old acquaintance $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}^*$, which is solvable. Hence G is also solvable, as a subgroup of a solvable group. Conversely, assume that G is solvable. By general Galois theory, G is a transitive subgroup of S_p, and (in particular) p divides $|G|$. By the Sylow theorem G contains a subgroup P of order p.

The following result is due to Galois; it is mentioned but not proved in the book of Childs [Chi00]. We will give a proof at the end of the section. Here is the statement.

Theorem 2.3.11 (Galois)**.** *A solvable subgroup G of S_p that contains an order p subgroup P is already contained in the normalizer of P, which can be identified with the holomorph of P.*

Now we assume the validity of the theorem: this shows our Galois group G lies between P and $\mathrm{Hol}(P)$, for a cyclic group P, and then we only have to take $N = P$ and appeal to the Byott translation. □

Proof. (of Theorem 2.3.11.) Assume the contrary, that is, P is not normal in G. As p^2 does not divide $|S_p|$, the subgroup P is a p-Sylow subgroup; if it is not normal, then G contains two (or more) subgroups of order p. The case $|G| = p$ (hence $G = P$) cannot occur. As G is solvable, G then contains a nontrivial subgroup H which is normal. Under the action of H, the set $\{1, \ldots, p\}$ splits up into disjoint orbits, which cannot all be trivial (singletons). On the other hand, G acts transitively on this orbit decomposition, so all H-orbits are of the same length. As p is prime, this is only possible if there is only one orbit, in other words: already H is transitive. Hence p divides $|H|$, and we can pick an order-p subgroup P' in H. Then P' is G-conjugate to all subgroups of order p in G, and there is more than one of them. As $P' \subset H$ and H is normal, all these conjugates lie already in H. We have shown: the statement "more than one subgroup of order p" is inherited from G down to H. But H is strictly smaller, and we may repeat the argument indefinitely. As our groups are finite, this is a contradiction. □

4 The Greither-Pareigis correspondence revisited

This section revolves around Theorem 2.2.16, the one commonly known as Greither-Pareigis theorem. In a few lines, if K is a field with algebraic closure $\overline{K}$ and $\Gamma = \mathrm{Gal}(\overline{K}/K)$, the theorem establishes that the equivalence from Section 2.1 between the categories $\mathcal{A}_K$ (finite-dimensional commutative K-algebras without nilpotent elements) and $\mathcal{S}_\Gamma$ (finite Γ-sets) defined by the maps Φ and Ψ restricts to a bijective correspondence between the Hopf-Galois structures on a separable extension of K with fixed subgroup Γ' and the simply transitive subgroups of $\mathrm{Perm}(\Gamma/\Gamma')$ normalized by left translations of Γ/Γ'. Most of the importance in this result lies in the fact that it ties the determination of Hopf-Galois structures on separable extensions with group theory. In this section, we will reformulate the theorem in a way that is more convenient for many applications, and we shall see the explicit form of the correspondence.

4.1 An alternative glance to the main theorem

We start by rewriting Theorem 2.2.16 in a convenient way to work with.

Let L/K be a separable field extension with algebraic closure $\overline{K}$. Call $\Gamma = \mathrm{Gal}(\overline{K}/K)$ and $\Gamma' = \mathrm{Gal}(\overline{L}/L)$. As already mentioned, Greither-Pareigis theorem establishes an one-to-one correspondence between Hopf-Galois structures on L/K and the subgroups of $\mathrm{Perm}(\Gamma/\Gamma')$ that are simply transitive and normalized by the set $\overline{\Lambda}$ of left translations by elements $\gamma \in \Gamma$.

First, simply transitive subgroups of $\mathrm{Perm}(\Gamma/\Gamma')$ are, by definition, those whose group action on Γ/Γ' is simply transitive. From now on, we shall refer to such subgroups as **regular**. For later use, we see some characterizations of this concept.

Proposition 2.4.1. *Let X be a finite set and let N be a subgroup of $\mathrm{Perm}(X)$. Consider the group action of N on X defined by evaluation. If two of the following three conditions are satisfied, so is the other one.*

1. $|N| = |X|$.
2. *N acts transitively on X.*
3. *Given $x \in X$, $\mathrm{Stab}_N(x) = \{\eta \in N \mid \eta(x) = x\} = \{1_N\}$.*

Proof. Fix $x \in X$. By the orbit-stabilizer theorem, we have $|N| = |\mathrm{Orb}(x)|\,|\mathrm{Stab}_N(x)|$. Now, let us note that 2 is equivalent to $|\mathrm{Orb}(x)| = |X|$ and 3 is equivalent to $|\mathrm{Stab}_N(x)| = 1$. Then the statement follows immediately. □

If X is a finite set and N is a subgroup of $\mathrm{Perm}(X)$, for each $x \in X$ we consider the map $\varphi_x \colon N \longrightarrow X$ defined by $\varphi_x(\eta) = \eta \cdot x$.

Proposition 2.4.2. *Let X be a finite set and let N be a subgroup of $\mathrm{Perm}(X)$. The following conditions are equivalent.*

1. *N is a regular subgroup of $\mathrm{Perm}(X)$.*
2. *Two of the conditions from Proposition 2.4.1 are satisfied.*
3. *The conditions from Proposition 2.4.1 are satisfied.*
4. *There is some $x \in X$ such that φ_x is bijective.*
5. *For every $x \in X$, φ_x is bijective.*

Proof. The equivalence between 2 and 3 has been already shown in Proposition 2.4.1.

Suppose that 1 holds, so that N acts simply transitively on X. In particular, the action is transitive. Let us fix $x \in X$. Then, for each $y \in X$ there is a unique $\eta_y \in N$ such that $\eta_y(x) = y$. By the uniqueness, the η_y define $|X|$ different elements in N, and they are all the elements of N (given $\eta \in N$, $\eta = \eta_{\eta(x)}$), so $|N| = |X|$. Hence 2 is satisfied. Conversely, assume that 3 holds. Let $x, y \in X$. Since N acts transitively on X, there is $\eta \in N$ such that $\eta(x) = y$. Suppose that $\mu \in N$ is such that $\mu(x) = y$. Then $\eta(x) = \mu(x)$, whence $\eta^{-1}\mu(x) = x$, that is, $\eta^{-1}\mu \in \mathrm{Stab}_N(x) = \{1_N\}$. Hence $\eta = \mu$, proving that the action is simply transitive.

Let us prove that 1 and 5 are equivalent. Given $x \in X$, we have that the map φ_x is bijective if and only if there is a unique $\eta \in N$ such that $\eta \cdot x = y$, whence the

claim follows. On the other hand, it is trivial that 5 implies 4. Finally, assume that 4 is satisfied, so that for some $x \in X$, φ_x is bijective. Then for each $y \in X$ there is a unique $\eta \in N$ such that $\eta \cdot x = y$, so N acts simply transitively on X and 1 holds. □

On the other hand, in Section 3, we have used an alternative quotient set G/G' of Galois groups, that comes from choosing the normal closure of our separable extension L/K, instead of its algebraic closure. This is valid because the left cosets of Γ/Γ' and G/G' can be identified. In the following we offer a complete proof for the validity of this step.

Proposition 2.4.3. *Let L/K be a finite and separable extension of fields and let E/K be a Galois extension with $L \subset E$. Call $G_E = \mathrm{Gal}(E/K)$ and $G'_E = \mathrm{Gal}(E/L)$. The Hopf-Galois structures on L/K are in bijective correspondence with the regular subgroups of $\mathrm{Perm}(G_E/G'_E)$ normalized by the set Λ of left translations by elements $g \in G$.*

Proof. We know by Theorem 2.2.16 that the Hopf-Galois structures on L/K are in bijective correspondence with the regular subgroups of $\mathrm{Perm}(\Gamma/\Gamma')$ normalized by the set $\overline{\Lambda}$ of left translations by elements $\gamma \in \Gamma$. We shall prove that the latter are in bijective correspondence with the regular subgroups of $\mathrm{Perm}(G_E/G'_E)$ normalized by Λ, whence the statement will follow.

Since E/K is Galois, by Theorem 1.1.58, $G(E) := \mathrm{Gal}(\overline{L}/E)$ is a normal subgroup of Γ and the restriction maps $\Gamma \longrightarrow G_E$, $\Gamma' \longrightarrow G'_E$ induce group isomorphisms

$$\Gamma/G(E) \cong G_E, \quad \Gamma'/G(E) \cong G'_E.$$

Then, the map $\varphi\colon \Gamma/\Gamma' \longrightarrow G_E/G'_E$ defined by $\varphi(\gamma\Gamma') = \gamma \mid_E G'_E$ is bijective. At the same time, such a map induces a group isomorphism $\Phi\colon \mathrm{Perm}(\Gamma/\Gamma') \longrightarrow \mathrm{Perm}(G_E/G'_E)$ defined as $\Phi(\eta)(\varphi(\gamma\Gamma')) = \varphi(\eta(\gamma\Gamma'))$. It is enough to check that a subgroup of $\mathrm{Perm}(\Gamma/\Gamma')$ is regular and normalized by $\overline{\Lambda}$ if and only if it is mapped by Φ to a regular subgroup of $\mathrm{Perm}(G_E/G'_E)$ normalized by Λ.

Let N be a regular subgroup of $\mathrm{Perm}(\Gamma/\Gamma')$ and let us prove that $\Phi(N)$ is regular. Let $a, b \in G_E/G'_E$ and write $x = \varphi^{-1}(a)$ and $y = \varphi^{-1}(b)$. Since N is regular and $x, y \in \Gamma/\Gamma'$, there is a unique $\eta \in N$ such that $\eta(x) = y$. Now, $\Phi(\eta)(a) = \Phi(\eta)(\varphi(x)) = \varphi(\eta(x)) = \varphi(y) = b$. The uniqueness of $\Phi(\eta)$ follows from the bijectivity of Φ. Hence $\Phi(N)$ is regular. The converse is proved in the same way.

Let N be a subgroup of $\mathrm{Perm}(\Gamma/\Gamma')$ normalized by $\overline{\Lambda}$. Given $\gamma, \mu \in \Gamma$, we have

$$\lambda_{\gamma|_E} \circ \varphi(\mu\Gamma') = \lambda_{\gamma|_E}(\mu \mid_E G'_E) = (\gamma\mu) \mid_E G'_E = \varphi(\gamma\mu\Gamma') = \varphi \circ \lambda_\gamma(\mu\Gamma').$$

Since μ is arbitrary, we obtain that $\lambda_{\gamma|_E} \circ \varphi = \varphi \circ \lambda_\gamma$. Let us check that $\lambda_{\gamma|_E} \circ \Phi(N) \circ \lambda_{\gamma|_E}^{-1} \subseteq \Phi(N)$. Let $\eta \in N$. For an arbitrary $g \in G_E$, let $\mu \in \Gamma$ be such that $g = \mu \mid_E$. Then

$$\begin{aligned}
\lambda_{\gamma|_E} \circ \Phi(\eta) \circ \lambda_{\gamma|_E}^{-1}(gG'_E) &= \lambda_{\gamma|_E} \circ \Phi(\eta)((\gamma^{-1}\mu) \mid_E G'_E) \\
&= \lambda_{\gamma|_E} \circ \Phi(\eta)(\varphi(\gamma^{-1}\mu\Gamma')) \\
&= \lambda_{\gamma|_E} \circ \varphi \circ \eta(\gamma^{-1}\mu\Gamma') \\
&= \varphi \circ \lambda_\gamma \circ \eta \circ \lambda_{\gamma^{-1}}(\mu\Gamma') \\
&= \Phi(\lambda_\gamma \circ \eta \circ \lambda_{\gamma^{-1}})(\varphi(\mu\Gamma')) \\
&= \Phi(\lambda_\gamma \circ \eta \circ \lambda_{\gamma^{-1}})(gG'_E).
\end{aligned}$$

Since g is arbitrary, $\lambda_{\gamma|_E} \circ \Phi(\gamma) \circ \lambda_{\gamma|_E}^{-1} = \Phi(\lambda_\gamma \circ \eta \circ \lambda_{\gamma^{-1}})$. Now, since N is normalized by left translations by hypothesis, we have $\lambda_\gamma \circ \eta \circ \lambda_{\gamma^{-1}} \in N$, so $\lambda_{\gamma|_E} \circ \Phi(\gamma) \circ \lambda_{\gamma|_E}^{-1} \in \Phi(N)$, as we wanted. We conclude that $\Phi(N)$ is normalized by Λ. The converse is proved likewise. □

Proposition 2.4.3 means that, in order to characterize Hopf-Galois structures on a separable extension L/K in terms of permutation subgroups, instead of choosing an algebraic closure to construct the Galois groups Γ and Γ', we can just choose any finite and Galois extension of E containing L, and choose the corresponding Galois groups G_E and G'_E.

The remaining ingredient concerning Theorem 2.2.16 is left translations of Γ/Γ'. We have proved in Proposition 2.4.3 that, for any Galois extension E of K containing L, we can consider instead the set of left translations $\lambda_g \colon hG'_E \mapsto ghG'_E$ of G_E/G'_E, where G_E and G'_E are in the statement of that result. We can regard this as the image of a map.

Definition 2.4.4. *Let L/K be a finite and separable extension, let E/K be a Galois extension with $L \subset E$ and acquire the above notation. The **left translation map** of L/K associated to E is the map*

$$\begin{array}{rccc} \lambda_E \colon & G_E & \longrightarrow & G_E/G'_E \\ & g & \longrightarrow & hG'_E \mapsto ghG'_E \end{array}$$

The left translation map is not in general injective, and its kernel can be characterized in terms of group theory.

Definition 2.4.5. *Let G be a group and let G' be a subgroup of G. The **core** of G' inside G is defined as*

$$\mathrm{Core}_G(G') = \bigcap_{g \in G} gG'g^{-1}.$$

In other words, it is the greatest normal subgroup of G contained in G'.

Proposition 2.4.6. *Let L/K be a finite and separable extension, and let E/K be a Galois extension with $L \subseteq E$. Call $G_E = \mathrm{Gal}(E/K)$, $G'_E = \mathrm{Gal}(E/L)$, and let $\lambda_E \colon G_E \longrightarrow G_E/G'_E$ be the left translation map of L/K associated to E. Then*

$$\mathrm{Ker}(\lambda_E) = \mathrm{Core}_{G_E}(G'_E).$$

Proof. Let $h \in G_E$. We have that

$$\begin{aligned} h \in \mathrm{Ker}(\lambda_E) &\iff \lambda_E(h) = \mathrm{Id}_{G_E/G'_E} \\ &\iff hgG'_E = gG'_E \text{ for all } g \in G_E \\ &\iff g^{-1}hgG'_E = G'_E \text{ for all } g \in G_E \\ &\iff h \in gG'_Eg^{-1} \text{ for all } g \in G_E \\ &\iff h \in \mathrm{Core}_{G_E}(G'_E) \end{aligned}$$

□

Let L/K be a finite and separable field extension. Note that the smallest field E such that $L \subset E$ is by definition the normal closure $\widetilde{L}$ of L/K. This will be our preferred choice when we make use of Greither-Pareigis theorem. Call $G = \mathrm{Gal}(\widetilde{L}/K)$ and $G' = \mathrm{Gal}(\widetilde{L}/L)$. In short, we will say that L/K is (G, G')-*separable* or G-*separable*. In this case, the left translation map $\lambda\colon G \longrightarrow G/G'$ of L/K associated to $\widetilde{L}$ is simply called the left translation map of L/K. If no more quotient groups arise, we will normally write left cosets of G/G' as $\overline{g}$ for a representative $g \in G$. Thus, for $g, h \in G$, $\lambda(g)(\overline{h}) = \lambda_g(\overline{h}) = \overline{gh}$.

Corollary 2.4.7. *The left translation map λ of a (G, G')-separable extension L/K is injective.*

Proof. We know from Proposition 2.4.6 that $\mathrm{Ker}(\lambda) = \mathrm{Core}_G(G')$, which is by definition the greatest normal subgroup of G contained in G'. By definition of normal closure, $\widetilde{L}$ is the smallest Galois field extension of K containing L. In other words, there are no Galois extensions of K containing L and properly contained in $\widetilde{L}$. Applying the Galois correspondence, we get that there are no non-trivial normal subgroups of G contained in G'. That is, $\mathrm{Core}_G(G') = \{\overline{1_G}\}$, proving the statement. □

Let us focus on the normality condition for a permutation subgroup at the Greither-Pareigis correspondence. Let L/K be a (G, G')-separable extension and let $\lambda\colon G \longrightarrow \mathrm{Perm}(G/G')$ be its left translation map. Since λ is injective, G is isomorphic with its image $\lambda(G)$, which is a subgroup of $\mathrm{Perm}(G/G')$. We have an action of G on $\mathrm{Perm}(G/G')$ by letting $\lambda(G)$ act by conjugation:

$$g \cdot \eta := \lambda(g)\eta\lambda(g^{-1}), \quad \eta \in \mathrm{Perm}(G/G').$$

The condition that a subgroup N of $\mathrm{Perm}(G/G')$ is normalized by the left translations is just that this action restricts to N.

Definition 2.4.8. *Let N be a subgroup of $\mathrm{Perm}(G/G')$. We say that N is G-**stable**, or that N is normalized by $\lambda(G)$, if for every $g \in G$ and $\eta \in N$,*

$$\lambda(g)\eta\lambda(g^{-1}) \in N,$$

that is, $\lambda(G)$ acts on N by conjugation.

Under this terminology, we can restate Theorem 2.2.16 as follows.

Theorem 2.4.9. *Let L/K be a (G, G')-separable extension. Then, there is a bijective correspondence between:*

1. *The Hopf-Galois structures on L/K.*
2. *The regular and G-stable subgroups of $\mathrm{Perm}(G/G')$.*

We also give a term for an concept that has already appeared; namely, the isomorphism class of a permutation subgroup corresponding to a Hopf-Galois structure on a separable extension.

Definition 2.4.10. *The **type** of a Hopf-Galois structure H on a (G, G')-separable extension is defined as the isomorphism class of the subgroup N of $\mathrm{Perm}(G/G')$ corresponding to H under the Greither-Pareigis correspondence. We denote it by $[N]$.*

We can classify Hopf-Galois structures on a separable extension according to their type. We saw that Byott's translation allows us to count Hopf-Galois structures of a given type on a separable extension.

4.2 The explicit form of the correspondence

Let L/K be a (G, G')-separable extension with normal closure $\widetilde{L}$. In this part we describe the definition of the bijective (and inverse-to-each-other) maps involved in the Greither-Pareigis correspondence. The following establishes a first relation between a Hopf-Galois structure H on L/K and its corresponding permutation subgroup N.

Proposition 2.4.11 ([GP87], Proposition 1.3)**.** *Let L/K be a (G, G')-separable extension with normal closure $\widetilde{L}$. Let H be a Hopf-Galois structure on L/K and let N be its corresponding regular and G-stable subgroup of* $\mathrm{Perm}(G/G')$*. Then $\widetilde{L} \otimes_K H \cong \widetilde{L}[N]$ as $\widetilde{L}$-Hopf algebras.*

First, we see how to recover H from N. To do so, we need some notions from Galois descent theory. First, it is easy to check that the K-Hopf algebras together with the homomorphisms of K-Hopf algebras form a category. The same is true for $\widetilde{L}$-Hopf algebras, but we shall consider a smaller category inside.

Let M be an $\widetilde{L}$-Hopf algebra. An $\widetilde{L}$-semilinear action of G on M is defined as a map $*\colon \widetilde{L}[G] \otimes_{\widetilde{L}} M \longrightarrow M$ such that for every $g \in G$, the map $g * -\colon M \longrightarrow M$ is $\widetilde{L}$-semilinear, that is, there is some field automorphism $\sigma_g \in \mathrm{Aut}(L)$ such that

$$g * (\lambda m) = \sigma_g(\lambda) g * m, \quad \lambda \in \widetilde{L},\ m \in M.$$

If there are $\widetilde{L}$-semilinear actions of G on $\widetilde{L}$-Hopf algebras M, M' respectively, an $\widetilde{L}$-linear map $f\colon M \longrightarrow M'$ is said to be G-equivariant if

$$g * f(m) = f(g * m), \quad g \in G,\ m \in M.$$

Definition 2.4.12. *Let M be an $\widetilde{L}$-Hopf algebra endowed with an $\widetilde{L}$-semilinear action from G. Consider the induced $\widetilde{L}$-semilinear action of G on $M \otimes_{\widetilde{L}} M$ as*

$$g * (m \otimes m') := (g * m) \otimes (g * m'), \quad g \in G,\ m, m' \in M.$$

We say that M is G-compatible if all the Hopf algebra operations of M are G-equivariant maps.

The G-compatible $\widetilde{L}$-Hopf algebras form a category where the morphisms are the G-equivariant $\widetilde{L}$-Hopf algebra homomorphisms.

Definition 2.4.13. *Let M be a G-compatible $\widetilde{L}$-Hopf algebra and write $*$ for the action of G on M. The sub-Hopf algebra of M fixed by G is*

$$M^G := \{m \in M \mid g * m = m\}.$$

The main result for our purposes is the following:

Theorem 2.4.14. *Let L/K be a separable extension with normal closure $\widetilde{L}$ and let $G = \mathrm{Gal}(\widetilde{L}/K)$.*

1. *If H is a K-Hopf algebra, then $\widetilde{L} \otimes_K H$ is a G-compatible $\widetilde{L}$-Hopf algebra.*
2. *If M is a G-compatible $\widetilde{L}$-Hopf algebra, then M^G is a K-Hopf algebra.*

Moreover, these assignments define an equivalence of categories between the category of K-Hopf algebras and the category of G-compatible $\widetilde{L}$-Hopf algebras.

This is explained at [Chi00, Paragraph before (2.13)].

As a consequence, for a G-compatible $\widetilde{L}$-Hopf algebra M, $\widetilde{L} \otimes M^G \cong M$ as G-compatible $\widetilde{L}$-Hopf algebras. Likewise, for a K-Hopf algebra H, $(\widetilde{L} \otimes_K H)^G \cong H$ as K-Hopf algebras.

Let N be a regular and G-stable subgroup of $\mathrm{Perm}(G/G')$. Let λ be the left translation map of L/K. That N is G-stable means that N is normalized by $\lambda(G)$, or equivalently, the conjugation action of G on $\mathrm{Perm}(G/G')$ leaves N invariant. We can easily extend this action to an $\widetilde{L}$-semilinear action of G on $\widetilde{L}[N]$ by letting G act on $\widetilde{L}$ by means of the usual Galois action and on N by the action above. Explicitly,

$$g * \Big(\sum_{i=1}^{n} h_i \eta_i \Big) = \sum_{i=1}^{n} g(h_i) \lambda(g) \eta_i \lambda(g^{-1}), \tag{2.1}$$

where $g \in G$, $n \in \mathbb{Z}_{>0}$ and, for each $1 \leq i \leq n$, $a_i \in \widetilde{L}$ and $\eta_i \in N$. This is indeed semilinear: if $g \in G$, $\lambda \in \widetilde{L}$ and $h = \sum_{i=1}^{n} h_i \eta_i \in \widetilde{L}[N]$, then

$$g * (\lambda h) = g * \Big(\sum_{i=1}^{n} \lambda h_i \eta_i \Big) = \sum_{i=1}^{n} g(\lambda) g(h_i) \lambda(g) \eta_i \lambda(g^{-1}) = g(\lambda) g * h.$$

Proposition 2.4.15. *Let L/K be a (G, G')-separable extension with normal closure $\widetilde{L}$. If N is a regular and G-stable subgroup of $\mathrm{Perm}(G/G')$, the $\widetilde{L}$-group algebra $\widetilde{L}[N]$ is a G-compatible $\widetilde{L}$-Hopf algebra with respect to the action $*$ of G on $\widetilde{L}[N]$ defined at (2.1).*

Proof. We need to check that the Hopf algebra operations of $\widetilde{L}[N]$ are G-equivariant.

- Multiplication: Given $h = \sum_{i=1}^{n} h_i \eta_i, h' = \sum_{j=1}^{n} h'_j \eta_j \in \widetilde{L}[N]$ and $g \in G$,

$$\begin{aligned}
g * m_{\widetilde{L}[N]}(h \otimes h') &= g * \sum_{i,j=1}^{n} h_i h'_j \eta_i \eta_j \\
&= \sum_{i,j=1}^{n} g(h_i h'_j) \lambda(g) \eta_i \eta_j \lambda(g^{-1}) \\
&= \sum_{i,j=1}^{n} g(h_i) g(h'_j) \lambda(g) \eta_i \lambda(g^{-1}) \lambda(g) \eta_j \lambda(g^{-1}) \\
&= \Big(\sum_{i=1}^{n} g(h_i) \lambda(g) \eta_i \lambda(g^{-1}) \Big) \Big(\sum_{j=1}^{n} g(h'_j) \lambda(g) \eta_j \lambda(g^{-1}) \Big) \\
&= (g * h)(g * h') \\
&= m_{\widetilde{L}[N]}((g * h) \otimes (g * h')) \\
&= m_{\widetilde{L}[N]}(g * (h \otimes h'))
\end{aligned} \tag{2.2}$$

- Unit: Given $r \in K$ and $g \in G$,

$$g * u_{K[G]}(r) = g * (r 1_G) = r 1_G = u_{K[G]}(g * r).$$

- Comultiplication: Let $h = \sum_{i=1}^{n} h_i\eta_i \in \widetilde{L}[N]$ and $g \in G$. Then,

$$\begin{aligned} g * \Delta_{\widetilde{L}[N]}(h) &= g * \Big(\sum_{i=1}^{n} h_i\eta_i \otimes \eta_i \Big) \\ &= \sum_{i=1}^{n} g(h_i)\lambda(g)\eta_i\lambda(g^{-1}) \otimes \lambda(g)\eta_i\lambda(g^{-1}) \\ &= \Delta_{\widetilde{L}[N]}\Big(\sum_{i=1}^{n} g(h_i)\lambda(g)\eta_i\lambda(g^{-1}) \Big) \\ &= \Delta_{\widetilde{L}[N]}(g * h). \end{aligned}$$

- Counit: For $h = \sum_{i=1}^{n} h_i\eta_i \in \widetilde{L}[N]$ and $g \in G$, we have

$$g * \varepsilon_{\widetilde{L}[N]}(h) = g * \Big(\sum_{i=1}^{n} h_i \Big) = \sum_{i=1}^{n} g(h_i) = \varepsilon_{\widetilde{L}[N]}(g * h)$$

- Coinverse: Again, given $h = \sum_{i=1}^{n} h_i\eta_i \in \widetilde{L}[N]$ and $g \in G$, we have

$$\begin{aligned} g * S_{\widetilde{L}[N]}(h) &= g * \sum_{i=1}^{n} h_i\eta_i^{-1} \\ &= \sum_{i=1}^{n} g(h_i)\lambda(g)\eta_i^{-1}\lambda(g^{-1}) \\ &= \sum_{i=1}^{n} g(h_i)(\lambda(g)\eta_i\lambda(g^{-1}))^{-1} \\ &= S_{\widetilde{L}[N]}(g * h). \end{aligned}$$

□

Taking into account Proposition 2.4.11, we obtain an explicit description for the underlying Hopf algebra. The action is also obtained by descent. We summarize what we get at the following.

Proposition 2.4.16. *Let L/K be a (G, G')-separable extension and let N be a regular and G-stable subgroup of* $\mathrm{Perm}(G/G')$. *Let H be the Hopf-Galois structure on L/K that corresponds to N under the Greither-Pareigis correspondence.*

1. *The underlying Hopf algebra of H is*

$$\widetilde{L}[N]^G = \{h \in \widetilde{L}[N] \mid g * h = h \text{ for all } g \in G\}.$$

2. *The action of H on L is given as follows: For $h = \sum_{i=1}^{n} h_i\eta_i \in H$ and $\alpha \in L$,*

$$h \cdot \alpha = \sum_{i=1}^{n} h_i\eta_i^{-1}(\overline{1})(\alpha), \tag{2.3}$$

where for each $1 \leq i \leq n$, $\eta_i^{-1}(\overline{1})(\alpha)$ is the image of α by a representative g of the left coset $\eta_i^{-1}(\overline{1}) \in G/G'$.

.

Let us check that the expression 2.3 is well defined. Take two representatives $g, k \in G$ of the left coset $\eta_i^{-1}(\overline{1})$ and an element $\alpha \in L$. Since g and k belong to the same left coset, $g^{-1}k \in G' = \mathrm{Gal}(\widetilde{L}/L)$, so $\alpha = g^{-1}k(\alpha)$, that is, $g(\alpha) = k(\alpha)$.

The correspondence in the converse direction follows easily from Proposition 2.4.11. Indeed, if H is a Hopf-Galois structure on a separable extension L/K with normal closure $\widetilde{L}$ and N is its corresponding subgroup, we have that $\widetilde{L} \otimes_K H \cong \widetilde{L}[N]$ as $\widetilde{L}$-Hopf algebras. By Corollary 1.2.19, N can be regarded as the group of grouplike elements of $\widetilde{L} \otimes_K H$.

4.3 The Greither-Pareigis theorem for Galois extensions

In this section we deepen in the specification of Greither-Pareigis theorem for Galois extensions from Section 2.4 so as to visualize the group-theoretical description of all their Hopf-Galois structures.

Let L/K be a Galois extension with group G. We know that $K[G]$ together with its classical action on L is a Hopf-Galois structure on L/K. We will often refer to this as the **classical Galois structure**.

By definition, the normal closure of L/K is $\widetilde{L} = L$. Thus, in this case, the groups G and G' appearing at the statement of Theorem 2.4.9 are $G = \mathrm{Gal}(L/K)$ and $G' = \{\mathrm{Id}_G\}$. In other words, L/K is $(G, \{\mathrm{Id}_G\})$-separable. Thus, Theorem 2.4.9 becomes:

Theorem 2.4.17. *Let L/K be a Galois extension with group G. There is a bijective correspondence between:*

- *The regular and G-stable subgroups of* $\mathrm{Perm}(G)$.
- *The Hopf-Galois structures on L/K.*

Let us specify what G-stable means in the Galois case. Following Definition 2.4.8, a subgroup $N \leq \mathrm{Perm}(G)$ is G-stable if the action of G on $\mathrm{Perm}(G)$ leaves N invariant. Such an action is defined by conjugation with the image of G by the left translation of L/K from Definition 2.4.4. Since $G' = \{1_G\}$, the left translation becomes

$$\begin{array}{rccl} \lambda\colon & G & \longrightarrow & \mathrm{Perm}(G), \\ & g & \longmapsto & \lambda(g)(h) = gh, \end{array}$$

which is nothing but the left regular representation of G into $\mathrm{Perm}(G)$. Thus, N being G-stable is just the condition that N is normalized by $\lambda(G)$.

The absence of G' allows us to consider an analogous map by the right side.

Definition 2.4.18. *Let L/K be a Galois extension with group G. The right regular representation of L/K is defined as the one of G, that is,*

$$\begin{array}{rccl} \rho\colon & G & \longrightarrow & \mathrm{Perm}(G), \\ & g & \longmapsto & \rho(g)(h) = hg^{-1}. \end{array}$$

The right regular representation ρ is clearly injective, as in the case of λ. In fact, $\rho(G)$ is the group of the right translations. Under this language, we have the following.

Proposition 2.4.19. *Let G be a group.*

1. *$\lambda(G)$ and $\rho(G)$ are regular subgroups of* $\mathrm{Perm}(G)$.
2. *$\rho(G)$ is centralized by $\lambda(G)$.*
3. *$\rho(G) = \lambda(G)$ if and only if G is abelian.*

As a consequence, $\lambda(G)$ and $\rho(G)$ are regular and G-stable subgroups, therefore giving Hopf-Galois structures on L/K.

Proposition 2.4.20 ([Chi00], (6.10))**.** *Let L/K be a Galois extension with group G. Then $\rho(G)$, as a regular and G-stable subgroup of* $\mathrm{Perm}(G)$*, corresponds to the classical Galois structure $(K[G], \cdot)$ on L/K.*

By Proposition 2.4.19 3, when G is abelian, $\lambda(G)$ and $\rho(G)$ give the same Hopf-Galois structure; otherwise they give two different Hopf-Galois structures.

Definition 2.4.21. *Let L/K be a Galois extension with group G and suppose that G is not abelian. The Hopf-Galois structure on L/K corresponding to $\lambda(G)$ is called the* ***canonical non-classical structure****.*

When both Hopf-Galois structures arise, we shall use the label H_c for the classical Galois structure, and write H_λ for the canonical non-classical structure.

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.

[GP87] C. Greither and B. Pareigis. "Hopf Galois theory for separable field extensions". In: *Journal of Algebra* 106.1 [1987], pp. 239–258. ISSN: 0021-8693. DOI: https://doi.org/10.1016/0021-8693(87)90029-9.

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

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