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

Introduction

Chapter 1

Preliminaries on Galois theory and Hopf algebras

1 Field theory and Galois theory

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

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

for which the expression

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

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

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

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

1.1 Finite and algebraic extensions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

There is the following basic result.

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

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

1.2 Subfield generated by a subset

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

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

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

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

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

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

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

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

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

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 $\alpha_1, \dots, \alpha_n \in L$ such that $L = K(\alpha_1, \dots, \alpha_n)$.*

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* min.poly.(α, 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*

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

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 $\tau \mid_K = \sigma$.*

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

1.5 Splitting fields and algebraic closure

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

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

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

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

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

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

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

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

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

This allows us to make the following definition.

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

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

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

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

1.6 Normal extensions

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

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

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

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

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

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

Example 1.1.30.

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

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

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

There is a notion of normal closure.

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

$$\begin{tikzcd}
L \arrow[r, hook] \arrow[dr, "\sigma"'] & N \arrow[d, "\tau"] \\
 & N'
\end{tikzcd}$$

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* min.poly.(α, 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 $S = \{\alpha_0, \dots, \alpha_{n-1}\}$ 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 $\alpha_1, \dots, \alpha_n$ 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*

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

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*

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

   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:

   $$\begin{tikzcd}
   H \otimes H \otimes H \arrow[r, "Id_H \otimes m_H"] \arrow[d, "m_H \otimes Id_H"'] & H \otimes H \arrow[d, "m_H"] \\
   H \otimes H \arrow[r, "m_H"] & H
   \end{tikzcd}$$

   (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:

   $$\begin{tikzcd}
   H \otimes R \arrow[r, "Id_H \otimes u_H"] \arrow[d, "s_2"'] & H \otimes H \arrow[dl, "m_H"'] \\
   H & R \otimes H \arrow[l, "s_1"] \arrow[u, "u_H \otimes Id_H"']
   \end{tikzcd}$$

   where $s_1\colon R \otimes H \longrightarrow H$ and $s_2\colon H \otimes R \longrightarrow H$ are defined by $s_1(r \otimes a) = r\,a = s_2(a \otimes r)$.

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

3. *$\Delta_H\colon H \longrightarrow H \otimes H$ and $\varepsilon_H\colon H \longrightarrow R$ are R-linear maps that satisfy:*

(a) **(Coassociative property)** *For all $h \in H$,*

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

Equivalently, there is a commutative diagram:

$$\begin{tikzcd}
H \otimes H \otimes H & & H \otimes H \arrow[ll, "\mathrm{Id}_H \otimes \Delta_H"'] \\
H \otimes H \arrow[u, "\Delta_H \otimes \mathrm{Id}_H"] & & H \arrow[ll, "\Delta_H"'] \arrow[u, "\Delta_H"']
\end{tikzcd}$$

(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:

$$\begin{tikzcd}
H \otimes R & & H \otimes H \arrow[ll, "Id_H \otimes \varepsilon_H"'] \arrow[d, "\varepsilon_H \otimes \mathrm{Id}_H"] \\
H \arrow[u, "- \otimes 1"] \arrow[urr, "\Delta_H"] \arrow[rr, "1 \otimes -"'] & & R \otimes H
\end{tikzcd}$$

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*

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

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:

$$\begin{tikzcd}
H \arrow[r, "f"] & H' \\
H \otimes H \arrow[u, "m_H"] \arrow[r, "f\otimes f"'] & H' \otimes H' \arrow[u, "m_{H'}"']
\end{tikzcd}
\qquad
\begin{tikzcd}
H \arrow[rr, "f"] & & H' \\
& R \arrow[lu, "m_H"] \arrow[ru, "m_{H'}"'] &
\end{tikzcd}$$

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

$$\begin{tikzcd}
H \arrow[r, "f"] \arrow[d, "\Delta_H"'] & H' \arrow[d, "\Delta_{H'}"] \\
H \otimes H \arrow[r, "f\otimes f"'] & H' \otimes H'
\end{tikzcd}
\qquad
\begin{tikzcd}
H \arrow[rr, "f"] \arrow[rd, "\Delta_H"'] & & H' \arrow[ld, "\Delta_{H'}"] \\
& R &
\end{tikzcd}$$

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

$$\begin{tikzcd}
H \arrow[r, "f"] \arrow[d, "S_H"'] & H' \arrow[d, "S_{H'}"] \\
H \arrow[r, "f"'] & H'
\end{tikzcd}$$

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

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

$$\begin{tikzcd} B \otimes B \arrow[r, "i\otimes \mathrm{Id}_B"] & H \otimes B \arrow[r, "\mathrm{Id}_H\otimes i"] & H \otimes H \end{tikzcd}$$

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

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

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

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

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

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

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

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

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

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

Then, B has a basis of the form

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

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

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

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

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

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

2.5 Sweedler's notation

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

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

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

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

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

On the other hand, the coassociative property gives

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

We denote this element by

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

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

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

Iterating this procedure, we write

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

for the unique element obtained by iterating coassociativity n times.

2.6 Grouplike elements

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

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

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

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

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

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

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

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

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

Theorem 1.2.18. *If R is an integral domain, $G(H)$ 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 is an integral domain 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 is an integral domain, 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 is an integral domain, 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 $h \in G(H)$,

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

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 is an integral domain, they are the only finitely generated and free R-Hopf algebras with this behaviour.

Corollary 1.2.21. *Suppose that R is an integral domain 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

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

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 $m_1, \dots, m_n \in M$, $f_1, \dots, f_n \in M^*$ 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 is an integral domain, 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 is an integral domain, $g(n) = 0$ 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 $m_{C^*} \colon C^* \otimes C^* \longrightarrow C^*$ defined by*

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

and unit map $u_{C^*} \colon R \longrightarrow C^*$ 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 homothecies 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 is an integral domain 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 $\Delta_C^* \mid_{C^* \otimes C^*}$, which is just the multiplication map m_{C^*}.

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

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

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

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

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

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

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

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

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

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

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

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

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

Indeed, let us write

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

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

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

as claimed. Hence

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

Likewise, it is proved that

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

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

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

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

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

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

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

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

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

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

Likewise,

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

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

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

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

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

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

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

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

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

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

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

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

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

- Given $h \in H$,

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

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

- Given $h \in H$ and $f \in H^*$,
$$S_{H^{**}} \circ \eta(h) = \eta(h) \circ S_{H^*}(f) = S_{H^*}(f)(h) = f \circ S_H(h) = \eta \circ S_H(h)(f).$$
Then $S_{H^{**}} \circ \eta = S_H$.

□

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

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

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

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

2.8 Modules and comodules

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

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

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

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

$$\begin{tikzcd}
H \otimes H \otimes A \arrow[r, "m_H \otimes \mathrm{Id}_A"] \arrow[d, "\mathrm{Id}_H \otimes \alpha"'] & H \otimes A \arrow[d, "\alpha"] \\
H \otimes A \arrow[r, "\alpha"] & H
\end{tikzcd}$$

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

$$\begin{tikzcd}
R \otimes A \arrow[d, "u_H \otimes \mathrm{Id}_A"'] \arrow[dr, "\mathfrak{s}"] & \\
H \otimes A \arrow[r, "\alpha"] & A
\end{tikzcd}$$

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

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

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

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

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

while the unit property translates into

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

Example 1.2.40. 1. The ground ring R has itself left H-module structure by means of

$$h \cdot r = \varepsilon_H(h) r, \quad h \in H, r \in R.$$

2. Let A be a left H-module. Then, $A \otimes A$ is also a left H-module with respect to

$$h \cdot (a \otimes b) := \sum_{(h)} (h_{(1)} \cdot a) \otimes (h_{(2)} \cdot b), \quad h \in H,\ a, b \in A.$$

3. An R-Hopf algebra H is a left H-module with the multiplication m_H as R-linear action.

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

$$\begin{tikzcd}
A \arrow[r, "f"] & A' \\
H \otimes A \arrow[u, "\alpha_A"] \arrow[r, "\mathrm{Id}_H \otimes f"] & H \otimes A' \arrow[u, "\alpha_{A'}"']
\end{tikzcd}$$

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:*

$$\begin{tikzcd}
A \otimes H \otimes H & A \otimes H \arrow[l, "\beta\otimes\mathrm{Id}_H"'] \\
A \otimes H \arrow[u, "\mathrm{Id}_A\otimes\Delta_H"] & A \arrow[l, "\beta"'] \arrow[u, "\beta"']
\end{tikzcd}$$

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:*

$$\begin{tikzcd}
A \otimes H \arrow[d, "\mathrm{Id}_A\otimes\varepsilon_H"'] & A \arrow[l, "\beta"'] \arrow[dl, "\iota"] \\
A \otimes R &
\end{tikzcd}$$

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:*

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\beta_A"] & A' \arrow[d, "\beta_{A'}"] \\
H \otimes A \arrow[r, "\mathrm{Id}_H \otimes f"] & H \otimes A'
\end{tikzcd}$$

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

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

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

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

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

We first check 1. The coassociative property for β means that
$$\sum_{(a)} \beta(a_{(0)}) \otimes a_{(1)} = \sum_{(a)} a_{(0)} \otimes \Delta_H(a_{(1)}), \quad a_{(0)} \in A, a_{(1)} \in H.$$

Writing down the Sweedler notation for $\beta(a_{(0)})$, we have
$$\sum_{(a)} a_{(0)} \otimes a_{(1)} \otimes a_{(2)} = \sum_{(a)} a_{(0)} \otimes \Delta_H(a_{(1)}).$$

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

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

as we wanted.

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

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

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

   Given $a \in A$, we have that

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

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

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

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

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

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

Finally, for $a \in A$ we have

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

□

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 $h \in H$,

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

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

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

□

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

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

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

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

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

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

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

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

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

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

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

We can complete Proposition 1.2.47 to the following.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $\varphi\in\operatorname{Hom}_R(H,A)$ and $h\in H$,

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

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

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

First, we have

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

Thus, given $h\in H$,

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

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

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

From this, we have that

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

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

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

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

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

Note that

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

Therefore,

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

Since

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

we see that

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

Going through the chain of equalities, we conclude that

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

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

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

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

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 $\{x_1, \dots, x_n\}$ 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 $(e_0, e_1, \dots e_{n-1})$ 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:

$$\begin{tikzcd}
A \otimes H \arrow[rr, "j"] \arrow[d, "\eta"] & & \mathrm{End}(A) \arrow[d, "\delta"] \\
\mathrm{Hom}_A(A \otimes H^*, A) \arrow[rr, "\gamma^*"] & & \mathrm{Hom}_A(A \otimes A, A).
\end{tikzcd}$$

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 $\bar{c}$ (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 $0 \le k < n$ 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 $\sum_{0 \le i < n; m|i} A_i = A_0 \oplus A_m \oplus A_{2m} \oplus \dots$.

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 $(x, \dots, x)$, 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

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

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, $(u_i, \overline{h_i})_{1 \leq i \leq k}$ 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 $S = \{1, \dots, n\}$, 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 $\mathfrak{m}_1, \dots, \mathfrak{m}_t$ 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 $\Psi(I) = \text{Maps}(I, K) = K^I$ 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 $\{1, \dots, n\}$; 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 $\eta \in N$:

$$\begin{tikzcd} G/G' \arrow[r, "\alpha(\eta)"] & G/G' \\ N \arrow[u, "a"] \arrow[r, "\lambda_\eta"] & N. \arrow[u, "a"'] \end{tikzcd}$$

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 $\{1, \dots, p\}$ 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

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

□

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,

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

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

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

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 $g \in G$,

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

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

$$g * u_{K[G]}(r) = g * (r1_G) = r1_G = u_{K[G]}(g * r).$$

- 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 $1 \le i \le n$, $\eta_i^{-1}(\overline{1})(\alpha)$ 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.

4.4 An example of application

Let $L = \mathbb{Q}(\alpha)$, where α is a root of the polynomial $f(x) = x^3 - 3x + 3$. Let us find all the Hopf-Galois structures on $L/\mathbb{Q}$ using Greither-Pareigis theorem.

First, we identify the groups G and G'. Since $[L : K] = 3$, G can be embedded as a transitive subgroup of $S_3 = D_3$, namely, $G \cong C_3$ or $G \cong D_3$. Since the discriminant of f is $\mathrm{disc}(f) = -135 = -3^3 \cdot 5$, which is not a square, we obtain that $G \cong D_3$. Therefore, G can be presented as

$$G = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = 1_G,\ \tau\sigma = \sigma^2\tau \rangle.$$

Under the Galois correspondence, L maps to $G' = \mathrm{Gal}(\widetilde{L}/L)$, and since $[L : K] = [G : G']$, G' is an order 2 subgroup of G. The order 2 subgroups of G are $\langle \tau \rangle$, $\langle \sigma\tau \rangle$ and $\langle \sigma^2\tau \rangle$; we can assume without loss of generality that $G' = \{\tau\}$.

Let us describe how σ and τ act on $\widetilde{L}$. We have $\widetilde{L} = \mathbb{Q}(\alpha, z)$ for $z = \sqrt{-15}$, so it is enough to give the images of α and z (since the definition in the other elements of $\widetilde{L}$ is given by extension by $\mathbb{Q}$-linearity). We know that σ can be seen as a permutation of the roots of f, so $\sigma(\alpha)$ is just one of the other two roots of f. This would give two possibilities for σ, among which there is free choice (exchange of the other two roots of f means replacement of σ by σ^2). On the other hand, let $M = \mathbb{Q}(z)$, which is a subfield of $\widetilde{L}$ that is quadratic over $\mathbb{Q}$. Then, under the Galois correspondence it yields an order 3 subgroup of G, but the only one is $\langle \sigma \rangle$. Therefore, $\mathrm{Gal}(\widetilde{L}/M) = \langle \sigma \rangle$, whence $\sigma(z) = z$. As for τ, the equality $G' = \langle \tau \rangle$ gives $\tau(\alpha) = \alpha$, and $\tau(z) = -z$ follows from the fact that $z^2 \in \mathbb{Q}$.

By Greither-Pareigis theorem, the Hopf-Galois structures on $L/\mathbb{Q}$ are in bijective correspondence with the regular subgroups of $\mathrm{Perm}(G/G')$ normalized by $\lambda(G)$. We have

$$G/G' = \{\overline{1_G}, \overline{\sigma}, \overline{\sigma^2}\}, \quad \overline{\sigma^i} = \{\sigma^i, \sigma^i\tau\},\ i = 0, 1, 2.$$

On the other hand, the left translation map of L/K is the map $\lambda\colon G \longrightarrow \mathrm{Perm}(G/G')$ defined by $\lambda(\sigma^i)(\overline{\sigma^j}) = \overline{\sigma^{i+j}}$.

Let us find the regular subgroups of $\mathrm{Perm}(G/G')$, which in particular have order 3. Since $|G/G'| = 3$, $\mathrm{Perm}(G/G') \cong S_3 = D_3$, the dihedral group of order 6. This possesses a unique order 3 subgroup

$$N := \{\mathrm{Id}_{G/G'}, (\overline{1_G}, \overline{\sigma}, \overline{\sigma^2}), (\overline{1_G}, \overline{\sigma^2}, \overline{\sigma})\}.$$

This is regular, as it is easy to check that its action on G/G' is transitive.

Thus, N defined as above is the only regular subgroup of $\mathrm{Perm}(G/G')$. Note that $N = \lambda(J)$, and this is normalized by $\lambda(G)$ because J is a normal subgroup of G and λ is injective. Therefore, N is the only regular and G-stable subgroup of $\mathrm{Perm}(G/G')$, and hence, L/K admits a unique Hopf-Galois structure H. Let us determine it.

We begin with the underlying Hopf algebra. Let $\cdot$ be the action of G on $\widetilde{L}[N]$ given by the classical Galois action on $\widetilde{L}$ and by conjugation with $\lambda(G)$ on N. Then, the underlying Hopf algebra H is formed by the elements of $\widetilde{L}[N]$ that are fixed by this action. Pick $h \in \widetilde{L}[N]^G$, so $h = \sum_{i=0}^{2} a_i\lambda(\sigma^i)$ for some $a_i \in \widetilde{L}$ and $g \cdot h = h$ for all $g \in G$. It is enough to study the action of the generators σ and τ of G. We have that

$$\sigma * \lambda(\sigma^i) = \lambda(\sigma\sigma^i\sigma^{-1}) = \lambda(\sigma^i), \quad i = 1, 2, 3,$$

so

$$h = \sigma * h = \sum_{i=0}^{2} \sigma(a_i)\lambda(\sigma^i).$$

By the uniqueness of coordinates, $a_i = \sigma(a_i)$ for all i, whence $a_i \in \widetilde{L}^{\langle\sigma\rangle} = M$. On the other hand,

$$\tau * \lambda(\sigma^i) = \lambda(\tau\sigma^i\tau^{-1}) = \lambda(\sigma^{-i}), \quad i = 1, 2, 3,$$

whence

$$h = \tau * h = \tau(a_0)1_{G/G'} + \tau(a_2)\lambda(\sigma) + \tau(a_1)\lambda(\sigma^2).$$

We deduce that $a_0 \in \widetilde{L}^{\langle\tau\rangle} = L$, so $a_0 \in L \cap M = \mathbb{Q}$, and $\tau(a_1) = a_2$, $\tau(a_2) = a_1$ (even though the second equality is redundant because τ is of order 2). Since $a_1 \in M = \mathbb{Q}(z)$, there are $b, c \in \mathbb{Q}$ such that $a_1 = b + cz$. Applying τ we obtain that $a_2 = b - cz$. Let us relabel $a_0 = a$. Then

$$\begin{aligned} h &= a_0\mathrm{Id}_{G/G'} + a_1\lambda(\sigma) + a_2\lambda(\sigma^2) \\ &= a\mathrm{Id}_{G/G'} + (b + cz)\lambda(\sigma) + (b - cz)\lambda(\sigma^2) \\ &= a\mathrm{Id}_{G/G'} + b(\lambda(\sigma) + \lambda(\sigma^2)) + cz(\lambda(\sigma) - \lambda(\sigma^2)) \end{aligned}$$

Hence, h lies in the subspace of $\widetilde{L}[N]$ generated by $1_{G/G'}$, $\lambda(\sigma) + \lambda(\sigma^2)$ and $z(\lambda(\sigma) - \lambda(\sigma^2))$. Since $h \in H$ is arbitrary, H is contained in such a subspace. But both H and the subspace have dimension 3 over $\mathbb{Q}$, so they coincide. In other words, H has $\mathbb{Q}$-basis

$$\{1_{G/G'}, \lambda(\sigma) + \lambda(\sigma^2), z(\lambda(\sigma) - \lambda(\sigma^2))\}.$$

Finally, let us determine the action of H on L. Of course, it is enough to find it on the basis elements of H, and for $1_{G/G'}$, it is trivial. Therefore, we are left to find how $\lambda(\sigma) + \lambda(\sigma^2)$ and $z(\lambda(\sigma) - \lambda(\sigma^2))$ act on elements of L. Given $x \in L$,

$$(\lambda(\sigma) + \lambda(\sigma^2)) \cdot x = \lambda(\sigma)^{-1}(\mathrm{Id}_G)(x) + \lambda(\sigma^2)^{-1}(\mathrm{Id}_G)(x) = \sigma^2(x) + \sigma(x) = (\sigma + \sigma^2)(x),$$

$$z(\lambda(\sigma) - \lambda(\sigma^2)) \cdot x = z(\sigma^2(x) - \sigma(x)) = -z(\sigma - \sigma^2)(x).$$

5 Further applications of Greither-Pareigis theory

5.1 Almost classically Galois extensions revisited

In Section 3.1 we introduced the class of finite separable extensions L/K for which one can find a normal extension M/K such that $L \cap M = K$ and the compositum of L and M is just the normal closure $\widetilde{L}$ of L/K. These extensions are usually called **almost classically Galois** in literature. Furthermore, it has been shown in Proposition 2.3.1 that such extensions are Hopf-Galois. In this section we consider them under the reformulation introduced in Section 4 and deepen in their properties.

First, let us view a notion that arises in the situation of an almost classically Galois extension, which we will find very often in the sequel.

Definition 2.5.1. *Let K be a field and let L and M be field extensions of K with $L, M \subset \overline{K}$. We say that L/K and M/K are linearly disjoint (or that L and M are K-linearly disjoint) if the map*

$$\begin{array}{ccc} L \otimes_K M & \longrightarrow & LM \\ x \otimes y & \longmapsto & xy \end{array}$$

is an isomorphism of K-algebras.

Note that the map at Definition 2.5.1 is always an epimorphism of K-algebras. The fact that two field extensions L/K, M/K are linearly disjoint means that for $x, x' \in L$ and $y, y' \in M$, $xy = x'y'$ if and only if there is some non-zero $r \in K$ such that $x' = rx$ and $y = ry'$ (actually, the latter is implied by the former). The intuition is that at the compositum of L and M, no elements of either field are collapsed. This phenomenon can be visualized through the following result:

Proposition 2.5.2. *If two field extensions L/K and M/K are linearly disjoint, then $L \cap M = K$. Moreover, if either of the extensions is separable and either (possibly the same) normal, the converse holds.*

Proof. The first part is easy and left as exercise. For the converse, see [Coh91, Chapter 5, Theorem 5.5]. □

In particular, two extensions L/K and M/K with M/K Galois are linearly disjoint if and only if $L \cap M = K$.

We study several equivalent definitions of an almost classically Galois extension.

Theorem 2.5.3. *Let L/K be a (G, G')-separable extension. The following statements are equivalent:*

1. *L/K is almost classically Galois.*
2. *There is some finite and Galois extension M/K such that $L \otimes_K M \cong \widetilde{L}$ as K-algebras.*
3. *There is some finite and Galois extension M/K such that $L \otimes_K M$ is isomorphic as a K-algebra to a field containing $\widetilde{L}$.*
4. *There is some normal complement J for G' in G.*
5. *There is a regular and G-stable subgroup N of $\mathrm{Perm}(G/G')$ such that $N \subset \lambda(G)$, where $\lambda\colon G \longrightarrow \mathrm{Perm}(G/G')$ is the left translation map of L/K.*

Proof. Suppose that L/K is almost classically Galois, so that there is a Galois extension M/K such that $L \cap M = K$ and $LM = \widetilde{L}$. Since M/K is Galois, from Proposition 2.5.2 we see that $L \otimes_K M \cong \widetilde{L}$ as K-algebras. Conversely, assume that there is a Galois extension M/K such that $L \otimes_K M \cong \widetilde{L}$ as K-algebras; in particular, $L \otimes_K M$ is a field. Taking into account the definition of the multiplication at $L \otimes_K M$, necessarily $L \otimes_K M \cong LM$ as K-algebras. Together with the previous isomorphism, we obtain $\widetilde{L} = LM$ and the map at Definition 2.5.1 is an isomorphism of K-algebras, so L/K is almost classically Galois.

It is trivial that 2 implies 3. Let us prove the converse. Let M/K be a Galois extension such that $L \otimes_K M$ is a field and $\widetilde{L} \hookrightarrow L \otimes_K M$ as K-algebras. We shall prove that M/K can be shrunk to a Galois extension M'/K such that $L \otimes_K M' \cong \widetilde{L}$ as K-algebras (see [GP87, Proof of Theorem 2.5]). Since $L \otimes_K M$ is a field, arguing as above, $L \otimes_K M \cong LM$ as K-algebras, so $\widetilde{L} \subseteq LM$. Now, by definition, $\widetilde{LM}$ is a field containing L and M, so $LM \subseteq \widetilde{LM}$. Joining both inclusions, we have $LM = \widetilde{LM}$, proving that LM/K is Galois. Hence, so are the extensions $LM/\widetilde{L}$, LM/L and LM/M. Call $\Gamma = \mathrm{Gal}(LM/K)$, $\overline{\Gamma} = \mathrm{Gal}(LM/\widetilde{L})$, $\Gamma_L = \mathrm{Gal}(LM/L)$ and $\Gamma_M = \mathrm{Gal}(LM/M)$. Since the lattice of subgroups of Γ is distributive with respect to the product and the intersection of subgroups and $\overline{\Gamma} \subseteq \Gamma_L$, $\overline{\Gamma}(\Gamma_L \cap \Gamma_M) = (\overline{\Gamma} \cdot \Gamma_L) \cap (\overline{\Gamma} \cdot \Gamma_M) = \Gamma_L \cap (\overline{\Gamma} \cdot \Gamma_M)$. Since the Galois correspondence is inclusion-reversing, applying it at both sides of the equality yields

$$\widetilde{L} \cap (LM) = L(\widetilde{L} \cap M).$$

But recall that LM contains $\widetilde{L}$, so $\widetilde{L} = \widetilde{L} \cap (LM) = L(\widetilde{L} \cap M)$. Let us define $M' := \widetilde{L} \cap M$. Since $\widetilde{L}/K$ and M/K are Galois, so is M'/K. Moreover, the previous equality becomes $\widetilde{L} = LM'$. It remains to prove that $LM' \cong L \otimes_K M'$ as K-algebras, or equivalently, that L and M' are K-linearly disjoint. Since $LM \cong L \otimes_K M$ as K-algebras, $L \cap M = K$. Moreover $M' \subseteq M$, so $L \cap M' = K$. Given that M'/K is Galois, applying Proposition 2.5.2 we obtain that L/K and M'/K are linearly disjoint, as we wanted.

Let us show that 1 and 4 are equivalent. Let M be an intermediate field of $\widetilde{L}/K$ and let $J = \mathrm{Gal}(\widetilde{L}/M)$. By the fundamental theorem of Galois theory, M/K is Galois if and only if J is a normal subgroup of G. In addition, $L \cap M = K$ and $LM = \widetilde{L}$ if and only if $JG = G'$ and $J \cap G' = \{1_G\}$. Hence, L/K is almost classically Galois with complement M if and only if J is a normal complement for G' in G, as we wanted.

Finally, we show the equivalence between 4 and 5. Suppose that there is a normal complement J for G' in G and let $N := \lambda(J)$. Since J is a normal subgroup of G and λ is a group monomorphism, N is G-stable. Let us see that the map $\varphi_{\overline{1}} \colon N \longrightarrow G/G'$ defined by $\varphi_{\overline{1}}(\eta) = \eta(\overline{1})$ is bijective. For $\sigma \in J$, $\varphi_{\overline{1}}(\lambda(\sigma)) = \lambda(\sigma)(\overline{1}) = \overline{\sigma}$. Since $G = JG'$ and $J \cap G'$, for each $g \in G$ there are unique $\sigma \in J$ and $\tau \in G'$ such that $g = \sigma\tau$, so $\overline{g} = \overline{\sigma\tau} = \overline{\sigma}$. Hence, each left coset in G/G' admits as representative a unique element of J (we say that J is a transversal of G' in G). This proves that $\varphi_{\overline{1}}$ is surjective, and the bijectivity follows from $|N| = |G/G'|$. By Proposition 2.4.2, N is regular.

Conversely, suppose that there is a regular and G-stable subgroup N of $\mathrm{Perm}(G/G')$ with $N \subset \lambda(G)$. Call $J := \lambda^{-1}(N)$. Since N is G-stable, J is a normal subgroup of G. First, let us note that for each $\tau \in G'$, $\lambda(\tau)(\overline{1_G}) = \overline{\tau} = \overline{1_G}$. Then $\lambda(G') \subset \mathrm{Stab}_{\lambda(G)}(\overline{1})$.

Now, since N is regular, we have that $\mathrm{Stab}_N(\overline{1}) = \{1_N\}$. Hence,

$$N \cap \lambda(G') \subset N \cap \mathrm{Stab}_{\lambda(G)}(\overline{1}) = \mathrm{Stab}_N(\overline{1}) = \{1_N\}.$$

We deduce that $N \cap \lambda(G') = \{1_N\}$. Applying λ^{-1}, we obtain $J \cap G' = \{1_G\}$. On the other hand, we have that $N\lambda(G') \subseteq \lambda(G)$ and

$$|N\lambda(G')| = |N|\,|\lambda(G')| = |G/G'|\,|G'| = |G| = |\lambda(G)|,$$

so $N\lambda(G') = \lambda(G)$. Applying λ^{-1}, we get $JG' = G$. We conclude that J is a normal complement for G' in G. □

For an almost classically Galois extension L/K with normal closure $\widetilde{L}$, $G = \mathrm{Gal}(\widetilde{L}/K)$ and $G' = \mathrm{Gal}(\widetilde{L}/L)$, we will say that L/K is (G, G')-almost classically Galois.

Remark 2.5.4. From the proof of Proposition 2.5.3 we can see that a field M satisfies 1 if and only if it satisfies 2, and that a field satisfying either is contained in a field satisfying 3. Moreover, a subgroup J of G satisfies 4 if and only if $\lambda(J)$ satisfies 5.

We have also seen that $\lambda(G') \subsetneq \mathrm{Stab}_{\lambda(J)}(\overline{1_G})$, where the stabilizer corresponds to the group action of $\lambda(G)$ on G/G' by evaluation. Since λ is an injection, we can carry this to an action of G on G/G'. In this context, we actually prove the equality.

Corollary 2.5.5. *Let L/K be an (G, G')-almost classically Galois extension and let J be a normal complement for G' in G. Consider the action of G on $\mathrm{Perm}(G/G')$ induced by λ. For $N = \lambda(J)$, we have*

$$G' = \mathrm{Stab}_N(\overline{1}) \equiv \{g \in G \mid \lambda(g)(\overline{1}) = \overline{1}\}.$$

Proof. The action of G on $\mathrm{Perm}(G/G')$ is defined as follows: for $g \in G$ and $\eta \in N$, $g(\eta) = \lambda(g)(\eta)$. Now, for $g \in G$, $g(\overline{1}) = \overline{g}$, so $g \in \mathrm{Stab}_G(\overline{1})$ if and only if $\overline{g} = \overline{1}$; if and only if $g \in G'$. □

It is also possible to define a notion of almost classically Galois structure.

Let L/K be a (G, G')-separable almost classically Galois extension. By Theorem 2.5.3 5, there is some subgroup N giving a Hopf-Galois structure on L/K under the Greither-Pareigis correspondence that in addition satisfies $N \subset \lambda(G)$. However, L/K might admit other Hopf-Galois structures, and so, given by subgroups that lie outside $\lambda(G)$. We give a name to those Hopf-Galois structures that come from a normal complement.

Definition 2.5.6. *Let L/K be a (G, G')-almost classically Galois extension. We say that a Hopf-Galois structure on L/K is almost classically Galois if its corresponding subgroup of $\mathrm{Perm}(G/G')$ under the Greither-Pareigis correspondence satisfies $N \subset \lambda(G)$.*

We have from Theorem 2.5.3 5 that every almost classically Galois extension admits some almost classically Galois structure H. Let N be the corresponding permutation subgroup, so that $N \subset \lambda(G)$. Since λ is a group embedding, we have that $N = \lambda(J)$ for some normal subgroup J of G. This may be a normal complement of G', but not necessarily.

Example 2.5.7. Let L/K be a (G,G')-separable extension with $G \cong D_4$ and $G' \cong C_2$. Then L/K is almost classically Galois because $G = J \rtimes G'$ with $J \cong C_4$. Call $J = \langle \sigma \mid \sigma^4 = 1_G \rangle$ and $G' = \langle \tau \mid \tau^2 = 1_G \rangle$, so that

$$G = \langle \sigma, \tau \mid \sigma^4 = 1_G,\, \tau^2 = 1_G,\, \tau\sigma = \sigma^3\tau \rangle.$$

It can be checked that the regular and G-stable subgroups of $\mathrm{Perm}(G/G')$ are:

$$N = \langle (\overline{1}, \overline{\sigma}, \overline{\sigma^2}, \overline{\sigma^3}) \rangle,$$

$$N' = \langle (\overline{1}, \overline{\sigma})(\overline{\sigma^2}, \overline{\sigma^3}), (\overline{1}, \overline{\sigma^2})(\overline{\sigma}, \overline{\sigma^3}) \rangle.$$

Note that $N = \lambda(J)$ and $N' = \lambda(J')$ with $J' = \langle \sigma^2, \sigma\tau \rangle$. Both J and J' are normal subgroups, but only J serves as a normal complement for G', as $J' \cong C_2 \times C_2$.

Note that an almost classically Galois structure need not be unique, just because a normal complement for a subgroup G' of a group G is not unique in general.

The underlying Hopf algebra of an almost classically Galois structure admits a simpler expression than the one given at Proposition 2.4.16 1.

Proposition 2.5.8. *Let L/K be a (G,G')-almost classically Galois extension with complement M. Let N be a regular and G-stable subgroup of* $\mathrm{Perm}(G/G')$ *with $N \subset \lambda(G)$. Then $\widetilde{L}[N]^G = M[N]^{G'}$.*

Proof. Recall that the action of G on $\widetilde{L}[N]$ is the one given at (2.1). Let $J = \mathrm{Gal}(\widetilde{L}/M)$. Since $G = J \rtimes G$, we have $\widetilde{L}[N]^G = (\widetilde{L}[N]^J)^{G'}$. Since $N \subset \lambda(G)$, $N = \lambda(J')$ for some normal subgroup J' of G. Since the conjugation by J leaves J' invariant, the conjugation by $\lambda(J)$ leaves $\lambda(J') = N$ invariant. Therefore, $\widetilde{L}[N]^J = \widetilde{L}^J[N] = M[N]$, and the statement follows. □

Example 2.5.9. Let us go back to the example from Section 4.4. We saw that $J = \langle \sigma \rangle$ is a normal complement for $G' = \langle \tau \rangle$, so L/K is almost classically Galois. When we picked an element $h \in \widetilde{L}[N]^G$, the condition that it is fixed by the action of J lead that it belongs to $M[N]^{G'}$, because h is already fixed by such an action. This is because $N = \lambda(J)$, so the action of J by conjugation leaves N invariant. One can see that the basis elements that we obtained are indeed fixed by the action of G'.

5.2 Byott's uniqueness theorem

In this part we study a sufficient condition found by Byott in the paper [Byo96] so as to ensure that a separable Hopf-Galois extension admits a unique Hopf-Galois structure, which is established using the techniques from Byott's translation that we saw at Section 3.2. Such a condition is related with a class of integer numbers, that are called Burnside.

Definition 2.5.10. *Let n be an integer number. We say that n is Burnside if it is coprime with its image by the Euler totient function φ, that is,* $\gcd(n, \varphi(n)) = 1$.

It is trivial from the definition that every prime number is Burnside. Moreover, every Burnside number is square-free. This follows directly from the remarks that $\varphi(p^r) = p^{r-1}(p-1)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ if $\gcd(a,b) = 1$. Burnside numbers are linked with group theory by the following result.

Theorem 2.5.11 (Burnside)**.** *Let $n \in \mathbb{Z}_{\geq 1}$ be a positive integer. Then every group of order n is cyclic if and only if n is Burnside.*

Byott's uniqueness thereom provides a sufficient condition which ensures that a separable Hopf-Galois extension admits a unique Hopf-Galois structure. Namely, this condition is that the degree of the extension is a Burnside number. We need the following technical lemma.

Lemma 2.5.12. *Let L/K be a (G, G')-separable degree n extension and suppose that n is Burnside. Suppose that N is a regular and G-stable subgroup of* $\mathrm{Perm}(G/G')$ *and let Λ_N be the set of left translations $\lambda_\eta \colon N \longrightarrow N$, $\eta \in N$. For each subgroup H of* $\mathrm{Hol}(N)$ *whose order is divisible by n, $\Lambda_N \subset H$.*

Proof. Recall that $\mathrm{Hol}(N) = \Lambda_N \rtimes \mathrm{Aut}(N)$ by definition. Consider the projection $\pi_2 \colon \mathrm{Hol}(N) \longrightarrow \mathrm{Aut}(N)$ onto the second component. Since π_2 is a group epimorphism (because $\mathrm{Aut}(N) \cong \mathrm{Hol}(N)/\Lambda_N$), it maps H onto a subgroup of $\mathrm{Aut}(N)$, whose order divides the order of $\mathrm{Aut}(N)$. Now, since n is Burnside and N has order n, we have that $N \cong \mathbb{Z}/n\mathbb{Z}$, and hence $\mathrm{Aut}(N) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. We deduce that $\mathrm{Aut}(N)$ has order $\varphi(n)$. It follows that the order of $\pi_2(H)$ divides $\varphi(n)$. Now, $\pi_2(H) \cong H\Lambda_N/\Lambda_N \cong H/\Lambda_N \cap H$, whence $|H/\Lambda_N \cap H| = \frac{|H|}{|\Lambda_N \cap H|}$ divides $\varphi(n)$. Taking into account that n divides $|H|$ and $\gcd(n, \varphi(n)) = 1$, necessarily $|\Lambda_N \cap H|$ is divisible by n. By the structure of semidirect product, Λ_N is the only order n subgroup of $\mathrm{Hol}(N)$. Now, Cauchy theorem gives that $\Lambda_N \cap H$ must have some subgroup of order n, which is necessarily Λ_N. We get $\Lambda_N \cap H = \Lambda_N$, and hence $\Lambda_N \subset H$ follows. □

Theorem 2.5.13 ([Byo96], Theorem 2)**.** *Let L/K be a G-separable degree n extension. If L/K is Hopf-Galois and n is Burnside, then G is solvable and L/K admits a unique Hopf-Galois structure, which is almost classically Galois (in particular, L/K is almost classically Galois).*

Proof. Let $\widetilde{L}$ be the normal closure of L/K, $G = \mathrm{Gal}(\widetilde{L}/K)$ and $G' = \mathrm{Gal}(\widetilde{L}/L)$. The hypothesis that L/K is Hopf-Galois ensures that it admits some Hopf-Galois structure H; let N be its corresponding regular and G-stable subgroup of $\mathrm{Perm}(G/G')$. Let $\alpha \colon N \longrightarrow \mathrm{Perm}(G/G')$ be the canonical inclusion. By Theorem 2.3.7, α corresponds to a group embedding $\beta \colon G \longrightarrow \mathrm{Perm}(N)$ such that $\beta(G) \subset \mathrm{Hol}(N)$. Now, note that $\Lambda_N = \lambda_N(N)$, where $\lambda_N \colon N \longrightarrow \mathrm{Aut}(N)$ is the left regular representation of N. Since λ_N is injective, Λ_N has order n. By Theorem 2.5.11, both Λ_N and N are cyclic. In addition, $\mathrm{Aut}(N) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, which is abelian. Therefore, $\mathrm{Hol}(N)$ is solvable. Since $\beta(G) \subset \mathrm{Hol}(N)$ with β injective, we conclude that G is solvable.

Let us prove that H is an almost classically Galois structure on L/K. We have that $\beta(G)$ is a subgroup of $\mathrm{Hol}(N)$ and its order is that of G, which is a multiple of n. Applying Lemma 2.5.12 with $H = \beta(G)$, we get $\Lambda_N \subset \beta(G)$. Going over the proof of Theorem 2.3.7, we see by (a) that $\beta = Ca^{-1} \circ \lambda$, where $Ca \colon \mathrm{Perm}(N) \longrightarrow \mathrm{Perm}(G/G')$ is the group isomorphism induced by the bijection $a \colon N \longrightarrow G/G'$, $a(\eta) = \eta(\overline{1_G})$. On the other hand, in (b) it is shown that $\lambda_N = Ca^{-1} \circ \alpha$. Applying Ca on the previous inclusion, we obtain that $N = \alpha(N) \subset \lambda(G)$, so the Hopf-Galois structure corresponding to N is almost classically Galois.

Finally, we shall prove that L/K does not admit other Hopf-Galois structures. Suppose that N' is a regular and G-stable subgroup of $\mathrm{Perm}(G/G')$. If we consider the canonical inclusion $\alpha' \colon N' \longrightarrow \mathrm{Perm}(G/G')$, the definition of α and α' are the same. Thus, if $\beta' \colon G \hookrightarrow \mathrm{Hol}(N')$ is the group embedding corresponding to α' by Byott's theorem, we have that $\beta' = Ca'^{-1} \circ \alpha'$, where $Ca' \colon \mathrm{Perm}(N') \longrightarrow \mathrm{Perm}(G/G')$ is the group isomorphism induced by the bijection $a \colon N' \longrightarrow G/G'$, and then the definitions of β and β' are the same. Then we can regard $\beta(G)$ as a subgroup of $\mathrm{Hol}(N')$. We then apply Lemma 2.5.12 with N' as regular and G-stable subgroup and $H = \beta(G)$, obtaining that $\Lambda_{N'} \subset \beta(G) \subset \mathrm{Hol}(N)$. Hence $\Lambda_{N'}$ is an order n subgroup of $\mathrm{Hol}(N)$, so once again by Lemma 2.5.12 (with N as regular and G-stable subgroup and $H = \Lambda_{N'}$), we obtain $\Lambda_N \subset \Lambda_{N'}$, both of which have order n. Necessarily $\Lambda_N = \Lambda_{N'}$, that is, $\lambda_N(N) = \lambda_{N'}(N')$. We use again that α and α' have the same definition to obtain that $\lambda_N = Ca^{-1} \circ \alpha$ and $\lambda_{N'} = Ca'^{-1} \circ \alpha'$ also do, to conclude that $N = N'$. □

A G-separable degree n extension with n Burnside and G solvable is not necessarily Hopf-Galois (see [Byo96, Example after Theorem 2] for a counterexample). Then, Theorem 2.5.13 can be restated by saying that a separable degree n extension with n Burnside admits at most one Hopf-Galois structure.

We shall show that the converse of Theorem 2.5.13 does not hold: a G-separable extension with G solvable and admitting a unique Hopf-Galois structure has not necessarily Burnside degree. Indeed, it can be checked that a G-separable quartic extension with $G \cong A_4$ or $G \cong S_4$ (thus, G solvable) admits a unique Hopf-Galois structure, and 4 is not a Burnside number because $\varphi(4) = 2$.

Let us specify Theorem 2.5.13 to the Galois case. If L/K is a Galois extension with group G with Burnside degree, then G is solvable and the classical Galois structure on L/K is the unique Hopf-Galois structure on L/K. In this case, having Burnside degree becomes a characterization for the uniqueness of Hopf-Galois structure.

Theorem 2.5.14 ([Byo96], Theorem 1)**.** *A degree n Galois extension L/K admits a unique Hopf-Galois structure if and only if n is Burnside.*

The right-to-left implication is just a particular case of Theorem 2.5.13. A proof for the converse can be found in [Chi00, §8].

Since prime numbers are Burnside, Theorem 2.5.13 yields the following.

Corollary 2.5.15. *Let p be a prime number and let L/K be a Hopf-Galois extension with degree p. Then L/K admits a unique Hopf-Galois structure.*

5.3 Opposite Hopf-Galois structures

The Greither-Pareigis theorem establishes a connection between the Hopf-Galois structures on a separable extension and group theory. Thus, one can wonder if notions or results on the latter can be translated to the former. One of these is the notion of opposite group, of which we shall study its Hopf-Galois counterpart. For a group $(N, \star)$, its opposite, denoted by N^{opp}, is defined as the group whose underlying set is also N and the operation is defined as

$$\eta \star' \mu := \mu \star \eta, \quad \mu, \eta \in N.$$

Let N be a permutation subgroup giving a Hopf-Galois structure on a separable extension under the Greither-Pareigis correspondence. We shall see that N^{opp} also gives a Hopf-Galois structure on the same extension. But, in order to do so, we need to visualize it as a subgroup of the same permutation group. We see that we can identify it with the centralizer of N.

Proposition 2.5.16. *Let X be a finite set and let N be a regular subgroup of* $\mathrm{Perm}(X)$. *Fix $x_0 \in X$ and for each $\eta \in N$, define a map $\phi_\eta \colon X \longrightarrow X$ as follows: for $x \in X$, $\phi_\eta(x) = \mu_x \circ \eta(x_0)$, where $\mu_x \in N$ is such that $\mu_x(x_0) = x$. The following statements hold:*

1. *For every $\eta \in N$, ϕ_η is well defined and bijective.*

2. $\mathrm{Cent}_{\mathrm{Perm}(X)}(N) = \{\phi_\eta \mid \eta \in N\}$.

3. *The map $\Phi \colon N^{\mathrm{opp}} \longrightarrow \mathrm{Cent}_{\mathrm{Perm}(X)}(N)$ defined by $\Phi(\eta) = \phi_\eta$ is a group isomorphism.*

Proof. 1. Let $\eta \in N$. Since N is regular, for each $x \in X$ there is a unique $\mu_x \in N$ such that $\mu_x(x_0) = x$. This ensures that ϕ_η is well defined. Let us see that it is bijective. Let $x, y \in X$ such that $\phi_\eta(x) = \phi_\eta(y)$, that is, $\mu_x \circ \eta(x_0) = \mu_y \circ \eta(x_0)$. Since $\mu_x, \mu_y, \eta \in N$, we have that both $\mu_x \circ \eta$ and $\mu_y \circ \eta$ belong to N, and by the regularity of N, they are completely determined by their definition at x_0. Hence, $\mu_x \circ \eta = \mu_y \circ \eta$, and composing on the right side by η^{-1}, we get $\mu_x = \mu_y$. Evaluating at x_0, we obtain that $x = y$, so ϕ_η is injective. Since it is defined from X to itself and X is finite, ϕ_η is bijective.

2. Let $\phi \in \mathrm{Cent}_{\mathrm{Perm}(X)}(N)$. By regularity, there is a unique $\eta \in N$ such that $\eta(x_0) = \phi(x_0)$. We claim that $\phi = \phi_\eta$. Take $x \in X$. By the definition of centralizer, $\mu_x \circ \phi = \phi \circ \mu_x$. Now,

$$\phi(x) = \phi \circ \mu_x(x_0) = \mu_x \circ \phi(x_0) = \mu_x \circ \eta(x_0) = \phi_\eta(x).$$

Hence $\phi = \phi_\eta$ as claimed. Conversely, take $\eta \in N$ and let us prove that ϕ_η centralizes N. We need to prove that, for each $\mu \in N$, $\phi_\eta \circ \mu = \mu \circ \phi_\eta$. Given $x \in X$, $\mu \circ \phi_\eta(x) = \mu \circ \mu_x \circ \eta(x_0)$. Now, note that

$$\mu \circ \mu_x(x_0) = \mu(x) = \mu_{\mu(x)}(x_0).$$

By regularity, $\mu \circ \mu_x = \mu_{\mu(x)}$. Then,

$$\mu \circ \phi_\eta(x) = \mu_{\mu(x)} \circ \eta(x_0) = \phi_\eta(\mu(x)) = \phi_\eta \circ \mu(x).$$

This proves that $\phi_\eta \circ \mu = \mu \circ \phi_\eta$, as we wanted.

3. We already know that for each $\phi \in \mathrm{Cent}_{\mathrm{Perm}(X)}(N)$ there is some η in the underlying set of N such that $\phi = \phi_\eta$. This is the same as the underlying set of N^{opp}, so Φ is surjective. On the other hand, if $\eta, \mu \in N$ are such that $\phi_\eta = \phi_\mu$, evaluating at any element $x \in X$ gives $\mu_x \circ \eta(x_0) = \mu_x \circ \mu(x_0)$, and composing by μ_x^{-1} on the left side gives $\eta(x_0) = \mu(x_0)$. Once again, the regularity of N gives that $\eta = \mu$. This proves that Φ is bijective. Let us check that it preserves the group structure. Given $\eta, \mu \in N$, we must check that $\Phi(\eta \circ' \mu) = \Phi(\eta) \circ \Phi(\mu)$, that is, $\phi_{\mu \circ \eta} = \phi_\eta \circ \phi_\mu$. Given $x \in X$, we have

$$\phi_\eta \circ \phi_\mu(x) = \mu_{\phi_\mu(x)} \circ \eta(x_0) = \mu_{\mu_x \circ \mu(x_0)} \circ \eta(x_0).$$

Now, $\mu_{\mu_x \circ \mu(x_0)}(x_0) = \mu_x \circ \mu(x_0)$, so $\mu_{\mu_x \circ \mu(x_0)} = \mu_x \circ \mu$ by regularity. Then,

$$\phi_\eta \circ \phi_\mu(x) = \mu_x \circ \mu \circ \eta(x_0) = \phi_{\mu \circ \eta}(x),$$

finishing the proof.

□

From now on, for each regular subgroup N of a permutation group $\mathrm{Perm}(X)$, we regard N^{opp} as a subgroup of $\mathrm{Perm}(X)$ by means of identifying $N^{\mathrm{opp}} = \mathrm{Cent}_{\mathrm{Perm}(X)}(N)$.

Proposition 2.5.17. *Let X be a finite set and let N be a regular subgroup of* $\mathrm{Perm}(X)$*. Then N^{opp} is regular.*

Proof. Since the underlying set of N^{opp} is the same as the underlying set of N, $|N^{\mathrm{opp}}| = |N|$. Let $x \in X$ and take $\phi \in \mathrm{Stab}_{N^{\mathrm{opp}}}(x)$. Let $\eta \in N$ be such that $\phi = \phi_\eta$. Then,

$$\mu_x \circ \eta(x_0) = \phi(x) = x = \mu_x(x_0).$$

The regularity of N yields that $\mu_x \circ \eta = \mu_x$, so $\eta = 1_N$. Then $\mathrm{Stab}_{N^{\mathrm{opp}}}(x) = \{\mathrm{Id}\}$. □

Now, we turn to the scenario of field extensions.

Proposition 2.5.18. *Let L/K be a (G, G')-separable extension and let N be a regular subgroup of* $\mathrm{Perm}(X)$*. If N is G-stable, then so is N^{opp}.*

Proof. Suppose that N is G-stable. Given $\eta \in N$ and $g \in G$, we shall prove that $\lambda(g) \circ \phi_\eta \circ \lambda(g^{-1}) \in N$, that is, $\lambda(g) \circ \phi_\eta \circ \lambda(g^{-1}) = \phi_{\eta'}$ for some $\eta' \in N$. Equivalently, $\lambda(g) \circ \phi_\eta \circ \lambda(g^{-1})(x) = \mu_x \circ \eta'(x_0)$ for some $\eta' \in N$. We have that

$$\begin{aligned}
\lambda(g) \circ \phi_\eta \circ \lambda(g^{-1})(x) &= \lambda(g) \circ \mu_{\lambda(g^{-1})(x)} \circ \eta(x_0) \\
&= \lambda(g) \circ \mu_{\lambda(g^{-1})(x)} \circ \eta \circ \lambda(g^{-1}) \circ \lambda(g)(x_0) \\
&= \lambda(g) \circ \mu_{\lambda(g^{-1})(x)} \circ \eta \circ \lambda(g^{-1}) \circ \mu_{\lambda(g)(x_0)}(x_0) \\
&= \mu_x \circ \mu_x^{-1} \circ \lambda(g) \circ \mu_{\lambda(g^{-1})(x)} \circ \eta \circ \lambda(g^{-1}) \circ \mu_{\lambda(g)(x_0)}(x_0).
\end{aligned}$$

Thus, it is enough to show that the element

$$\eta'_x := \mu_x^{-1} \circ \lambda(g) \circ \mu_{\lambda(g^{-1})(x)} \circ \eta \circ \lambda(g^{-1}) \circ \mu_{\lambda(g)(x_0)} \in N$$

does not depend on x. Note that

$$\lambda(g) \circ \mu_{\lambda(g^{-1})(x)} \circ \lambda(g^{-1}) \circ \mu_{\lambda(g)(x_0)}(x_0) = x$$

with $\lambda(g) \circ \mu_{\lambda(g^{-1})(x)} \circ \lambda(g^{-1}) \circ \mu_{\lambda(g)(x_0)} \in N$, so

$$\mu_x = \lambda(g) \circ \mu_{\lambda(g^{-1})(x)} \circ \lambda(g^{-1}) \circ \mu_{\lambda(g)(x_0)}.$$

Equivalently,

$$\lambda(g) \circ \mu_{\lambda(g^{-1})(x)} \circ \lambda(g^{-1}) = \mu_x \circ \mu_{\lambda(g)(x_0)}^{-1}.$$

Then,

$$\begin{aligned}
\eta'_x &= \mu_x^{-1} \circ \lambda(g) \circ \mu_{\lambda(g^{-1})(x)} \circ \eta \circ \lambda(g^{-1}) \circ \mu_{\lambda(g)(x_0)} \\
&= \mu_x^{-1} \circ \lambda(g) \circ \mu_{\lambda(g^{-1})(x)} \circ \lambda(g^{-1}) \circ \lambda(g) \circ \eta \circ \lambda(g^{-1}) \circ \mu_{\lambda(g)(x_0)} \\
&= \mu_x^{-1} \circ \mu_x \circ \mu_{\lambda(g)(x_0)}^{-1} \circ \lambda(g) \circ \eta \circ \lambda(g^{-1}) \circ \mu_{\lambda(g)(x_0)} \\
&= \mu_{\lambda(g)(x_0)}^{-1} \circ \lambda(g) \circ \eta \circ \lambda(g^{-1}) \circ \mu_{\lambda(g)(x_0)},
\end{aligned}$$

which does not depend on x_0. Let us relabel

$$\eta' := \mu_{\lambda(g)(x_0)}^{-1} \circ \lambda(g) \circ \eta \circ \lambda(g^{-1}) \circ \mu_{\lambda(g)(x_0)}.$$

We obtain that

$$\lambda(g) \circ \phi_\eta \circ \lambda(g^{-1})(x) = \mu_x \circ \eta'(x) = \phi_{\eta'}(x)$$

for every $x \in X$, whence $\lambda(g) \circ \phi_\eta \circ \lambda(g^{-1}) = \phi_{\eta'} \in N$. □

We conclude that, for a (G, G')-separable extension, the opposite of a regular and G-stable subgroup of $\mathrm{Perm}(G/G')$ also is. The Greither-Pareigis correspondence yields the following notion.

Definition 2.5.19. *Let L/K be a (G, G')-separable Hopf-Galois extension. Let H be a Hopf-Galois structure on L/K and let N be a regular and G-stable subgroup of* $\mathrm{Perm}(G/G')$*. The* ***opposite Hopf-Galois structure*** *of H, denoted as H^{opp}, is the one whose corresponding permutation subgroup is N^{opp}.*

If N is abelian, the opposite Hopf-Galois structure of H is itself.

Let L/K be a Galois extension with group G and let λ (resp. ρ) be the left (resp. right) regular representation of G. Recall by Proposition 2.4.19 2 that $\rho(G)$ is centralized by $\lambda(G)$, whence $\mathrm{Cent}_{\mathrm{Perm}(G)}(\rho(G)) = \lambda(G)$. We obtain:

Corollary 2.5.20. *Let L/K be a Galois non-abelian extension. The opposite Hopf-Galois structure of the classical Galois structure is the canonical non-classical structure.*

Remark 2.5.21. The opposite of an almost classically Galois structure need not be almost classically Galois. As a counterexample, consider the situation at Corollary 2.5.20. The classical Galois structure on L/K corresponds to the subgroup $\lambda(G)$, while its opposite, the canonical non-classical structure, corresponds to $\rho(G)$. The classical Galois structure is trivially almost classically Galois, while the canonical non-classical structure is not because $\rho(G) \not\subset \lambda(G)$, which follows from Proposition 2.4.19 3.

Recall from Proposition 2.4.11 that if a Hopf-Galois structure H corresponds to a subgroup N, $\widetilde{L} \otimes_K H \cong \widetilde{L}[N]$ as $\widetilde{L}$-Hopf algebras. Using the notion of opposite group we can find the smallest field base field with that property.

Proposition 2.5.22. *Let L/K be a separable extension with normal closure $\widetilde{L}$. Let H be a Hopf-Galois structure on L/K and let N be its corresponding permutation subgroup. Let $G_0 = \lambda^{-1}(N^{\mathrm{opp}})$ and let $L_0 = \widetilde{L}^{G_0}$. Then L_0 is the smallest extension of K such that*

$$L_0 \otimes_K H \cong L_0[N]$$

as L_0-algebras.

The proof of Proposition 2.5.22 makes use of descent theory and cohomology, and it is beyond the scope of these notes. It can be consulted at [GP87, Corollary 3.2].

Note that G_0 is the subgroup of elements of G that fix all the elements of N by the action $*$ defined at (2.1). Assume that L/K is almost classically Galois with J a normal complement of G' and choose $N = \lambda(J)^{\mathrm{opp}}$. Then $N^{\mathrm{opp}} = \lambda(J)$ and, consequently, $J = G_0$. Thus, the field L_0 is the complement of L/K as an almost classically Galois extension.

Corollary 2.5.23. *Let L/K be a (G, G')-separable almost classically Galois extension with complement M, and let $J = \mathrm{Gal}(\widetilde{L}/M)$. Let $N = \lambda(J)^{\mathrm{opp}}$ and let H be its corresponding Hopf-Galois structure on L/K. Then M is the smallest extension of K such that*

$$M \otimes_K H \cong M[N].$$

It is remarkable that Corollary 2.5.23 states a property for the opposite of an almost classically Galois structure. For this reason, some authors call these almost classically Galois structures; namely, the ones given by a permutation subgroup N such that $N^{\mathrm{opp}} \subset \lambda(G)$.

5.4 Induced Hopf-Galois structures

Let E/K be a finite and Galois extension with Galois group of the form $G = J \rtimes G'$, where J is a normal subgroup of G and G' is any subgroup of G. Call $L = E^{G'}$. It is possible to build a Hopf-Galois structure on E/K from a pair of Hopf-Galois structures from E/L and L/K. Such Hopf-Galois structures are called induced, and were introduced by Crespo, Rio and Vela in the paper [CRV16].

In order to introduce the notion of induced Hopf-Galois structure, we make use of the Greither-Pareigis correspondence. Namely, we will see that the direct product of the permutation subgroups corresponding to Hopf-Galois structures on E/L and L/K is isomorphic to a subgroup giving a Hopf-Galois structure on L/K.

Both of the extensions E/K and E/L are Galois with groups G and G' respectively. By Greither-Pareigis theorem:

1. The Hopf-Galois structures on E/L are in bijective correspondence with the regular subgroups of $\mathrm{Perm}(G')$ normalized by the image of the left translation map $\lambda^{G'} \colon G' \longrightarrow \mathrm{Perm}(G')$.

2. The Hopf-Galois structures on E/K are in bijective correspondence with the regular subgroups of $\mathrm{Perm}(G)$ normalized by the image of the left translation map $\lambda \colon G \longrightarrow \mathrm{Perm}(G)$ of L/K.

The situation is a bit trickier for the extension L/K, which is typically non-Galois. Note that E is a Galois field extension of K containing L, so E contains the normal closure $\widetilde{L}$ of L. However, in general it does not hold that $E = \widetilde{L}$ (for instance, when the semidirect product is direct). By Proposition 2.4.3, we can apply Greither-Pareigis theorem to characterize the Hopf-Galois structures on L/K choosing any Galois extension of K containing L, not just its normal closure. In particular, we can choose E/K. Thus, the Hopf-Galois structures on L/K are in bijective correspondence with the regular subgroups of $\mathrm{Perm}(G/G')$ normalized by $\lambda_E(G)$, where $\lambda_E\colon G \longrightarrow \mathrm{Perm}(G/G')$ is the left translation map of L/K associated to E.

Another of the key ingredients for the existence of induced Hopf-Galois structures is that J is a transversal of G' in G, which is a consequence of J being a normal complement for G' in G. This means that each left coset of G/G' intersects with J in exactly one element. Let us write $J = \{\sigma_1, \dots, \sigma_n\}$, where $n = [L : K]$. Then, we can write $G/G' = \{\sigma_1 G', \dots, \sigma_n G'\}$ and identify J with G/G'. Carrying this identification to the map $\lambda_L\colon G \longrightarrow \mathrm{Perm}(G/G')$, we get a map $\lambda_c\colon G \longrightarrow \mathrm{Perm}(J)$ whose definition corresponds to the action of G on the left cosets of G/G' by means of λ_L. Namely, for a given element $g \in G$, $\lambda_c(g)$ is the permutation of J that takes an element $\sigma_i \in J$ to the representative of J in the left coset $\lambda_L(g)(\sigma_i G')$. Let us calculate it. Write $g = \sigma\tau$ with $\sigma \in J$ and $\tau \in G'$. For every $1 \leq i \leq n$,

$$\begin{aligned}\lambda_L(g)(\sigma_i G') &= \sigma\tau\sigma_i G'\\ &= \sigma\tau\sigma_i\tau^{-1}\tau G'\\ &= \sigma C_\tau(\sigma_i) G'\\ &= \lambda^J(\sigma) \circ C_\tau(\sigma_i) G',\end{aligned}$$

where $C_\tau \in \mathrm{Aut}(G)$ is the conjugation by τ and $\lambda^J\colon J \longrightarrow \mathrm{Perm}(J)$ is the left translation map associated to L/F. Note that $C_\tau(\sigma_i) \in J$ because J is a normal subgroup of G, so $\lambda^J(\sigma) \circ C_\tau(\sigma_i)$ makes sense and belongs to J. Thus, for $g = \sigma\tau \in G$,

$$\lambda_c(g)(\sigma_i) = \lambda^J(\sigma) \circ C_\tau(\sigma_i) \tag{2.4}$$

Proposition 2.5.24. *Let $\lambda\colon G \longrightarrow \mathrm{Perm}(G)$ be the left regular representation of E/K. Then, $\lambda = \iota \circ \chi$, where*

$$\begin{array}{cccc} \chi\colon & G & \longrightarrow & \mathrm{Perm}(J) \times \mathrm{Perm}(G') \\ & \sigma\tau & \longmapsto & (\lambda_c(\sigma\tau), \lambda^{G'}(\tau)), \\ \iota\colon & \mathrm{Perm}(J) \times \mathrm{Perm}(G') & \longrightarrow & \mathrm{Perm}(G) \\ & (\varphi, \psi) & \longmapsto & \sigma\tau \mapsto \varphi(\sigma)\psi(\tau). \end{array}$$

Proof. Given $g = \sigma\tau \in G$ and $g' = \sigma'\tau' \in G$, we have

$$\begin{aligned}\lambda(g)(g') = gg' = \sigma\tau\sigma'\tau' &= \sigma\tau\sigma'\tau^{-1}\tau\tau'\\ &= \sigma C_\tau(\sigma')\lambda^{G'}(\tau)(\tau')\\ &= \lambda_c(g)(\sigma')\lambda^{G'}(\tau)(\tau')\\ &= \iota(\lambda_c(g), \lambda^{G'}(\tau))(g')\\ &= \iota \circ \chi(g)(g'),\end{aligned}$$

where, from the second to the third line, we have used (2.4). □

We are ready to build the so-called induced Hopf-Galois structures.

Proposition 2.5.25. *Let N_1 be a subgroup of* $\mathrm{Perm}(J)$ *and let N_2 be a subgroup of* $\mathrm{Perm}(G')$. *Let $N = \iota(N_1 \times N_2)$.*

1. *If N_1 and N_2 are regular, so is N.*

2. *If N_1 is normalized by $\lambda_L(G)$ and N_2 is normalized by $\lambda^{G'}(G')$, then N is normalized by $\lambda(G)$.*

Proof. 1. Suppose that N_1 and N_2 are regular. We have

$$|N| = |\iota(N_1 \times N_2)| = |N_1 \times N_2| = |N_1||N_2| = |J||G'| = |G|,$$

so it is enough to check that the action of N on G is transitive. Let $g = \sigma\tau$, $g' = \sigma'\tau' \in G$ with $\sigma, \sigma' \in J$ and $\tau, \tau' \in G'$. Since N_1 (resp. N_2) is regular, there exists $\varphi \in \mathrm{Perm}(J)$ (resp. $\psi \in \mathrm{Perm}(G')$) such that $\varphi(\sigma) = \sigma'$ (resp. $\psi(\tau) = \tau'$). Then,

$$\iota(\varphi, \psi)(g) = \iota(\varphi, \psi)(\sigma\tau) = \varphi(\sigma)\psi(\tau) = \sigma'\tau' = g'.$$

2. Let $g = \sigma\tau \in G$ with $\sigma \in J$ and $\tau \in G'$. Given $(\eta, \mu) \in N_1 \times N_2$,

$$\chi(g)(\eta, \mu)\chi(g^{-1}) = (\lambda_c(g)\eta\lambda_c(g)^{-1}, \lambda^{G'}(\tau)\mu\lambda^{G'}(\tau^{-1})) \in N_1 \times N_2.$$

Applying ι, since it is a group homomorphism, we obtain

$$\lambda(g)\iota(\eta, \mu)\lambda(g^{-1}) = \iota(\chi(g)(\eta, \mu)\chi(g^{-1})) \in \iota(N_1 \times N_2) = N.$$

□

Applying Greither-Pareigis theorem, we get the following.

Corollary 2.5.26. *Let E/K be a Galois extension with Galois group $G = J \rtimes G'$ and let $L = E^{G'}$. If N_1 is a subgroup of $\mathrm{Perm}(J)$ giving L/K a Hopf-Galois structure and N_2 is a subgroup of $\mathrm{Perm}(G')$ giving E/L a Hopf-Galois structure, then $N = \iota(N_1 \times N_2)$ is a subgroup giving E/K a Hopf-Galois structure.*

Definition 2.5.27. *A Hopf-Galois structure on E/K as in Corollary 2.5.26 is called an **induced Hopf-Galois structure** on E/K.*

If an induced Hopf-Galois structure H on E/K is built from Hopf-Galois structures H_1 on L/K and H_2 on E/L, we will also say that H is induced from H_1 and H_2, or that H_1 and H_2 induce H. The Hopf-Galois structures H_1 and H_2 receive the name of inducing Hopf-Galois structures.

Induced Hopf-Galois structures only make sense for Galois extensions whose Galois group is a semidirect product. In particular, if the Galois group of a Galois extension E/K is a direct product, then there are induced Hopf-Galois structures on E/K as well. In that case, both of the extensions E/L and L/K are Galois, and one can prove that the classical Galois structures on L/E and E/K induce the classical Galois structure on L/K.

We see an equivalent approach to think of induced Hopf-Galois structures.

Proposition 2.5.28. *Let E/K be a Galois extension with group $G = J \rtimes G'$ and call $L = E^{G'}$, $M = L^J$. Then, the Hopf Galois structures of E/L and M/K are in one-to-one correspondence.*

Proof. Let $\overline{G} := \mathrm{Gal}(M/K)$. Applying the Galois correspondence to $G = J \rtimes G'$, we get $L \cap M = K$, so the map $\cdot\,|_M \colon G' \longrightarrow \overline{G}$ defined by $\tau \mapsto \tau\,|_M$ is a group isomorphism. Moreover, E/L is Galois with group G', and since J is normal in G, M/K is Galois with group $\overline{G}$. By Greither-Pareigis theorem, the Hopf Galois structures of E/L (resp. M/K) are in one-to-one correspondence with the regular subgroups of $\mathrm{Perm}(G')$ (resp. $\mathrm{Perm}(\overline{G})$) normalized by $\lambda^{G'}(G')$ (resp. $\lambda^{\overline{G}}(\overline{G})$). The map $\cdot\,|_F$ induces a group isomorphism $\varphi\colon \mathrm{Perm}(G') \longrightarrow \mathrm{Perm}(\overline{G})$ defined as $\varphi(\eta) = \cdot\,|_F \circ \eta \circ (\cdot\,|_F)^{-1}$.

Let N be a subgroup of $\mathrm{Perm}(G')$. Let us check that N is regular if and only if so is $\varphi(N)$. Since they have the same order as $\overline{G}$, it is enough to check that if N is transitive, so is $\varphi(N)$. Let $\tau\,|_F, \tau'\,|_F \in \overline{G}$. Since N is transitive, there is $\eta \in N$ such that $\eta(\tau) = \tau'$. Then, $\varphi(\eta)(\tau\,|_F) = \eta(\tau)\,|_F = \tau'\,|_F$.

We claim that the following diagram is commutative:

$$\begin{tikzcd}
G' \arrow[r, "\cdot|_M"] \arrow[d, "\lambda^{G'}"'] & \overline{G} \arrow[d, "\lambda^{\overline{G}}"] \\
\mathrm{Perm}(G') \arrow[r, "\varphi"] & \mathrm{Perm}(\overline{G})
\end{tikzcd} \tag{2.5}$$

Indeed, if $\tau, \tau' \in G'$,

$$\lambda^{\overline{G}}(\tau\,|_M)(\tau'\,|_M) = \tau\tau'\,|_M = \cdot\,|_M \circ \lambda^{G'}(\tau)(\tau') = \varphi(\lambda^{G'}(\tau))(\tau'\,|_M).$$

Then $\lambda^{\overline{G}}(\tau\,|_M) = \varphi(\lambda^{G'}(\tau))$, whence $\lambda^{\overline{G}} \circ\, |_M = \varphi \circ \lambda^{G}$, as we wanted. It follows that N is normalized by the image of $\lambda^{G'}$ if and only if $\varphi(N)$ is normalized by the image of $\lambda^{\overline{G}}$. □

We have shown in the proof that there is a group isomorphism $\mathrm{Perm}(G') \cong \mathrm{Perm}(\overline{G})$ such that a subgroup $N \leq \mathrm{Perm}(G')$ gives E/L a Hopf-Galois structure if and only if its image in $\mathrm{Perm}(\overline{G})$ gives M/K a Hopf-Galois structure. Thus, we can modify suitably the map ι to obtain a map $\mathrm{Perm}(J) \times \mathrm{Perm}(\overline{G}) \longrightarrow \mathrm{Perm}(G)$. By abuse of notation, we also call this map ι.

Corollary 2.5.29. *If N_1 is a regular subgroup of $\mathrm{Perm}(J)$ normalized by $\lambda_c(J)$ and N_2 is a regular subgroup of $\mathrm{Perm}(\overline{G})$ normalized by $\lambda^{\overline{G}}(\overline{G})$, then $\iota(N_1 \times N_2)$ is a regular subgroup of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$. Accordingly, from a Hopf-Galois structure on L/K and a Hopf-Galois structure on M/K, we obtain an induced Hopf-Galois structure on E/K.*

The advantage of this approach is that the description of the underlying Hopf algebra and the action of an induced Hopf-Galois structure arise naturally from those of the inducing Hopf-Galois structures.

Proposition 2.5.30. *Let E/K be a Galois extension with group $G = J \rtimes G'$, and call $L = E^{G'}$, $M = L^J$. Let H be an induced Hopf-Galois structure on L/K from inducing Hopf-Galois structures H_1 on L/K and H_2 on M/K.*

1. *There is an isomorphism of K-Hopf algebras $H \longrightarrow H_1 \otimes_K H_2$ between the underlying Hopf algebras of H and $H_1 \otimes_K H_2$.*

2. *Given $w \in H_1$, $\eta \in H_2$, $x \in L$ and $y \in M$,*

$$(w\eta) \cdot (xy) = (w \cdot x)(\eta \cdot y).$$

Proof. 1. Recall from Example 2.2.6 that the functor Φ transforms tensor products of K-algebras into cartesian products of sets, so Ψ does the other way around. Let $N_i = \Phi(H_i)$, $i \in \{1,2\}$. By definition of induced Hopf-Galois structure $\Phi(H) = N_1 \times N_2 = \Phi(H_1) \times \Phi(H_2)$. Applying Ψ, we get an isomorphism of K-Hopf algebras $H \cong H_1 \otimes_K H_2$.

2. Let us write $N_1 = \{\eta_i\}_{i=1}^n$ and $N_2 = \{\mu_j\}_{j=1}^m$. Then,

$$w \in H_1 = E[N_1]^G \Longrightarrow w = \sum_{i=1}^{r} c_i\eta_i, c_i \in E,$$

$$\eta \in H_2 = E[N_2]^G \Longrightarrow \eta = \sum_{j=1}^{u} d_j\mu_j,\ d_j \in E.$$

Hence,

$$\begin{aligned}(w\eta) \cdot (xy) &= \left(\sum_{i=1}^{n}\sum_{j=1}^{m} c_i d_j \iota(\eta_i, \mu_j)\right) \cdot (xy) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{m} c_i d_j \iota(\eta_i, \mu_j)^{-1}(\mathrm{Id}_G)(xy) = \sum_{i=1}^{n}\sum_{j=1}^{m} c_i d_j \iota(\eta_i^{-1}, \mu_j^{-1})(\mathrm{Id}_G)(xy) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{m} c_i d_j \eta_i^{-1}(\mathrm{Id}_J)(x)\mu_j^{-1}(\mathrm{Id}_{G'})(y) \\ &= \left(\sum_{i=1}^{n} c_i\eta_i^{-1}(\mathrm{Id}_J)(x)\right)\left(\sum_{j=1}^{m} d_j\mu_j^{-1}(\mathrm{Id}_{G'})(y)\right) \\ &= (w \cdot x)(\eta \cdot y)\end{aligned}$$

□

Remark 2.5.31. If L/K is any H-Galois extension, then we can define a K-linear map $\rho_H \colon H \longrightarrow \mathrm{End}_K(L)$ by $\rho_H(h)(x) = h \cdot x$. In the case that E/K is a Galois extension with group $G = J \rtimes G'$ and $H = H_1 \otimes_K H_2$ is an induced Hopf-Galois structure on E/K, Proposition 2.5.30 2 means that $\rho_H = \rho_{H_1} \otimes_K \rho_{H_2}$.

6 Exercises

6.1 Exercises on Sections 1-3

1. Give a direct proof that the fixed "set" $\mathrm{Fix}(A, H')$ under a sub-Hopf algebra $H' \subset H$ defined in Section 1 is a subalgebra of the H-Galois extension A.

2. (a) The symmetric group S_n of order $n!$ acts naturally on the set $\{1, \dots, n\}$. What is the stabilizer of an element in that set? (You may take the element n, for example.)

(b) The linear group $GL(n, K)$ acts naturally on the n-dimensional column space K^n. Describe the stabilizer of a non-zero column vector. (You may take for instance the first standard basis vector.)

(c) The special orthogonal group $SO(3, \mathbb{R})$ acts on $\mathbb{R}^3$. Can you describe the stabilizer of $e_1 = (1, 0, 0)^T$?

3. Assume that the group Γ acts on a set S, and that $s, t \in S$ are in the same orbit. Describe the relation between the stabilizer Γ_s of s and the stabilizer Γ_t of t. Is there any relation in general if s and t are in different orbits?

4. Suppose that $\Gamma = \Gamma_K$ acts on a finite set S such that the open subgroup U of finite index acts trivially. Show there is a normal subgroup $U' < U$ which is still open of finite index in Γ. (Hint: consider conjugates of U.)

5. In Section 2.5 we defined a certain Hopf algebra H^* and specific elements $c, s \in H^*$. Show that the two elements 1 and $h := (1, -1, 1, -1) = c^2 - s^2$ are the only group-like elements in H^*. What is the automorphism of L induced by h?

6. Find a base field K and a degree five polynomial f over it, such that the Galois group of f (i.e. of the splitting field of f) is A_5. Note that this splitting field is the normal closure of the extension L/K obtained by adjoining a root of f. (Any means are allowed: the literature, the Internet, your own ideas.)

7. In th context of Lemma 2.3.4, find two more equivalent conditions, now involving right translations ρ_w, with w in the group X.

8. Let C be a cyclic group of order p. Show that every group between $C = C \rtimes 1$ and $\mathrm{Hol}(C) = C \rtimes \mathrm{Aut}(C)$ has the form $C \rtimes \Delta$, where Δ is cyclic and $r = |\Delta|$ divides $p - 1$. Do all these r actually occur?

6.2 Exercises on Sections 4-5

1. Let L/K be a (G, G')-separable Hopf-Galois extension and let N_1, N_2 be regular and G-stable subgroups of $\mathrm{Perm}(G/G')$. Consider the action $*$ of G on N_1 and N_2 defined as conjugation by $\lambda(G)$. Show that $N_1 \cong N_2$ as G-groups (that is, there is a G-equivariant group isomorphism between them) if and only if $\widetilde{L}[N_1]^G \cong \widetilde{L}[N_2]^G$ as K-Hopf algebras.

2. Two Hopf-Galois structures $(H, \cdot)$, $(H', \cdot')$ on the same field extension L/K are said to be isomorphic if there is an isomorphism of K-Hopf algebras $f \colon H \longrightarrow H'$ such that $h \cdot \alpha = f(h) \cdot' \alpha$. In practice, isomorphic Hopf-Galois structures on L/K are considered as the same Hopf-Galois structure (for instance, in the Greither-Pareigis theorem).

   (a) Let L/K be a Galois extension with group G. Prove that the classical Galois structure on L/K and the Hopf-Galois structure corresponding to $\rho(G)$ under the Greither-Pareigis correspondence are isomorphic.

   (b) Give an example of separable Hopf-Galois extension L/K and different (non-isomorphic) Hopf-Galois structures H and H' on L/K such that $N \cong N'$, where N (resp. N') is the permutation subgroup corresponding to H (resp. H').

3. Let L/K be a Galois extension with group G and let N be a regular and G-stable subgroup of $\mathrm{Perm}(G)$. Show that for each $\varphi \in \mathrm{Aut}(G)$, $(\varphi \circ N \circ \varphi^{-1})^{\mathrm{opp}} = \varphi \circ N^{\mathrm{opp}} \circ \varphi^{-1}$.

4. Let L/K be a Galois extension with group G. For each regular and G-stable subgroup N of $\mathrm{Perm}(G)$ and each $g \in G$, call $N_g := \rho(g)N\rho(g^{-1})$. Two Hopf-Galois structures on L/K corresponding to permutation subgroups N, N' are said to be ρ-conjugate if $N' = N_g$ for some $g \in G$. Fix such a subgroup N of $\mathrm{Perm}(G)$ and $g \in G$.

   (a) Prove that N_g is indeed a regular and G-stable subgroup of $\mathrm{Perm}(G)$.

   (b) Show that the map $\phi\colon L[N]^G \longrightarrow L[N_g]^G$ defined by $\phi(\sum_{\eta \in N} c_\eta \eta) = \sum_{\eta \in N} c_\eta \rho(g)\eta\rho(g^{-1})$ is an isomorphism of K-Hopf algebras.

   (c) Prove that $N_g^{\mathrm{opp}} = (N^{\mathrm{opp}})_g$.

5. Prove that every separable field extension of degree at most 4 is almost classically Galois.

6. Let L/K be a (G, G')-separable almost classically Galois extension and let J be a normal complement for G' in G. Write $*$ for the action of G on $M[J]$ defined as the Galois action on M and the conjugation by G on J. Show that if J is abelian, then there is an isomorphism of Hopf-Galois structures between

$$M[J]^{G'} = \{h \in M[J] \mid \tau * h = h \text{ for all } \tau \in G'\}$$

   together with its classical action on L and the Hopf-Galois structure on L/K corresponding to $\lambda(J)$.

7. Consider the extension L/K at Example 2.5.7. Determine explicitly the Hopf-Galois structure associated to the permutation subgroup $N = \langle(\overline{1_G}, \overline{\sigma}, \overline{\sigma^2}, \overline{\sigma^3})\rangle$.

8. Let E/K be a Galois extension with group of the form $J \times G'$ and call $L = E^{G'}$. Prove that the classical Galois structure on E/K is the induced Hopf-Galois structure from the classical Galois structures on E/L and L/K.

Chapter 3

Hopf-Galois extensions in number theory

We have seen that a finite field extension L/K is Galois if and only if the canonical map $j\colon L \otimes_K K[G] \longrightarrow \mathrm{End}_K(L)$ is bijective, where $G = \mathrm{Aut}_K(L)$. This is a characterization of the Galois condition in terms of the action of G on L. Thus, we may wonder if any notion on Galois theory depending on the Galois action can be generalized or translated to Hopf-Galois theory. An example, already studied, is the Galois correspondence: the notion of fixed field by a subgroup is generalized to the one of fixed field by a sub-Hopf algebra, and there is a (weaker) Hopf-Galois version of the fundamental theorem of Galois theory.

In this chapter, we will use this idea to study a generalization of Galois module theory to the Hopf-Galois context. Galois module theory consists in the study of the ring of integers in a Galois extension L/K of number or p-adic fields as a module over an object depending on the Galois group of the extension. The behavior of such a module is closely linked with the ramification of the prime ideals in the extension, and hence falls directly into the domain of number theory. Moreover, such an object that will be the ground ring of the module is characterized in terms of the Galois action. Replacing it by the action of a Hopf-Galois structure is how the so called Hopf-Galois module theory arises.

1 Normal bases and normal basis generators

1.1 The normal basis theorem

A Galois module is an abelian group M receiving a group action from a Galois group in such a way that the operation of M is preserved by the action. For instance, a Galois field extension is a Galois module. The starting point of Galois module theory is the normal basis theorem, which makes use of this action so as to find a basis of the field.

Theorem 3.1.1 (Normal basis theorem). *Let L/K be a finite and Galois extension with Galois group G. Then, there is some element $\alpha \in L$ such that*

$$\{g(\alpha) \mid g \in G\}$$

is a K-basis of L.

In other words, the normal basis theorem asserts that a finite and Galois extension possesses a basis formed by the Galois conjugates of a single element α. Such a basis is called a normal basis, and consequently, α is called a normal basis generator. Of course, a normal basis generator is not necessarily unique: if α is a normal basis generator and $u \in K^\times$, then αu is also a normal basis generator. In fact, all normal basis generators of a Galois extension are of this form.

The normal basis theorem was first conjecture in the 19th century, and was proved in the first half of the 20th century. Even though it is not entirely clear who discovered the theorem, there is some consensus that the first uniform proof was given by Deuring in 1932. A complete proof can be found in [Coh93, Theorem 3.2.12].

We reformulate the normal basis theorem in a more convenient way for our purposes. Let L/K be a finite and Galois extension and suppose that α is a normal basis generator. Then, every $x \in L$ can be written uniquely as

$$x = \sum_{g \in G} x_g g(\alpha), \quad x_g \in K.$$

That is, x is a linear combination of the elements $g(\alpha)$ with unique scalar multiples $x_g \in K$. Now, let us change the perspective: we regard x as the result of let the element $h = \sum_{g\in G} x_g g \in K[G]$ act on α. The uniqueness of the x_g gives also the uniqueness of h in $K[G]$. This approach gives rise to the following equivalent statement.

Theorem 3.1.2 (Reformulation of the NBT). *Let L/K be a finite and Galois extension with Galois group G. Then, L is a free $K[G]$-module.*

Note that since both L and $K[G]$ are K-vector spaces of dimension $[L : K]$, L is of rank one as a free $K[G]$-module. It is through this reformulation how we generalize normal basis theorem.

1.2 A Hopf-Galois version of the normal basis theorem

Let L/K be a Hopf-Galois extension and let H be a Hopf-Galois structure on L/K. We know by definition that L is a left H-module algebra with respect to the action $\cdot$ of H on L; in particular it is an H-module.

Theorem 3.1.3. *Let L/K be an H-Galois extension. Then L is H-free of rank one.*

Proof. Since L/K is H-Galois, it is also an H^*-Galois object via the map $\beta \colon L \longrightarrow L \otimes_K H^*$ obtained from the action of H as in Proposition 1.2.46. Let us write the Sweedler-like notation for β as a coaction. On the other hand, we have an action of H on H^* defined by

$$h * f := \sum_{(f)} f_{(1)} \langle f_{(2)}, h \rangle, \quad h \in H,\ f \in H^*.$$

The map

$$\begin{array}{cccc} \gamma\colon & L \otimes_K L & \longrightarrow & L \otimes_K H^* \\ & x \otimes y & \longmapsto & \sum_{(y)} x y_{(0)} \otimes y_{(1)} \end{array}$$

is bijective. Now, consider the action of H on $L \otimes_K L$ via the second factor and the action of H on $L \otimes_K H^*$ defined by

$$h \cdot (x \otimes f) = (h \cdot x) \otimes (h * f).$$

Then, both $L \otimes_K L$ and $L \otimes_K H^*$ are H-modules. Now, given $x, y \in L$ and $h \in H$, we have

$$\begin{aligned}\gamma(x \otimes (h \cdot y)) &= \gamma\Big(x \otimes \Big(\sum_{(y)} y_{(0)} \langle y_{(1)}, h\rangle\Big)\Big)\\ &= \sum_{(y)} xy_{(0)} \otimes y_{(1)} \langle y_{(2)}, h\rangle\\ &= \sum_{(y)} xy_{(0)} \otimes h * y_{(1)}\\ &= h \cdot \gamma(x \otimes y).\end{aligned}$$

This proves that γ is a homomorphism of H-modules. Let $n = [L : K]$. We have that both L and H^* have dimension n as K-vector spaces. It follows that

$$L \oplus \overset{(n)}{\dots} \oplus L \cong H^* \oplus \overset{(n)}{\dots} \oplus H^*$$

as H-modules. Now, we can use Krull-Schmidt-Azumaya theorem, which ensures that both isomorphic H-modules decompose uniquely as H-modules. Necessarily $L \cong H^*$ as H-modules, and since $H^* \cong H$ as H-modules, we conclude that $L \cong H$ as H-modules, that is, L is free of rank one as an H-module. □

This proof of Theorem 3.1.3 comes from [Chi00, (2.16)]. In fact, it is possible to define the H-Galois condition for extensions of commutative rings, and the result as stated therein holds for such extensions.

If L/K is Galois and we choose H to be the classical Galois structure on L/K, then we recover the usual normal basis theorem. Following this analogy, we will say that any generator θ of L as an H-module generates an H-normal basis or that it is an H-normal basis generator.

1.3 Normal basis generators for Hopf-Galois extensions

Let L/K be a (G, G')-separable H-Galois extension with normal closure $\widetilde{L}$. Then we know that $H = \widetilde{L}[N]^G$ for some regular and G-stable subgroup N of $\mathrm{Perm}(G/G')$. It is possible to give a criterion for an element $\beta \in L$ to be an H-normal basis generator for L in terms of the elements of N and their action on L through the action of G. There is a first visible issue: since the elements of N are not typically elements of H. The strategy will be to tensorize H with $\widetilde{L}$ to obtain a space where the elements of N form a basis and the action is easy to calculate. Actually, this is the approach for the proof of Greither-Pareigis theorem given at [Chi00, Chapter 2], which we proceed to sketch.

Since the space $\widetilde{L} \otimes_K L$ is not especially convenient to work with, we shall identify it with $M := \mathrm{Maps}(G/G', \widetilde{L})$. An $\widetilde{L}$-basis of M is formed by the elements

$$u_{\overline{g}}(\overline{h}) = \delta_{\overline{g},\overline{h}}, \quad g, h \in G.$$

Consider the action of G on M given by

$$\sigma(f)(\overline{g}) = \sigma \circ f(\overline{\sigma^{-1} \circ g}), \quad \sigma, g \in G, \, f \in M.$$

Then M is a G-compatible $\widetilde{L}$-Hopf algebra.

Proposition 3.1.4 ([Chi00], (6.1))**.** *The map $\gamma \colon \widetilde{L} \otimes_K L \longrightarrow M$ defined by*

$$\gamma(x \otimes y)(\overline{\sigma}) = x\sigma(y)$$

is a G-equivariant isomorphism of K-algebras.

Note that by Theorem 2.4.14, $M \cong \widetilde{L} \otimes_K M^G$. But that the same time, the proposition gives a G-equivariant isomorphism $M \cong \widetilde{L} \otimes_K L$ as $\widetilde{L}$-algebras. We obtain then a G-equivariant isomorphism $\widetilde{L} \otimes_K L \cong \widetilde{L} \otimes_K M^G$ of $\widetilde{L}$-algebras. By descent, we get an isomorphism of K-algebras

$$\begin{array}{ccl} L & \longrightarrow & M^G, \\ x & \longmapsto & f_x := \sum_{\overline{g} \in G/G'} \overline{g}(x) u_{\overline{g}}. \end{array} \tag{3.1}$$

Let H be a Hopf-Galois structure on L/K. By [Chi00, (6.3)], there is a regular subgroup N of $\mathrm{Perm}(G/G')$ such that $\widetilde{L} \otimes_K H = \widetilde{L}[N]$. In addition, M is an $\widetilde{L}[N]$-Galois extension of $\widetilde{L}$ (of rings). Thus, we have an action of $\widetilde{L}[N]$ on M, which acquires a special form on the elements $u_{\overline{g}}$.

Lemma 3.1.5. *Let L/K be a (G, G')-separable H-Galois extension and let N be the corresponding permutation subgroup. Then, there is a group action of N on M such that for each $\eta \in N$ and each $\overline{g} \in G/G'$, there is a unique $\eta(\overline{g}) \in G/G'$ with $\eta(u_{\overline{g}}) = u_{\eta(\overline{g})}$.*

This result is inserted in the proof of [Chi00, (6.3)]. By translating this expression of the action by descent to the action of H on L, we get the description given at Proposition (2.3). On the other hand, the equality $H = \widetilde{L}[N]^G$ is also obtained via the equivalence of categories at 2.4.14.

In order to give a criterion for an element of L to be an H-normal basis generator, we prove that we can raise it to M. Note that since M is an $\widetilde{L}[N]$-Galois extension of $\widetilde{L}$ and the generalization of the normal basis theorem also holds for this case, it makes sense to consider $\widetilde{L}[N]$-normal basis generators at M.

Lemma 3.1.6. *An element $x \in L$ is an H-normal basis generator for L if and only if f_x is an $\widetilde{L}[N]$-normal basis generator for M.*

Proof. Fix $x \in L$. Suppose that $L = H \cdot x$. Applying the isomorphism at (3.1), we obtain $M^G = \widetilde{L}[N]^G \cdot f_x$. Since $\widetilde{L} \otimes_K M^G = M$ and $\widetilde{L} \otimes_K \widetilde{L}[N]^G = \widetilde{L}[N]$, tensorizing by $\widetilde{L}$ yields $M = \widetilde{L}[N] \cdot f_x$. Conversely, assume that $M = \widetilde{L}[N] \cdot f_x$. Since the action $\cdot$ is G-equivariant and $f_x \in M^G$, $M^G = (\widetilde{L}[N] \cdot f_x)^G = \widetilde{L}[N]^G \cdot f_x$, whence $L = H \cdot x$. □

Next, we characterize the $\widetilde{L}[N]$-normal basis generators for M and carry them to L.

Proposition 3.1.7. *An element $x \in L$ is an H-normal basis generator for L if and only if the matrix*

$$T_N(x) := (\eta(\overline{g})(x))_{\eta \in N, \overline{g} \in G/G'}$$

is non-singular.

Proof. Fix $x \in L$. By Lemma 3.1.6, $L = H \cdot x$ if and only if $M = \widetilde{L}[N] \cdot f_x$. By standard linear algebra, this happens if and only if the matrix whose columns are the coordinates of the elements $\eta \cdot f_x$ (where η runs through N) is non-sigular. Now, given $\eta \in N$,

$$\begin{aligned}\eta \cdot f_x &= \eta \cdot \Big(\sum_{\overline{g} \in G/G'} \overline{g}(x) u_{\overline{g}} \Big) \\ &= \sum_{\overline{g} \in G/G'} \overline{g}(x) u_{\eta(\overline{g})} \\ &= \sum_{\overline{g} \in G/G'} \eta^{-1}(\overline{g})(x) u_{\overline{g}}\end{aligned}$$

We obtain that the aforemetioned matrix is $T_N(x)$ up to a permutation of the rows, whence the statement follows. □

An interesting application is that a Hopf-Galois extension have the same normal basis generators for opposite Hopf-Galois structures.

Proposition 3.1.8. *Let L/K be an H-Galois extension. Then x is an H-normal basis generator for L if and only if x is an H^{opp}-normal basis generator for L.*

Proof. Let G and G' be such that L/K is (G, G')-separable. Let N be the regular and G-stable subgroup of $\text{Perm}(G/G')$ corresponding to H. Recall that N^{opp} is identified with the centralizer of N in $\text{Perm}(G/G')$. We shall show that $T_N(x)$ is non-singular if and only if $T_{N^{\text{opp}}}(x)$ is non-singular. Let $n = [L : K]$ and write $G/G' = \{\overline{g_j}\}_{j=1}^n$. For each $1 \leq j \leq n$, let η_j (resp. η'_j) be the element of N (resp. N') such that $\eta_j(\overline{1}) = \overline{g_j}$ (resp. $\eta'_j(\overline{1}) = \overline{g_j}$). Then

$$\begin{aligned}\det(T_N(x)) &= \det((\eta_i(\overline{g_j}))_{i,j=1}^n) \\ &= \det((\eta_i \circ \eta'_j(\overline{g_1}))_{i,j=1}^n) \\ &= \det((\eta'_j \circ \eta_i(\overline{g_1}))_{i,j=1}^n) \\ &= \det((\eta'_j(\overline{g_i}))_{i,j=1}^n) \\ &= \det(T_{N^{\text{opp}}}(x)^t) \\ &= \det(T_{N^{\text{opp}}}(x)).\end{aligned} \tag{3.2}$$

□

Corollary 3.1.9. *Let L/K be a Galois extension. An element $x \in L$ is an H_c-normal basis generator for L if and only if it is an H_λ-normal basis generator for L.*

2 Elements of algebraic number theory

Prior to the introduction of Galois module theory for rings of integers and its generalization to Hopf-Galois theory, we shall view some basic notions on algebraic number theory that we will need. The main references for this section are [LL07, Chapters 23-25] and [Neu99, Chapter 2].

2.1 Dedekind domains and their fraction fields

Dedekind domains are rings whose ideals have a similar arithmetic as the integer numbers. The study of ideals historically arose from the study of Fermat's last theorem. Particularly, there was an interest in studying whether rings of integers of number fields possess the unique factorization property. In the end, it was found that the answer is negative (for instance, $6 = 3 \cdot 2 = (1+\sqrt{-5})(1-\sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$, which is the ring of integers of $\mathbb{Q}(\sqrt{-5})$ because $-5 \equiv 3 \pmod 4$)). In view of this behavior, Kummer introduced the so called ideal numbers, which also capture the integer multiples, and proved that for this there is a unique factorization property. This derived into the modern notion of ideal of a ring.

Proposition 3.2.1 ([Rib72], Chapter 7, Theorem 1)**.** *Let A be an integral domain. The following statements are equivalent:*

1. *A is Noetherian, integrally closed and with Krull dimension 1 (that is, every non-zero prime ideal of A is maximal).*

2. *For every ideal I of A, there are unique prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ of A and unique non-negative integers $\alpha_1, \dots, \alpha_r$ such that $I = \prod_{i=1}^{r} \mathfrak{p}_i^{\alpha_i}$.*

Definition 3.2.2. *Every integral domain R satisfying the equivalent conditions at Proposition 3.2.1 is called a* ***Dedekind domain****.*

Let A be a Dedekind domain. The product of ideals in A somehow imitates the product of integer numbers. The condition 2 means that each ideal of A factorizes as a product of prime ideals with non-negative exponents. Moreover, the trivial ideal A is the identity for this product. Integer numbers admit multiplicative inverses as soon as we introduce the rational numbers in the picture. Let us see that something similar happens for Dedekind domains. Let $K = \mathrm{Frac}(A)$. The modules of the form

$$\alpha I, \quad \alpha \in K^{\times},\ I \text{ ideal of } A$$

are called fractional ideals of A. The ideals of A are also fractional ideals, and in this context often receive the name of integral ideals. Each fractional ideal (including the integral ones) admits an inverse for the product, and consequently each fractional ideal factorizes uniquely as a product of prime ideals of A with non-necessarily non-negative exponents.

Dedekind domains are of our interest because they include the rings of integers of number fields and p-adic fields, for any prime p. For this reason, it is useful to work with the fields of fractions of Dedekind domains, and the extensions of such fields. Let K be the field of fractions of a Dedekind domain $\mathcal{O}_K$, let L be a finite and separable field extension of K and let $\mathcal{O}_L$ be the integral closure of $\mathcal{O}_K$ in L (so that L is the fraction field of $\mathcal{O}_L$). In short, we will write that L/K is an *extension associated to Dedekind domains*. In such a situation, $\mathcal{O}_L$ is again a Dedekind domain (see [Neu99, Proposition 8.1]).

2.1.1 Trace, norm and discriminant

Definition 3.2.3. *Let L/K be an extension associated to Dedekind domains. Let $n = [L : K]$, let $\sigma_1, \dots, \sigma_n$ be the K-embeddings of L and let $\alpha \in L$.*

1. *The trace of α is defined as $\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$.*
2. *The norm of α is defined as $\mathrm{N}_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$.*

Note that the trace and the norm of an element $\alpha \in L$ lie in K, and they even lie in $\mathcal{O}_K$ if $\alpha \in \mathcal{O}_L$. Furthermore, for any tower of fields $K \leq E \leq L$, we have

$$\mathrm{Tr}_{L/K} = \mathrm{Tr}_{E/K} \circ \mathrm{Tr}_{L/E}, \quad \mathrm{N}_{L/K} = \mathrm{N}_{E/K} \circ \mathrm{N}_{L/E}.$$

Definition 3.2.4. *Let L/K be a degree n extension of number fields and let $\sigma_1, \dots, \sigma_n$ be the K-embeddings of L. The **discriminant** of an n-uple $(\alpha_1, \dots, \alpha_n) \in L^n$ is defined as*

$$\mathrm{disc}_{L/K}(\alpha_1, \dots, \alpha_n) = \det((\sigma_i(\alpha_j))_{i,j=1}^{n})^2.$$

The discriminant also admits the expression

$$\mathrm{disc}_{L/K}(\alpha_1, \dots, \alpha_n) = \det((\mathrm{Tr}_{L/K}(\alpha_i\alpha_j))_{i,j=1}^{n}).$$

If $K \leq E \leq L$ is a tower of fields, then

$$\mathrm{disc}_{L/K}(\alpha_1, \dots, \alpha_n) = \mathrm{disc}_{E/K}(\alpha_1, \dots, \alpha_n)^n \mathrm{N}_{E/K}(\mathrm{disc}_{L/E}(\alpha_1, \dots, \alpha_n)).$$

Proposition 3.2.5. *Let L/K be a degree n extension of number fields. Given $\alpha_1, \dots, \alpha_n \in L$, $\mathrm{disc}(\alpha_1, \dots, \alpha_n) \neq 0$ if and only if $\alpha_1, \dots, \alpha_n$ are K-linearly independent.*

Given $\alpha \in L$, we denote $\mathrm{disc}_{L/K}(\alpha) \equiv \mathrm{disc}_{L/K}(1, \alpha, \dots, \alpha^{n-1})$. If $f = \text{min.poly.}(\alpha, K)$, then $\mathrm{disc}_{L/K} = \mathrm{disc}(f)$, where the discriminant of f is defined as just after Proposition 1.1.49.

In all the cases where no ambiguity arise, we may omit subscripts.

2.1.2 Bases of Dedekind domains

This section is motivated by the following result:

Proposition 3.2.6 ([MR89], Corollary to Theorem 11.7)**.** *Let L/K be an extension associated to Dedekind domains. Then, $\mathcal{O}_L$ is finitely generated as an $\mathcal{O}_K$-module.*

If such an extension L/K happens to be free, it admits some finite basis.

Definition 3.2.7. *Let L/K be an extension associated to Dedekind domains and assume that $\mathcal{O}_L$ is free as an $\mathcal{O}_K$-module. We shall refer to an $\mathcal{O}_K$-basis for $\mathcal{O}_L$ as an **integral basis** for L/K or a K-integral basis for L.*

It is well known that finitely generated torsion-free modules over principal ideal domains (PID) are free. If we assume that $\mathrm{char}(K) = 0$ and that $\mathcal{O}_K$ is a PID, then L/K admits some integral basis.

The discriminant is an invariant of the integral bases: if $\{\beta_i\}_{i=1}^{n}$ and $\{\gamma_j\}_{j=1}^{n}$ are integral bases for L/K, then $\mathrm{disc}(\beta_1, \dots, \beta_n) = \mathrm{disc}(\gamma_1, \dots, \gamma_n)$ (see [Chi00, (22.3)]; there it is proved for a more general notion of discriminant for algebras over commutative rings). Thus, the following concept makes sense.

Definition 3.2.8. *Let L/K be an extension associated to Dedekind domains and suppose that $\mathcal{O}_L$ is $\mathcal{O}_K$-free. The discriminant of L/K, denoted $\mathrm{disc}(L/K)$, is defined as the discriminant of an integral basis for L.*

2.2 Number fields and their rings of integers

Recall that number fields are defined as the finite field extensions of the field $\mathbb{Q}$ of rational numbers. The ring of integers of a number field L is the set of algebraic integers (roots of monic polynomials with integer coefficients) inside L. Any number field is the fraction field of its ring of integers. It is known that the ring of integers of a number field is a Dedekind domain (see for example [Mar77, Theorem 14]). Then, we can consider the notions of trace, norm and discriminant for number fields, and ideals of rings of integers decompose uniquely as products of prime ideals.

2.2.1 Integral bases

Let L/K be an extension of number fields. Since L/K is an extension associated to Dedekind domains, if we assume that $\mathcal{O}_K$ is a PID, we have that $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of rank $n := [L : K]$. Then, we can consider K-integral bases of $\mathbb{Q}$. In particular, all of this applies when $K = \mathbb{Q}$ (so that we consider just a number field L), because $\mathbb{Z}$ is a PID. In that case, we just talk about integral bases for L.

Example 3.2.9. Let $L = \mathbb{Q}(\sqrt{m})$ be a quadratic field. Then, an integral basis for L is

$$\begin{cases} \{1, \frac{1+\sqrt{m}}{2}\} & \text{if } m \equiv 1 \pmod 4, \\ \{1, \sqrt{m}\} & \text{if } m \equiv 2, 3\, (\mathrm{mod}, 4). \end{cases}$$

Example 3.2.10. Let $L = \mathbb{Q}(\zeta_m)$ be the m-th cyclotomic field. Then, an integral basis for L is

$$\{\zeta_m^k \mid 1 \leq k \leq m, \, \gcd(k, m) = 1\}.$$

Consequently, $\mathcal{O}_L = \mathbb{Z}[\zeta_m]$.

Both quadratic and cyclotomic fields have the property that their rings of integers are generated as $\mathbb{Z}$-algebras as a single element.

Definition 3.2.11. *A number field L is said to be* ***monogenic*** *if there is some element $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathbb{Z}[\alpha]$.*

It turns out that monogenic number fields are extremely uncommon, and the problem of characterizing the monogenity for a family of number fields is often extraordinarily difficult.

2.2.2 Ramification of primes of a number field

Now, suppose that we have an extension L/K of number fields and $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$. Then

$$\mathfrak{p}\mathcal{O}_L = \Big\{ \sum_{i=1}^{s} \alpha_i \beta_i \mid \alpha_i \in \mathfrak{p}, \, \beta_i \in \mathcal{O}_L \Big\}$$

is clearly an ideal of $\mathcal{O}_L$. Thus, it factorizes uniquely as a product of prime ideals. The features of the primes that appear in such a factorization is what we understand by the ramification of a prime ideal of $\mathcal{O}_K$.

At this point, for any number field E, we will refer to a prime ideal of $\mathcal{O}_E$ just as a prime of E.

Definition 3.2.12. *Let L/K be an extension of number fields. Let $\mathfrak{p}$ be a prime of K and let $\mathfrak{P}$ be a prime of L. We will say that $\mathfrak{P}$ lies over $\mathfrak{p}$, or that $\mathfrak{p}$ lies under $\mathfrak{P}$, if $\mathfrak{p} = \mathfrak{P} \cap K$.*

While for a prime $\mathfrak{p}$ of K there may be several primes of L lying over $\mathfrak{p}$ (the ones at the factorization of $\mathfrak{p}\mathcal{O}_L$), for each prime $\mathfrak{P}$ of L, there is a unique prime of K lying under $\mathfrak{P}$; namely $\mathfrak{p} := \mathfrak{P} \cap K$.

Definition 3.2.13. *Let L/K be an extension of number fields. Let $\mathfrak{p}$ be a prime of K and let $\mathfrak{P}$ be a prime of L over $\mathfrak{p}$.*

1. *The* ***ramification index*** *of $\mathfrak{P}$ over $\mathfrak{p}$, denoted $e(\mathfrak{P}/\mathfrak{p})$, is defined as the exponent of $\mathfrak{P}$ in the factorization of $\mathfrak{p}\mathcal{O}_L$.*

2. *The* ***inertia degree*** *of $\mathfrak{P}$ over $\mathfrak{p}$ is defined as $f(\mathfrak{P}/\mathfrak{p}) = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$.*

The inertia degree is well defined because the inclusion $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$ induces a field monomorphism $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{P}$.

The following states that both the ramification index and the inertia degree are multiplicative by towers.

Proposition 3.2.14 ([Mar77], Chapter 3, Exercise 10)**.** *Let $K \leq E \leq L$ be a tower of number fields and consider a tower of primes $\mathfrak{p}_K \leq \mathfrak{p}_E \leq \mathfrak{p}_L$ inside. Then*

$$e(\mathfrak{p}_L/\mathfrak{p}_K) = e(\mathfrak{p}_L/\mathfrak{p}_E)e(\mathfrak{p}_E/\mathfrak{p}_K),$$

$$f(\mathfrak{p}_L/\mathfrak{p}_K) = f(\mathfrak{p}_L/\mathfrak{p}_E)f(\mathfrak{p}_E/\mathfrak{p}_K).$$

Moreover, we have a basic relation of these objects with the degree of the extension to which they refer.

Theorem 3.2.15 ([Mar77], Chapter 3, Theorem 21)**.** *Let L/K be a degree n extension of number fields. Let $\mathfrak{p}$ be a prime of K and let $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ the primes of L lying over $\mathfrak{p}$. Then*

$$n = \sum_{i=1}^{r} e(\mathfrak{P}_i/\mathfrak{p}) f(\mathfrak{P}_i/\mathfrak{p})$$

This gives an upper bound for the possible values of the ramification index and the inertia degree of each prime over $\mathfrak{p}$, as well as for the amount of primes at the factorization of $\mathfrak{p}\mathcal{O}_L$.

We establish some terminology that will be appearing repeatedly.

Definition 3.2.16. *Let L/K be a degree n extension of number fields and let $\mathfrak{p}$ be a prime of K. We say that $\mathfrak{p}$ is:*

1. ***Ramified*** *at a prime $\mathfrak{P}$ of L over $\mathfrak{p}$, if $e(\mathfrak{P}/\mathfrak{p}) > 1$. We will also say that $\mathfrak{p}$ is ramified in L if it is so at some prime of L lying over $\mathfrak{p}$.*

2. ***Unramified*** *at a prime $\mathfrak{P}$ of L, if it is not ramified at $\mathfrak{P}$. Likewise, we say that it is unramified in L if it is not ramified in L.*

3. ***Totally ramified*** *in L, if there is some prime $\mathfrak{P}$ of L such that $e(\mathfrak{P}/\mathfrak{p}) = n$.*

4. ***Split*** *in L, if there is more than a prime of L over $\mathfrak{p}$. Otherwise, we say that $\mathfrak{p}$ is* ***non-split*** *in L.*

5. ***Inert*** *in L, if $\mathfrak{p}\mathcal{O}_L$ is a prime ideal of $\mathcal{O}_L$.*

6. ***Totally split*** *in L, if in the factorization of $\mathfrak{p}\mathcal{O}_L$ there are n distinct primes of L.*

7. ***Tamely ramified*** *at a prime $\mathfrak{P}$ of L over $\mathfrak{p}$, if $p \nmid e(\mathfrak{P}/\mathfrak{p})$, where p is the rational prime under $\mathfrak{p}$. If $\mathfrak{p}$ is tamely ramified at all primes of L, we will say that $\mathfrak{p}$ is tamely ramified in L.*

8. ***Wildly ramified*** *at a prime $\mathfrak{P}$ of L, if it is not tamely ramified at $\mathfrak{P}$. We will also say that it is wildly ramified in L if it is not tamely ramified in L.*

The condition that $\mathfrak{p}$ is totally ramified in L means that there is exactly one prime $\mathfrak{P}$ of L over $\mathfrak{p}$, for which $e(\mathfrak{P}/\mathfrak{p}) = n$ and $f(\mathfrak{P}/\mathfrak{p}) = 1$. The condition that $\mathfrak{p}$ is inert also implies that there is exactly one prime $\mathfrak{P}$ of L over $\mathfrak{p}$, but in this case $e(\mathfrak{P}/\mathfrak{p}) = 1$ and $f(\mathfrak{P}/\mathfrak{p}) = n$. Both situations are particular cases of the non-split one, in which we just know that $e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}) = n$. The condition that $\mathfrak{p}$ is totally split means that there are exactly n primes $\mathfrak{P}_1, \dots, \mathfrak{P}_n$ of L over $\mathfrak{p}$ and $e(\mathfrak{P}_i/\mathfrak{p}) = f(\mathfrak{P}_i/\mathfrak{p}) = 1$ for all $1 \leq i \leq n$.

An important remark is that the ramified primes of a number field can be characterized arithmetically and, in particular, they are a finite number.

Theorem 3.2.17. *Let L be a number field and let p be a rational prime. Then p is ramified in L if and only if $p \mid \operatorname{disc}(L)$.*

We finish the section by discussing tamely ramified extensions, which are very interesting from the point of view of number theory, as they can be connected with other arithmetic invariants of an extension.

Proposition 3.2.18. *Let L be an abelian number field. Then $L/\mathbb{Q}$ is tamely ramified if and only if there exists $n \in \mathbb{Z}_{\geq 1}$ odd and square-free such that $L \subset \mathbb{Q}(\zeta_n)$.*

This result is related with the commonly known as the Kronecker-Webber theorem: every abelian number field is contained in some cyclotomic extension. It is easy to check that the if $n \mid m$, the n-th cyclotomic field is contained in the m-th cyclotomic field. The minimal integer n for which an abelian number field L is contained in the n-th cyclotomic field is called the conductor of L. Thus, Proposition 3.2.18 means that tamely ramified extensions are the abelian number fields with odd and square-free conductor.

2.3 Extensions of p-adic fields and their ramification

Let p be a prime number. The beginning of the theory of p-adic fields is the introduction of the field $\mathbb{Q}_p$ of p-adic numbers, which is obtained by adjoining to $\mathbb{Q}$ the limits of the rational Cauchy sequences with respect to the p-adic absolute value $|\cdot|_p \colon \mathbb{Q} \longrightarrow \mathbb{R}_{\geq 0}$. We view briefly this construction.

Absolute values and valuations

Definition 3.2.19. *Let L be a field. An **absolute value** on L is a map $|\cdot| \colon L \longrightarrow \mathbb{R}_{\geq 0}$ with the following properties:*

1. *For any element $a \in L$, $|a| = 0$ if and only if $a = 0$.*

2. $|ab| = |a||b|$ *for every* $a, b \in L$.

3. $|a + b| \leq |a| + |b|$ *for every* $a, b \in L$.

If $|L^\times|$ is discrete with respect to the usual topology of the real line, we say that $|\cdot|$ is discrete. In that case, it can be proved that $|\cdot|$ is non-archimedean, that is,

$$|a + b| \leq \max(|a|, |b|) \quad \text{for every } a, b \in L,$$

which is a stronger property than (3).

Definition 3.2.20. *Let L be a field. A* ***valuation*** *on L is a map* $v \colon L \longrightarrow \mathbb{R} \cup \{\infty\}$ *such that:*

1. *For any element* $a \in L$, $v(a) = \infty$ *if and only if* $a = 0$.

2. $v(ab) = v(a) + v(b)$ *for every* $a, b \in L$.

3. $v(a + b) \geq \min\{v(a), v(b)\}$ *for every* $a, b \in L$.

Non-archimedean absolute values and valuations on a field L correspond to each other by the equality $|x| = c^{v(x)}$ for every $x \in L^\times$, where $c \in (0, 1)$. The condition that $|\cdot|$ is discrete translates into $v(L) \subseteq \mathbb{Z}$, in which case we also say that v is discrete.

An absolute value on a field induces a metric, and hence a topology. If a field equipped with an absolute value contains all the limits of Cauchy sequences, we will say that it is **complete**. Any field L with an absolute value can be completed by adjoining the limits of Cauchy sequences. The field obtained in this procedure is what we understand by the completion of L. Formally:

Definition 3.2.21. *Let L be a field and let* $|\cdot|$ *be an absolute value on L. A* ***completion*** *of* $(L, |\cdot|)$ *is a pair* $(\widehat{L}, \widehat{|\cdot|})$ *where* $\widehat{L}$ *is a field containing L and* $\widehat{|\cdot|}$ *is an absolute value on* $\widehat{L}$ *such that:*

1. *The restriction of* $\widehat{|\cdot|}$ *to L coincides with* $|\cdot|$.

2. *L is dense in* $\widehat{L}$ *with respect to* $\widehat{|\cdot|}$.

3. $(\widehat{L}, \widehat{|\cdot|})$ *is a complete metric space.*

Theorem 3.2.22 ([LL07], Chapter 23, Theorem 2)**.** *Let K be a field and let* $|\cdot|$ *be an absolute value on K. Then a completion of* $(K, |\cdot|)$ *exists and is unique up to absolute-value-preserving K-isomorphism.*

The field $\mathbb{Q}_p$ of p-adic numbers

Let p be a prime number. On $\mathbb{Q}$, we can define $|\cdot|_p \colon \mathbb{Q} \longrightarrow \mathbb{R}_{\geq 0}$ as $|0|_p = 0$ and, for any non-zero $a \in \mathbb{Q}$, as

$$|a|_p = p^{-v_p(a)},$$

where $v_p(a)$ is the exponent of p in the factorization of a. This is a discrete absolute value, the so-called ***p*-adic absolute value**. Consequently, $v_p \colon \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$ is a discrete valuation. In fact, $v_p(\mathbb{Q}) = \mathbb{Z}$. The field $\mathbb{Q}_p$ is defined as the completion of $\mathbb{Q}$ with the p-adic absolute value.

2.3.1 The structure of p-adic fields

For a prime p, p-adic fields can be seen as the analogues of number fields for $\mathbb{Q}_p$.

Definition 3.2.23. *A p-**adic field** is a finite field extension of $\mathbb{Q}_p$.*

As in the case of number fields, since the field $\mathbb{Q}_p$ has characteristic zero, it is perfect, so every extension of p-adic fields is separable.

By [LL07, Chapter 23, Theorem 4], absolute values of a complete field can be uniquely extended to an absolute value on a field extension. Moreover, extensions of discrete absolute values are discrete. Consequently, any p-adic field L can be endowed with a discrete absolute value $|\cdot|_L$, from which we can define a valuation v_L, which we refer to as the L-valuation.

Valuation rings

We state the following result it for p-adic fields, but it actually holds for a larger class of fields.

Proposition 3.2.24 ([LL07], Chapter 23, F4)**.** *Let L be a p-adic field.*

1. *$\mathcal{O}_L := \{a \in L \mid v_L(a) \geq 0\}$ is a subring of L, called the **valuation ring of** L.*
2. *$\mathfrak{p}_L := \{a \in L \mid v_L(a) = 0\}$ is an ideal of $\mathcal{O}_L$, called the **valuation ideal of** L.*
3. *An element $u \in \mathcal{O}_L$ is a unit if and only if $v_L(u) = 0$, so $\mathfrak{p}_L$ is a maximal ideal of $\mathcal{O}_L$.*
4. *$\kappa_L := \mathcal{O}_L/\mathfrak{p}_L$ is a field, called the **residue field** of L.*

The valuation ring of $\mathbb{Q}_p$ is denoted by $\mathbb{Z}_p$, commonly known as the ring of p-adic integers. It can be obtained as the projective limit

$$\mathbb{Z}_p = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}.$$

From [LL07, Chapter 23, Theorem 4′], we have that any element $\alpha \in \overline{\mathbb{Q}_p}$ is integral over $\mathbb{Z}_p$ if and only if min.poly.$(\alpha, \mathbb{Q}_p) \in \mathbb{Z}_p[x]$. Thus, for any p-adic field L, the elements of the valuation ring $\mathcal{O}_L$ of L are the elements of L that are integral over $\mathbb{Z}_p$. Hence, we can regard valuation rings as a p-adic analogue of rings of integers in number fields.

The residue field κ_L of a p-adic field is always finite and possesses characteristic p. This is the reason why some authors identify the case of p-adic fields as the *mixed characteristic case*.

Discrete structure

The valuation ring of a p-adic field is a **discrete valuation ring** (DVR), that is, a PID that possesses a unique prime ideal. All discrete valuation rings are Dedekind domains. In the case of a p-adic field L, the only prime ideal is the valuation ideal $\mathfrak{p}_L$.

An element of a p-adic field L with L-valuation 1 is called a **uniformizer** of L. We shall denote it by π_L. It is unique up to multiplication by units. Consequently, every $x \in L$ is expressed as

$$x = \pi_L^{v_L(x)} u$$

for some $u \in \mathcal{O}_L^\times$. If we make a choice of the uniformizer, u is unique. It holds that $\mathfrak{p}_L = \pi_L\mathcal{O}_L$. We deduce that for every ideal I of $\mathcal{O}_L$, there is a unique $e \in \mathbb{Z}_{\geq 0}$ such that $I = \mathfrak{p}_L^e$. In the case of $\mathbb{Z}_p$, the uniformizer (up to multiplication by units) is p. Unlike in the case of extensions of number fields, the extensions of p-adic fields L/K always admit an integral basis. This is because $\mathcal{O}_K$ is a DVR, and hence a PID.

Adic completions of number fields

It is possible to describe p-adic fields as completions of number fields. Let K be a number field and let $\mathfrak{p}$ be a prime of K. For each $a \in K^\times$, let $v_\mathfrak{p}(a)$ be the exponent of $\mathfrak{p}$ at the factorization of the fractional ideal $a\mathcal{O}_K$. Together with the rule $v_\mathfrak{p}(0) = \infty$, this defines a function $v_\mathfrak{p} \colon K \longrightarrow \mathbb{R} \cup \{\infty\}$ which turns out to be a discrete valuation on K. Let $K_\mathfrak{p}$ be the completion of K with respect to the absolute value coming from $v_\mathfrak{p}$. It turns out that $K_\mathfrak{p}$ is a p-adic field, where p is the rational prime under $\mathfrak{p}$. Conversely, every p-adic field is the completion of some number field (see [LL07, Chapter 25, F3]). The valuation ring of $K_\mathfrak{p}$ is the completion $\mathcal{O}_{K,\mathfrak{p}}$ of $\mathcal{O}_K$ with respect to $\mathfrak{p}$, that is, the result of adjoining to $\mathcal{O}_K$ all limits of Cauchy sequences in $\mathcal{O}_K$.

If L is a finite Galois extension of K, then

$$L_\mathfrak{p} := L \otimes_K K_\mathfrak{p} \cong \prod_{\mathfrak{P} | \mathfrak{p}\mathcal{O}_L} L_\mathfrak{P},$$

where $\mathfrak{P}$ runs through the primes of L dividing $\mathfrak{p}\mathcal{O}_L$. In particular, $L_\mathfrak{p}$ is a field (in which case, it is a p-adic field) if and only if $\mathfrak{p}$ is non-split in L. At the integral level, we have

$$\mathcal{O}_{L,\mathfrak{p}} := \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_{K,\mathfrak{p}} \cong \prod_{\mathfrak{P} | \mathfrak{p}\mathcal{O}_L} \mathcal{O}_{L,\mathfrak{P}}$$

(see [FT92, Theorem 17]). Note that $\mathcal{O}_{L,\mathfrak{p}}$ is already defined when $L_\mathfrak{p}$ is a field as the ring of integers of $L_\mathfrak{p}$, but this is consistent with the definition above.

2.3.2 Ramification at extensions of p-adic fields

Since the valuation rings of p-adic fields contain a unique prime ideal, the ramification theory for extensions of p-adic fields can be seen, roughly speaking, as an analogue of the one for number fields with a unique prime ideal. For this reason, we will talk of ramification of extensions, rather than ramification of primes.

Definition 3.2.25. *Let L/K be an extension of p-adic fields.*

1. *The **ramification index** of L/K, denoted $e(L/K)$, is the integer number defined by the equality $\mathfrak{p}_K\mathcal{O}_L = \mathfrak{p}_L^{e(L/K)}$.*
2. *The **residue class degree** of L/K, denoted $f(L/K)$, is defined as the degree of the extension κ_L/κ_K of residue fields.*

We list a couple of facts that are as in the case of number fields.

Proposition 3.2.26. *1. Let $K \leq E \leq L$ be a tower of p-adic fields. Then*

$$e(L/K) = e(L/E)e(E/K), \quad f(L/K) = f(L/E)f(L/K).$$

2. *Let L/K be an extension of p-adic fields. Then*
$$[L:K] = e(L/K)f(L/K).$$

Now, we set some terminology related with ramification following the style of Definition 3.2.16.

Definition 3.2.27. *Let L/K be an extension of p-adic fields. We say that L/K is:*

1. ***Ramified**, if $e(L/K) > 1$. Otherwise, we say that L/K is **unramified**.*

2. ***Totally ramified**, if $e(L/K) = [L:K]$.*

3. ***Tamely ramified**, if $p \nmid e(L/K)$. Otherwise, we say that L/K is **wildly ramified**.*

The condition that L/K is unramified means equivalently that $f(L/K) = [L:K]$. Then the extension of residue fields κ_L/κ_K is as large as possible, and it is Galois because residue fields are finite. One can prove that in this case the K-automorphisms of L identify with the elements of $\mathrm{Gal}(\kappa_L/\kappa_K)$. From this, one can reach the following important conclusion.

Proposition 3.2.28. *Every unramified extension of p-adic fields is cyclic (in particular, Galois).*

On the other side, totally ramified extensions are those for which $f(L/K) = 1$, so the extensions of residue fields is trivial. In that case, we have that $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$, that is, the valuation ring $\mathcal{O}_L$ is generated by a uniformizer π_L as an $\mathcal{O}_K$-algebra. There is a sufficient condition for this situation, which is convenient in practice.

Proposition 3.2.29 ([FT92], Theorem 24)**.** *Let L/K be an extension of p-adic fields. If $\alpha \in L$ is a primitive element of L/K which is a root of some π_K-Eisenstein polynomial, then L/K is totally ramified and α is a uniformizer of L.*

For example, the 3-adic field $L = \mathbb{Q}(\alpha)$ with $\alpha^3 + 3 = 0$ is totally ramified and has α as uniformizer.

Recall from Theorem 3.2.17 that the rational primes dividing the discriminant of a number field are the ramified ones. This result can be translated to the setting of p-adic fields, but the uniqueness of prime ideal makes the situation much simpler: the discriminant of an extension of p-adic fields is a power of the prime ideal, and it will be the full ring of integers if and only if the extension is unramified.

3 Hopf-Galois module theory over fields

3.1 The Galois case

Recall that normal basis theorem asserts that every finite and Galois extension admits a normal basis, that is, a basis formed by the Galois conjugates of a single element. Equivalently, the top field is free of rank one as a module over the ground field. Now, assume that L/K is a Galois extension associated to Dedekind domains and assume that $\mathcal{O}_L$ is $\mathcal{O}_K$-free. Then, we may wonder whether there is some normal basis for L/K which is integral, or equivalently, if $\mathcal{O}_L$ is free as an $\mathcal{O}_K[G]$-module, where $G = \mathrm{Gal}(L/K)$. The answer is that not in general.

Example 3.3.1. Let $L = \mathbb{Q}(\sqrt{2})$, which is a Galois extension over $\mathbb{Q}$ with group $G = \langle\sigma\rangle$, $\sigma(\sqrt{2}) = -\sqrt{2}$. Suppose that there is some $\alpha \in L$ such that $\mathcal{O}_L = \mathbb{Z}[G] \cdot \alpha$. We know that $\mathcal{O}_L = \mathbb{Z}[\sqrt{2}]$, so $1 \in \mathbb{Z}[G] \cdot \alpha$. Let $a, b \in \mathbb{Z}$ be such that $\alpha = a + b\sqrt{2}$. Then there are $\lambda, \mu \in \mathbb{Z}$ such that

$$1 = \lambda(a + b\sqrt{2}) + \mu(a - b\sqrt{2}) = (\lambda + \mu)a + (\lambda - \mu)b\sqrt{2}.$$

Therefore,

$$\begin{cases} (\lambda + \mu)a = 1, \\ (\lambda - \mu)b = 0. \end{cases}$$

From the second equality we deduce that $\lambda = \mu$. Carrying this to the first one, we get $2\lambda a = 1$. This implies that $\lambda = \frac{1}{2a} \in \mathbb{Z}$ with $a \in \mathbb{Z}$, which is a contradiction. Hence no normal basis of $L/\mathbb{Q}$ is integral.

However, there are extensions where it is the other way around.

Example 3.3.2. Let $L = \mathbb{Q}(\sqrt{5})$. As in the previous example, the Galois group G is generated by the order 2 automorphism $\sigma\colon \sqrt{5} \mapsto -\sqrt{5}$. However, in this case, $\mathcal{O}_L = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. Now, we have that

$$1 = \frac{1+\sqrt{5}}{2} + \frac{1-\sqrt{5}}{2} = \frac{1+\sqrt{5}}{2} + \sigma\Big(\frac{1+\sqrt{5}}{2}\Big).$$

Hence the normal basis

$$\Big\{\frac{1+\sqrt{5}}{2}, \sigma\Big(\frac{1+\sqrt{5}}{2}\Big)\Big\}$$

for $L/\mathbb{Q}$ is also integral.

We put the natural name for bases with this property.

Definition 3.3.3. *Let L/K be an extension associated to Dedekind domains. A **normal integral basis** (NIB) is a normal basis for L/K that in addition is integral.*

By definition, normal integral bases only arise when $\mathcal{O}_L$ is $\mathcal{O}_K$-free (which involves no restriction for the p-adic case). On the other hand, it is immediate that L/K admits a NIB if and only if $\mathcal{O}_L$ is free as an $\mathcal{O}_K[G]$-module. Since both $\mathcal{O}_L$ and $\mathcal{O}_K[G]$ are free $\mathcal{O}_K$-modules of rank $[L : K]$, if $\mathcal{O}_L$ is free as an $\mathcal{O}_K[G]$-module, necessarily it is of rank one.

Let L/K be a finite and Galois extension of number fields and let $\mathfrak{p}$ be a prime of K. Recall that the completion $K_{\mathfrak{p}}$ is a p-adic field with valuation ring $\mathcal{O}_{K,\mathfrak{p}}$. Moreover, $\mathcal{O}_{K,\mathfrak{p}}[G] = \mathcal{O}_K[G] \otimes_{\mathcal{O}_K} \mathcal{O}_{K,\mathfrak{p}}$. We know that $L_{\mathfrak{p}}$ is a field if and only if $\mathfrak{p}$ is non-split in L, and in that case, $\mathcal{O}_{L,\mathfrak{p}} = \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_{K,\mathfrak{p}}$. Even if $L_{\mathfrak{p}}$ is not a field, we can define $\mathcal{O}_{L,\mathfrak{p}} := \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_{K,\mathfrak{p}}$. Now, $\mathcal{O}_{L,\mathfrak{p}}$ admits a natural structure of $\mathcal{O}_{K,\mathfrak{p}}[G]$-module, and we may wonder whether it is free.

Definition 3.3.4. *Let L/K be a Galois extension of number fields. We say that $\mathcal{O}_L$ is $\mathcal{O}_K[G]$-locally free if $\mathcal{O}_{L,\mathfrak{p}}$ is free as an $\mathcal{O}_{K,\mathfrak{p}}[G]$-module for every prime $\mathfrak{p}$ of K.*

Note that for every prime $\mathfrak{p}$ of K, $\mathcal{O}_{K,\mathfrak{p}}$ is a flat $\mathcal{O}_K$-module. Hence, for a Galois extension of number fields L/K with group G, if $\mathcal{O}_L$ is $\mathcal{O}_K[G]$-free, then $\mathcal{O}_L$ is $\mathcal{O}_K[G]$-locally free. The converse in general does not hold.

The existence of a NIB for extensions of p-adic fields was characterized by Emmy Noether in [Noe32].

Theorem 3.3.5 (Noether). *An extension of p-adic fields admits a normal integral basis if and only if it is tamely ramified.*

In the case of G-Galois extensions of number fields L/K, Noether's theorem says that $\mathcal{O}_L$ is $\mathcal{O}_K[G]$-locally free if and only if L/K is tamely ramified.

Theorem 3.3.5 is satisfactory in the sense that it provides a characterization for a behavior for the ring of integers in an extension of p-adic fields, which is an optimal result from a point of view. But at the same time it is unsatisfactory, because its scope is very limited; namely, it does not capture wildly ramified extensions.

3.2 Associated orders in Hopf-Galois extensions

It is possible to broaden the range of extensions under study by replacing $\mathcal{O}_K[G]$ by a suitable algebraic structure to serve as the ground ring for a module structure for $\mathcal{O}_L$. That suitable object is an $\mathcal{O}_K$-order in a K-algebra.

Definition 3.3.6. *Let K be the fraction field of a Dedekind domain $\mathcal{O}_K$ and let A be a K-algebra. We say that a unitary subring $\mathfrak{A}$ of A is an $\mathcal{O}_K$-order in A if:*

1. *$\mathfrak{A}$ is finitely generated as an $\mathcal{O}_K$-module.*
2. *$\mathfrak{A} \otimes_{\mathcal{O}_K} K = A$.*

If L/K is a Galois extension with group G, $\mathcal{O}_K[G]$ is an $\mathcal{O}_K$-order in $K[G]$ acting on $\mathcal{O}_L$. But instead, we consider directly a more general situation. Let L/K be an H-Galois extension associated to Dedekind domains. Then, we can look for $\mathcal{O}_K$-orders in H acting on $\mathcal{O}_L$. If L/K is separable, we have the following analogue of $\mathcal{O}_K[G]$.

Proposition 3.3.7. *Let L/K be a (G,G')-separable H-Galois extension associated to Dedekind domains. Let N be the regular and G-stable subgroup of* $\mathrm{Perm}(G/G')$ *such that $H = \widetilde{L}[N]^G$. Then $\mathcal{O}_{\widetilde{L}}[N]^G$ is an $\mathcal{O}_K$-order in H.*

Proof. First, note that since the Galois action leaves algebraic integers invariant inside a field, $\mathcal{O}_{\widetilde{L}}[N]^G$ is well defined. On the other hand, $\mathcal{O}_{\widetilde{L}}[N]^G \subset \mathcal{O}_{\widetilde{L}}[N]$, which is $\mathcal{O}_K$-finitely generated because so is $\mathcal{O}_{\widetilde{L}}$ by Proposition 3.2.6. Since $\mathcal{O}_K$ is Noetherian, $\mathcal{O}_{\widetilde{L}}[N]^G$ is finitely generated. Finally, we check that $\mathcal{O}_{\widetilde{L}}[N]^G \otimes_{\mathcal{O}_K} K = H$. Since $\mathcal{O}_{\widetilde{L}}$ is a finitely generated torsion-free $\mathcal{O}_K$-module, there is $d \in \mathcal{O}_K - \{0\}$ such that $d\widetilde{L} \subset \mathcal{O}_{\widetilde{L}}$. Now, let $W = \{w_1, \dots, w_n\}$ be a K-basis of H. Then for each $1 \leq i \leq n$, we have that $dw_i \in \mathcal{O}_{\widetilde{L}}[N] \cap \widetilde{L}[N]^G = \mathcal{O}_{\widetilde{L}}[N]^G$, and $dW = \{dw_1, \dots, dw_n\}$ is a K-basis of H because W is and $d \neq 0$. This finishes the proof. □

For a Galois extension L/K with group G, if we take $N = \rho(G)$ (i.e, the classical Galois structure), we recover $\mathcal{O}_K[G]$.

It is immediate that $\mathcal{O}_{\widetilde{L}}[N]^G$ acts on $\mathcal{O}_L$. However, in many situations presents severe limitations, just as $\mathcal{O}_K[G]$ in the Galois case. Instead, we consider the set of all elements in H acting on $\mathcal{O}_L$.

Definition 3.3.8. *Let L/K be an H-Galois extension associated to Dedekind domains. The* ***associated order*** *of $\mathcal{O}_L$ in H is defined as*

$$\mathfrak{A}_H := \{h \in H \mid h \cdot \mathcal{O}_L \subset \mathcal{O}_L\}.$$

If L/K is Galois with group G and H is the classical Galois structure on L/K, we obtain the associated order in $K[G]$, which we denote by $\mathfrak{A}_{L/K}$. Its study lies in the field of Galois module theory. Since we are working in a more general situation, everything we are going to state is also valid in that case.

Proposition 3.3.9. *The associated order $\mathfrak{A}_H$ of H in L is an $\mathcal{O}_K$-order in H.*

Proof. Let θ be an H-normal basis generator for L and let $\mathfrak{A}_\theta = \{h \in H \mid h \cdot \theta \in \mathcal{O}_L\}$, which is clearly an $\mathcal{O}_K$-module. From $L = H \cdot \theta$ we get immediately that $\mathfrak{A}_\theta \cdot \theta = \mathcal{O}_L$, and then the map $\mathfrak{A}_\theta \longrightarrow \mathcal{O}_L$ defined by $h \mapsto h \cdot \theta$ is an isomorphism of $\mathcal{O}_K$-modules. Since, by Proposition 3.2.6, $\mathcal{O}_L$ is finitely generated as an $\mathcal{O}_K$-module, we deduce that so is $\mathfrak{A}_\theta$. Now, $\mathfrak{A}_H \subset \mathfrak{A}_\theta$ and $\mathcal{O}_K$ is Noetherian, whence it follows that $\mathfrak{A}_H$ is finitely generated as an $\mathcal{O}_K$-module.

It remains to check that $\mathfrak{A}_H \otimes_{\mathcal{O}_K} K = H$, or equivalently, $\mathfrak{A}_H$ contains a K-basis of H. Let N be the permutation subgroup corresponding to H, so that $H = \widetilde{L}[N]^G$. From Exercise 4, we have $\mathcal{O}_{\widetilde{L}}[N]^G \subseteq \mathfrak{A}_H$. Now, by Proposition 3.3.7, $\mathcal{O}_{\widetilde{L}}[N]^G$ contains a K-basis of H, and hence so does $\mathfrak{A}_H$. □

We may wonder whether the associated order $\mathfrak{A}_H$ is $\mathcal{O}_K$-free. The condition that $\mathcal{O}_L$ is $\mathcal{O}_K$-free is not enough to ensure the $\mathfrak{A}_H$-freeness of $\mathcal{O}_L$.

Example 3.3.10. Let $K = \mathbb{Q}(\sqrt{-6})$ and $L = K(\sqrt{1+2\sqrt{-6}})$. The extension L/K is quadratic, so it is Galois with group $G \cong C_2$. It can be checked that $\mathcal{O}_L$ is $\mathcal{O}_K$-free but $\mathfrak{A}_{L/K}$ is not.

However, the $\mathcal{O}_K$-freeness of $\mathfrak{A}_H$ holds if we assume that $\mathcal{O}_K$ is a PID (which holds for instance if K is a p-adic field or a number field with class number 1; in particular $\mathbb{Q}$).

The ring $\mathcal{O}_L$ admits a natural structure of $\mathfrak{A}_H$-module. Suppose that both $\mathcal{O}_L$ and $\mathfrak{A}_H$ are free $\mathcal{O}_K$-modules. Then both of them have rank $[L:K]$. If $\mathcal{O}_L$ is free as an $\mathfrak{A}_H$-module, it has rank one. The associated order is the right ground ring of a module structure for $\mathcal{O}_L$, due to the following result.

Proposition 3.3.11. *Suppose that both $\mathcal{O}_L$ and $\mathfrak{A}_H$ are free as $\mathcal{O}_K$-modules and let $\mathfrak{A}$ be an $\mathcal{O}_K$-order in H such that $\mathcal{O}_L$ is $\mathfrak{A}$-free. Then $\mathfrak{A} = \mathfrak{A}_H$.*

Proof. It is enough to prove that $\mathfrak{A}_H \subseteq \mathfrak{A}$, since the other inclusion trivially follows from the fact that $\mathfrak{A}_H$ is the maximal $\mathcal{O}_K$-order in H acting on $\mathcal{O}_L$. Suppose that $\mathcal{O}_L = \mathfrak{A} \cdot \alpha$ and let $\lambda \in \mathfrak{A}_H$. Then $\lambda \cdot \alpha \in \mathcal{O}_L = \mathfrak{A} \cdot \alpha$, so there is some $h \in \mathfrak{A}$ such that $\lambda \cdot \alpha = h \cdot \alpha$. But this is an equality in $L = H \cdot \alpha$, so necessarily $\lambda = h \in \mathfrak{A}$. □

This result shows that the associated order $\mathfrak{A}_H$ is the only $\mathcal{O}_K$-order over which $\mathcal{O}_L$ may possibly be $\mathfrak{A}_H$-free. However, there are examples with different behaviors. Thus, we consider the following problem.

Problem 3.3.12. *Let L/K be an H-Galois extension associated to Dedekind domains and suppose that $\mathcal{O}_L$ and $\mathfrak{A}_H$ are free as $\mathcal{O}_K$-modules. Find a necessary and sufficient condition for $\mathcal{O}_L$ being free as an $\mathfrak{A}_H$-module.*

Research in this area so far has focused in two directions:

1. How freeness in a Hopf-Galois structure affects in others, especially in the case of Galois extensions.

2. Freeness in Hopf-Galois extensions that are not Galois.

We see a result belonging to the first of these two items.

Proposition 3.3.13. *Let L/K be an H-Galois extension associated to Dedekind domains. Then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free if and only if it is $\mathfrak{A}_{H^{\mathrm{opp}}}$-free.*

Proof. It is enough to prove one implication as $(H^{\mathrm{opp}})^{\mathrm{opp}} = H$. Suppose that $\mathcal{O}_L$ is $\mathfrak{A}_H$-free and let $x \in \mathcal{O}_L$ be an $\mathfrak{A}_H$-free generator of $\mathcal{O}_L$. By Proposition 3.1.8, x is a free generator of L as an H^{opp}-module. Thus for each $a \in \mathfrak{A}_H$ there is $z_a \in H^{\mathrm{opp}}$ such that $a \cdot x = z_a \cdot x$.

Let us show that $z_a \in \mathfrak{A}_{H^{\mathrm{opp}}}$. Let $y \in \mathcal{O}_L$. Since $\mathcal{O}_L$ is $\mathfrak{A}_H$-free, there is a unique $b \in \mathfrak{A}_H$ such that $y = b \cdot x$. Since the elements of H and H^{opp} commute by definition of the latter, we have

$$z_a \cdot y = z_a \cdot (b \cdot x) = b \cdot (z_a \cdot x) = b \cdot (a \cdot x).$$

Since $a, b \in \mathfrak{A}_H$, we conclude that $z_a \cdot y \in \mathcal{O}_L$.

Let $z \in \mathfrak{A}_{H^{\mathrm{opp}}}$. Then $z \cdot x \in \mathcal{O}_L = \mathfrak{A}_H \cdot x$, so there is some $a \in \mathfrak{A}_H$ such that $z \cdot x = a \cdot x = z_a \cdot x$. Since this lies in $L = H \cdot x$, necessarily $z = z_a$. We obtain that

$$\mathfrak{A}_{H^{\mathrm{opp}}} = \{z_a \mid a \in \mathfrak{A}_H\},$$

whence x is an $\mathfrak{A}_{H^{\mathrm{opp}}}$-free generator of $\mathcal{O}_L$. □

Corollary 3.3.14. *Let L/K be a Galois non-abelian extension associated to Dedekind domains. Then $\mathcal{O}_L$ is $\mathfrak{A}_{H_c}$-free if and only if $\mathfrak{A}_{H_\lambda}$-free.*

We close the section with an interaction between freeness over an associated order and induced Hopf-Galois structures. Let E/K be a Galois extension with group $G = J \rtimes G'$ and call $L = E^{G'}$ and $M = E^J$. Recall by Proposition 2.5.30 that an induced Hopf-Galois structure on E/K is of the form $H = H_1 \otimes_K H_2$, where H_1 (resp. H_2) is a Hopf-Galois structure on L/K (resp. M/K). We may wonder if the same relation holds for the corresponding associated orders, that is, $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}$. The answer is negative in general, but there is a sufficient condition.

Definition 3.3.15. *We say that two extensions L_1/K and L_2/K associated to Dedekind domains are **arithmetically disjoint** if they are linearly disjoint and their discriminants are coprime.*

Proposition 3.3.16 ([FT92], Chapter III, (2.13))**.** *If two field extensions L_1/K and L_2/K are arithmetically disjoint, then $\mathcal{O}_{L_1L_2} = \mathcal{O}_{L_1} \otimes_{\mathcal{O}_K} \mathcal{O}_{L_2}$.*

Under arithmetic disjointness, the freeness over the associated order in an induced Hopf-Galois structure behaves as one could expect.

Theorem 3.3.17. *Let E/K be a Galois extension associated to Dedekind domains with group $G = J \rtimes G'$ and call $L = E^{G'}$ and $M = E^{J}$.Suppose that $\mathcal{O}_K$ is a PID and that L/K and M/K are arithmetically disjoint. Let $H = H_1 \otimes_K H_2$ be an induced Hopf-Galois structure on L/K. Then:*

1. *$\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}$.*

2. *If $\mathcal{O}_L$ is $\mathfrak{A}_{H_1}$-free and $\mathcal{O}_M$ is $\mathfrak{A}_{H_2}$-free, then $\mathcal{O}_E$ is $\mathfrak{A}_H$-free.*

Note that 2 follows easily from 1 by using Proposition 3.3.16. The same result also yields easily that $\mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2} \subseteq \mathfrak{A}_H$. However, the converse inclusion is not trivial. A complete proof can be found at [GR22b, Section 5], and consists in applying a method to build a basis of the associated order in a Hopf-Galois structure. An alternative proof is offered at [Tru25, Proposition 6.5] using techniques related with skew braces, algebraic structures with a ring-like definition (but a twisted distributive property) that were introduced so as to construct set-theoretical solutions to the Yang-Baxter equation. This is just another one among the endeless applications of the connection between skew braces and Hopf-Galois structures hinted by Bachiller at [Bac16] and formalized in the appendix by Byott and Vendramin at [SV18].

If $G = J \times G'$ and H_1 (resp. H_2) is the classical Galois structure on L/K (resp. M/K), Exercise 8 from Section 6.2 yields that H is the classical Galois structure on L/K. If we specialize Theorem 3.3.17 to this case, we get that $\mathfrak{A}_{E/K} = \mathfrak{A}_{L/K} \otimes_{\mathcal{O}_K} \mathfrak{A}_{M/K}$. This was previously stated at [BL96, Lemma 5], but without the restriction that $\mathcal{O}_K$ is a PID.

4 Hopf-Galois module theory over rings

The study of Problem 3.3.12 concerns extensions of Dedekind domains whose fraction fields are a Hopf-Galois extension. In this section, we present some notions and results belonging to Hopf-Galois module theory that focus rather in the rings than in the fields. In some cases, we can actually remove the fields from the picture. The main (but not unique) source is [Chi00, Chapter 3].

As in Chapter 1, we fix a commutative ring R with unity.

4.1 H-Galois extensions of rings

First, we establish a Hopf-Galois condition for extensions of rings. It has the same flavor as the one for field extensions, but we require both the ring extension and the Hopf algebra to be finite (finitely generated and projective). Namely, let H be a cocommutative R-Hopf algebra and let S be a commutative R-algebra, both finite as R-modules.

Definition 3.4.1. *We say that S is H-Galois if there is an R-linear action $\cdot \colon H \otimes S \longrightarrow S$ endowing S with left H-module algebra structure such that the canonical map $j \colon S \otimes H \longrightarrow \mathrm{End}_R(H)$ is an R-linear isomorphism.*

As already mentioned, we have a normal basis theorem in this context.

Theorem 3.4.2. *Suppose that R is complete, local and Noetherian. If S is H-Galois, then it is H-free.*

The proof of Theorem 3.1.3 remains valid for this case, since the hypotheses imposed on R are the ones needed so that Krull-Schmidt-Azumaya theorem can be applied.

Remark 3.4.3. If S is $R[G]$-Galois for some finite group G, we say that S is a Galois extension of R. Several characterizations for this condition can be consulted at [Chi00, (2.5)]. One of them is that for every maximal ideal $\mathfrak{m}$ of S and every $\sigma \in G$, $\sigma \neq 1_G$, there is some $s \in S$ such that $\sigma(s) - s \notin \mathfrak{m}$. If S and R are rings of integers of number fields L and K, this is equivalent to the condition that all primes $\mathfrak{p}$ of K being unramified in L. Likewise, if the fields are p-adic, the equivalence is with L/K being unramified.

We know that $j\colon L \otimes_K H \longrightarrow \operatorname{End}_R(S)$ is an homomorphism of R-modules. It is possible to introduce an alternative internal product on $S \otimes H$ so that j becomes a homomorphism of R-algebras.

Definition 3.4.4. *The **smash product** $S\#H$ of S and H is the R-algebra with underlying R-module $S \otimes_R H$ and multiplication given by*

$$(s\#h)(t\#h') = \sum_{(h)} s(h_{(1)} \cdot t)\#h_{(2)}h'.$$

It is easy (but long) to check that this product endows $S\#H$ with R-algebra structure.

Proposition 3.4.5. *The map $j\colon S\#H \longrightarrow \operatorname{End}_R(S)$ is a homomorphism of R-algebras.*

Proof. If $s \otimes h, t \otimes h' \in S\#H$, then for all $u \in S$,

$$\begin{aligned}
j(s\#h) \circ j(t\#h')(u) &= j(s\#h)(t(h' \cdot u)) \\
&= s(h \cdot (t(h' \cdot u))) \\
&= s\left(\sum_{(h)} (h_{(1)} \cdot t)(h_{(2)} \cdot (h' \cdot u))\right) \\
&= \sum_{(h)} s(h_{(1)} \cdot t)((h_{(2)}h') \cdot u) \\
&= \sum_{(h)} j(s(h_{(1)} \cdot t)\#h_{(2)}h')(u) \\
&= j\Big(\sum_{(h)} s(h_{(1)} \cdot t)\#h_{(2)}h'\Big)(u) \\
&= j((s\#h)(t\#h'))(u).
\end{aligned}$$

Thus, $j(s\#h) \circ j(t\#h') = j((s\#h)(t\#h'))$. □

Since H acts on S, we can consider the elements that are *fixed* in the sense of actions from Hopf algebras.

Definition 3.4.6. *The **fixed subring** of S by H is defined as*

$$S^H = \{s \in S \mid h \cdot s = \varepsilon_H(h)s \text{ for all } h \in H\}.$$

In the case that L/K is an H-Galois field extension, we have that $L^H = K$. There is an analogous result for the case of rings.

Lemma 3.4.7. *Let R be a commutative ring with unity and let S be a commutative R-algebra which is finite as an R-module. The center of $\mathrm{End}_R(S)$ is formed by the homothecies by elements of $u_S(R)$.*

Proof. Let $\phi \in Z(\mathrm{End}_R(S))$. By definition, ϕ commutes with all the R-endomorphisms of S; in particular it commutes with the ones of the form $x \mapsto sx$, where $s \in S$. We get that $s\phi(x) = \phi(sx)$ for all $s \in S$, so $\phi \in \mathrm{End}(S)$. Hence, $\phi(x) = \phi(1_S)x$ for all $x \in S$.

Call $t = \phi(1_S)$. We shall prove that $t \in u_S(R)$. For each $f \in S^*$, let $\psi_f \colon S \longrightarrow S$ be defined by $\psi_f(x) = f(x)1_S$. Then $\psi_f \in \mathrm{End}_R(S)$, so $\phi \circ \psi_f = \psi_f \circ \phi$. Given $x \in S$,

$$\phi \circ \psi_f(x) = \phi(f(x)1_S) = f(x)t,$$

$$\psi_f \circ \phi(x) = f \circ \phi(x)1_S = f(tx)1_S.$$

We get $tf(x) = f(tx)1_S$ for all $f \in S^*$ and $s \in S$.

Let $\{s_i, f_i\}_{i=1}^n$ be a projective coordinate system of S. For each $1 \leq j \leq n$, let $\{a_{kj}\}_{k=1}^n \subset R$ be such that $ts_j = \sum_{k=1}^n a_{kj}s_k$. Applying f_i for each $1 \leq i \leq n$, we get $f_i(ts_j) = \sum_{k=1}^n a_{kj}\delta_{ik} = a_{ij}$. The unit map u_S maps this equality to $f_i(ts_j)1_S = a_{ij}1_S$. Now, by the previous paragraph,

$$f_i(ts_j)1_S = tf_i(s_j) = t\delta_{ij}.$$

Hence $t\delta_{ij} = a_{ij}1_S$ for all $1 \leq i, j \leq n$, whence $t = a_{ii}1_S \in u_S(R)$ for every $1 \leq i \leq n$, finishing the proof. □

Proposition 3.4.8. *If S is an H-Galois extension, then $S^H = u_S(R)$.*

Proof. Let $r \in R$. Then, for all $h \in H$,

$$h \cdot u_S(r) = h \cdot (r1_S) = r(h \cdot 1_S) = r\varepsilon_H(h)1_S = \varepsilon_H(h)u_S(r).$$

This proves that $u_S(R) \subseteq S^H$. Let us prove the converse. Let $s \in S^H$. Then, for all $t\#h \in S\#H$,

$$\begin{aligned}
(s\#1)(t\#h) &= st\#h \\
&= st\#\left(\sum_{(h)} \varepsilon_H(h_{(1)})h_{(2)}\right) \\
&= \sum_{(h)} ts\#\varepsilon_H(h_{(1)})h_{(2)} \\
&= \sum_{(h)} t(\varepsilon_H(h_{(1)})s)\#h_{(2)} \\
&= \sum_{(h)} t(h_{(1)} \cdot s)\#h_{(2)} \\
&= (t\#h)(s\#1),
\end{aligned}$$

where we have used that $\varepsilon_H(h_{(1)})s = h_{(1)} \cdot s$ because $s \in S^H$. Since j is an homomorphism of R-algebras, $j(s\#1) \circ j(t\#h) = j(t\#h) \circ j(s\#1)$ for all $t\#h \in S\#H$. We deduce that $j(s\#1)$ lies in the center of $\mathrm{End}_R(S)$. By Lemma 3.4.7, every element in the center of $\mathrm{End}_R(S)$ is multiplication by an element of $u_S(R)$. Then, there is $r \in R$ such that for every $t \in S$,

$$u_S(r)t = j(s\#1_H)(t) = st.$$

We conclude that $s = u_S(r) \in u_S(R)$. □

Rank of a projective module

If L/K is a field H-Galois extension, we know that $\dim_K(L) = \dim_K(H)$. In our case, if we assume that both S and H are R-free, then it follows directly that $\mathrm{rank}_R(H) = \mathrm{rank}_R(S)$. It is even possible to introduce a notion of rank for finite R-modules, so that we can reach the same conclusion without further restrictions on S and H. We follow the development in [Bou72, Chapter 2, Section 5]. The key result is the following:

Theorem 3.4.9 ([Bou72], Chapter 2, Section 5.2, Theorem 1)**.** *An R-module M is finite if and only if the following conditions are satisfied:*

1. *M is a finitely generated R-module.*
2. *For every $\mathfrak{p} \in \mathrm{Spec}(R)$, the localization $M_\mathfrak{p}$ is R-free.*
3. *The function $\mathrm{rank}_R(M)\colon \mathrm{Spec}(R) \longrightarrow \mathbb{Z}_{\geq 0}$, $\mathrm{rank}_R(M)(\mathfrak{p}) = \mathrm{rank}_{R_\mathfrak{p}}(M_\mathfrak{p})$ is locally constant when we consider the Zariski topology in $\mathrm{Spec}(R)$.*

This result seems to be unsatisfactory for our purposes: an R-module may have many ranks; concretely, one rank for each connected component of $\mathrm{Spec}(R)$. To fulfill this difficulty, we add the hypothesis that $\mathrm{Spec}(R)$ is connected. This is equivalent to the absence of non-trivial idempotents in R. We write in short that R is connected.

With the hypothesis that R is connected, the function $\mathrm{rank}_R(M)$ is constant, so that its value does not depend on the prime ideal P we choose.

Definition 3.4.10. *Suppose that R is connected and let M be a finite R-module. We define the **rank of** M as*

$$\mathrm{rank}_R(M) := \mathrm{rank}_{R_\mathfrak{p}}(M_\mathfrak{p}),$$

where $\mathfrak{p} \in \mathrm{Spec}(R)$.

The rank of projective modules extends the usual rank for free modules since the localization of a free module is a free module with the same rank. Moreover, it has to be finite because the localization of a finite module is a finitely generated free module.

Note that both rings of integers of number fields and valuation rings of p-adic fields are connected because they do not possess non-trivial idempotent elements. On the other hand, local rings are always connected because they do not have non-trivial idempotents. Then, the notion of rank for a projective module applies in those situations.

These considerations also have an immediate consequence: some basic relations that concern the classic notion of rank are naturally generalized to this situation.

Proposition 3.4.11. *Suppose that R is connected. Let M and N be finite R-modules. Then:*

1. $\text{rank}_R(M \otimes_R N) = \text{rank}_R(M)\,\text{rank}_R(N)$.

2. $\text{rank}_R(M \oplus N) = \text{rank}_R(M) + \text{rank}_R(N)$.

3. $\text{rank}_R(M) = \text{rank}_R(M^*)$.

We assume now that R is complete, local and Noetherian (in particular R is connected). From Theorem 3.4.2 we know that S is H-free of rank one, whence it follows that $\text{rank}_R(S) = \text{rank}_R(H)$.

4.2 Integrals of a Hopf algebra

Let H be an R-Hopf algebra. If M is a left H-module, the submodule fixed by H is defined as

$$M^H = \{m \in M \mid hm = \varepsilon(h)m \text{ for all } h \in H\}.$$

Now, H is endowed with the trivial left and right H-module structures, so we may consider its fixed elements under such actions.

Definition 3.4.12. *Let H be an R-Hopf algebra.*

1. *A **left integral** in H is an element $\theta \in H$ such that $h\theta = \varepsilon(h)\theta$ for every $h \in H$.*

2. *A **right integral** in H is an element $\theta \in H$ such that $\theta h = \varepsilon(h)\theta$ for every $h \in H$.*

We shall write $\int_H^l$ for the set of left integrals of H and $\int_H^r$ for the set of right integrals of H.

The trivial left H-module structure of H is given by the product in its underlying algebra, so $\int_H^l$ is a two-sided ideal of H:

$$h'(h\theta) = (h'h)\theta = \varepsilon(h'h)\theta = \varepsilon(h')\varepsilon(h)\theta = \varepsilon(h')h\theta \implies h\theta \in \int_H^l,$$

$$h'(\theta h) = (h'\theta)h = \varepsilon(h')\theta h \implies \theta h \in \int_H^l.$$

Definition 3.4.13. *We say that an R-Hopf algebra H is **unimodular** if its module of left integrals coincides with its module of right integrals.*

If an R-Hopf algebra H is commutative or it is a finite R-group algebra, then it is unimodular.

Example 3.4.14. Let G be a finite group and let us consider the R-Hopf algebra $R[G]$. Let $\theta = \sum_{\sigma\in G}\sigma$. Then, for $\tau \in G$,

$$\theta\tau = \left(\sum_{\sigma\in G}\sigma\right)\tau = \sum_{\sigma\in G}\sigma\,\tau = \theta = \varepsilon_{R[G]}(\tau)\theta,$$

and similarly,

$$\tau\theta = \theta = \varepsilon_{R[G]}(\tau)\theta.$$

Since G is a basis of $R[G]$ and multiplication by θ is R-linear, it is true for every element of $R[G]$. Then, θ is both left and right integral of $R[G]$. A straightforward computation shows that in fact $\int_{R[G]}^{r}$ and $\int_{R[G]}^{l}$ are generated by θ, so they coincide. On the other hand, we consider the R-Hopf algebra $R[G]^*$. Recall that $R[G]^*$ is free with basis $\{e_\sigma\}_{\sigma\in G}$, where, $e_\sigma(\tau) = \delta_{\sigma,\tau}$. From this basis, e_1 is both left and right integral of $R[G]^*$. Indeed,

$$e_\sigma e_1 = \delta_{1,\sigma} e_1 = \varepsilon_{R[G]^*}(e_\sigma)e_1.$$

Again, this integral generates $\int_{R[G]^*}^{l}$ and $\int_{R[G]^*}^{r}$, from which we deduce that they coincide. Thus, $R[G]$ and $R[G]^*$ are both unimodular.

Recall that $R[G]$ acts on $R[G]^*$ by means of

$$h * f = \sum_{(f)} f_{(1)}\langle f_{(2)}, x\rangle, \quad h \in R[G], f \in R[G]^*$$

The comultiplication of $R[G]^*$ is

$$\Delta_{R[G]^*}(e_\tau) = \sum_{gh=\tau} e_g \otimes e_h, \quad \tau \in G$$

Then, given $\sigma, \tau \in G$, we have

$$\sigma * e_\tau = \sum_{gh=\tau} e_g\langle e_h, \sigma\rangle = \sum_{gh=\tau} e_g\delta_{h,\sigma} = e_{\tau\sigma^{-1}}.$$

We obtain that $R[G]^* = R[G] * e_1$ and e_1 is a generating integral of $R[G]^*$. Likewise, $R[G]^*$ acts on $R[G]$ by

$$f * h = \sum_{(h)} h_{(1)}\langle f, h_{(2)}\rangle.$$

Since $\Delta_{R[G]}(\tau) = \tau \otimes \tau$, we get

$$e_\sigma * \tau = \delta_{\sigma\tau}\tau.$$

We deduce then that $R[G] = R[G]^* * (\sum_{\sigma\in G}\sigma)$, where the last element is a generating integral of $R[G]$.

In the previous example, we have obtained an explicit relation between $R[G]$ and $R[G]^*$ in terms of their generating integrals. We can establish similar descriptions of R-Hopf algebras and their duals because of Larson-Sweedler's theorem (see [Chi00, (3.3)]).

Theorem 3.4.15 (Larson-Sweedler). *If H is a finite R-Hopf algebra, then*

$$H^* \cong H \otimes_R \int_{H^*}^{l}$$

as R-modules.

This theorem is very useful to obtain information about the module of left integrals of a finite Hopf algebra. Recall that H is finite if and only if so is H^* and $H^{**} \cong H$. Then, the theorem applied to H^* gives $H \cong H^* \otimes_R \int_{H}^{l}$.

We apply Larson-Sweedler's theorem to prove that the module of left integrals of a finite Hopf algebra is projective with rank one.

Proposition 3.4.16 ([Chi00], (3.4)). *Suppose that R is connected and let H be a finite R-Hopf algebra. Then, $\int_H^l$ is a projective R-module of rank one.*

Proof. Since H is finite, $H^{**} \cong H$. Then, by Larson-Sweedler's Theorem,

$$H \cong H^* \otimes_R \int_H^l . \tag{3.3}$$

Since R is connected, we can consider the rank n of H, which is a finite number. Moreover, using Proposition 3.4.11 3, $n = \mathrm{rank}_R(H^*)$.

Next, for $r \in R$ we have

$$\varepsilon_{H^*} \circ \lambda_{H^*}(r) = \varepsilon_{H^*}(r1_{H^*}) = r\varepsilon_{H^*}(1_{H^*}) = r1_R = r$$

for all $r \in R$. This says that $\varepsilon_{H^*} \circ \lambda_{H^*} = \mathrm{Id}_R$, so the short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Ker}(\varepsilon_{H^*}) \arrow[r] & H^* \arrow[r, "\varepsilon_{H^*}"] & R \arrow[r] & 0 \end{tikzcd}$$

splits. Thus, $H^* \cong \mathrm{Ker}(\varepsilon_{H^*}) \oplus R$. If we carry this to (3.3), we obtain

$$H \cong H^* \otimes_R \int_H^l \cong (\mathrm{Ker}(\varepsilon_{H^*}) \oplus R) \otimes_R \int_H^l \cong \left(\mathrm{Ker}(\varepsilon_{H^*}) \otimes_R \int_H^l\right) \oplus \int_H^l .$$

This proves that $\int_H^l$ is a direct summand of H, which is a projective module, thus a direct summand of a free module. Hence $\int_H^l$ is a direct summand of a free module, so it is projective.

Finally, Proposition 3.4.11 1 applied to (3.3) gives us that $\int_H^l$ has rank one. □

Since projective modules over local rings are free, we deduce the following.

Corollary 3.4.17. *Let R be a local ring and let H be a finite R-Hopf algebra. Then, $\int_H^l$ is a free R-module of rank one.*

4.3 Hopf orders

In this section we introduce Hopf orders, which can be regarded as orders in Hopf algebras inheriting the Hopf algebra structure. The main guides will be [Tru09, Section 2.3.1] and [Chi00, Chapter 1, Section 5].

We consider orders in a K-Hopf algebra A, where K is the quotient field of some Dedekind domain $\mathcal{O}_K$, and we want to impose conditions to $\mathcal{O}_K$-orders H in A to inherit the K-Hopf algebra structure of A.

A natural difficulty arises from this purpose: the K-Hopf algebra structure must give rise to a $\mathcal{O}_K$-Hopf algebra structure. Concretely, if H is an $\mathcal{O}_K$-order in A, we want to restrict the structural maps of A to similar maps with $\mathcal{O}_K$, in such a way that asking whether H is an $\mathcal{O}_K$-Hopf algebra with these restriction maps makes sense. In the case of $u_A \colon K \longrightarrow A$, $\varepsilon_A \colon A \longrightarrow K$ and $S_A \colon A \longrightarrow A$, we simply take the respective restrictions $u_H = u_A|_{\mathcal{O}_K}$, $\varepsilon_H = \varepsilon_A|_H$ and $S_H = S_A|_H$. We require $u_A(\mathcal{O}_K) \subset H$, $\varepsilon_H(H) \subset \mathcal{O}_K$, and $S_A(H) \subset H$. Note that the first inclusion is always satisfied by the definition of the unit map of an $\mathcal{O}_K$-algebra.

However, in the case of the maps $m_A\colon A\otimes_K A\longrightarrow A$ and $\Delta_A\colon A\longrightarrow A\otimes_K A$, we need to embed $H\otimes_{\mathcal{O}_K} H$ into $A\otimes_K A$. This can be done by means of the map

$$\begin{array}{rccc} \nu\colon & H\otimes_{\mathcal{O}_K} H & \longrightarrow & A\otimes_K A \\ & a\otimes_{\mathcal{O}_K} b & \longmapsto & a\otimes_K b \end{array},$$

which is clearly an homomorphism of $\mathcal{O}_K$-algebras. Let us prove that ν is injective. We reduce the problem to a local question. Given $\mathfrak{p}\in\operatorname{Spec}(\mathcal{O}_K)$, if H is finitely generated and projective as an $\mathcal{O}_K$-module, then $H_{\mathfrak{p}}$ is finitely generated and free as $\mathcal{O}_{K,\mathfrak{p}}$-module. Moreover,

$$(H\otimes_{\mathcal{O}_K} H)_{\mathfrak{p}}\cong H_{\mathfrak{p}}\otimes_{\mathcal{O}_{K,\mathfrak{p}}} H_{\mathfrak{p}},$$

$$(A\otimes_K A)_{\mathfrak{p}}\cong A_{\mathfrak{p}}\otimes_K A_{\mathfrak{p}}.$$

Then, the localization of ν at $\mathfrak{p}$ is $\nu_{\mathfrak{p}}\colon H_{\mathfrak{p}}\otimes_{\mathcal{O}_{K,\mathfrak{p}}} H_{\mathfrak{p}}\longrightarrow A_{\mathfrak{p}}\otimes_K A_{\mathfrak{p}}$, and ν is a monomorphism if and only if so is $\nu_{\mathfrak{p}}$ for all $\mathfrak{p}\in\operatorname{Spec}(\mathcal{O}_K)$. Then, we can assume that $\mathcal{O}_K$ is local and H is finitely generated and free over $\mathcal{O}_K$. Let $\{h_1,...,h_n\}$ be an $\mathcal{O}_K$-basis of H. Then, $\{h_i\otimes_{\mathcal{O}_K} h_j\,|\,i,j\in\{1,...,n\}\}$ is an $\mathcal{O}_K$-basis of $H\otimes_{\mathcal{O}_K} H$. The image of this basis by ν is $\{h_i\otimes_K h_j\,|\,i,j\in\{1,...,n\}\}$, which is a K-linearly independent set in $A\otimes_K A$ by definition of tensor product. Hence, ν is injective.

Definition 3.4.18. *Let K be the fraction field of a Dedekind domain $\mathcal{O}_K$. Let A be a finite K-Hopf algebra and let H be a finite $\mathcal{O}_K$-order in A. We say that H is an $\mathcal{O}_K$-**Hopf order** in A if the K-Hopf algebra structure of A induces an $\mathcal{O}_K$-Hopf algebra structure on H, that is, $m_A(H\otimes_{\mathcal{O}_K} H)\subset H$, $\Delta_A(H)\subset H\otimes_{\mathcal{O}_K} H$, $\varepsilon_A(H)\subset\mathcal{O}_K$ and $S_A(H)\subset H$.*

From this definition it seems tricky to check that a given R-order in A is an R-Hopf order. However, when A is the K-group algebra $K[G]$ of some finite group G, there is a criterion that reduces the Hopf order condition to check that the comultiplication map can be restricted.

Proposition 3.4.19 ([Tru09], Proposition 2.3.12)**.** *Let K be the fraction field of a Dedekind domain $\mathcal{O}_K$. Let G be a finite group and let H be an $\mathcal{O}_K$-order in $K[G]$. If $\Delta_{K[G]}(H)\subset H\otimes_{\mathcal{O}_K} H$, then H is an $\mathcal{O}_K$-Hopf order in $K[G]$.*

Proof. Since H is an $\mathcal{O}_K$-order in $K[G]$, the multiplication map $m_{K[G]}\colon K[G]\otimes_K K[G]\longrightarrow K[G]$ restricts to H: $m_{K[G]}(H\otimes_{\mathcal{O}_K} H)\subset H$. We must check that $\varepsilon_{K[G]}\colon K[G]\longrightarrow K$ and $S_{K[G]}\colon K[G]\longrightarrow K[G]$ satisfy $\varepsilon_{K[G]}(H)\subset\mathcal{O}_K$ and $S_{K[G]}(H)\subset H$. Let us define:

$$\Delta_1=\Delta_{K[G]},$$

$$\Delta_i=(\mathrm{Id}_{K[G]}^{i-1}\otimes\Delta)\circ\Delta_{i-1}\colon K[G]\longrightarrow\otimes_{j=1}^{i+1}K[G],\ i\geq 1.$$

We define also:

$$m_1=m,$$

$$m_i=m_{i-1}\circ(\mathrm{Id}_{K[G]}^{i-1}\otimes m)\colon\ \otimes_{j=1}^{i+1}K[G]\longrightarrow K[G].$$

Given $g\in G$,

$$m_i\circ\Delta_i(g)=g^{i+1}$$

for all $i \geq 1$. Then, given $z = \sum_{g \in G} k_g \, g \in K[G]$,

$$m_{n-1} \circ \Delta_{n-1}(z) = \sum_{g \in G} k_g g^n = \sum_{g \in G} k_g = \varepsilon_{K[G]}(z),$$

$$m_{n-2} \circ \Delta_{n-2}(z) = \sum_{g \in G} k_g g^{n-1} = \sum_{g \in G} k_g g^{-1} = S_{K[G]}(z),$$

where $n = |G|$. Let $h \in H$. Since $\Delta_i(H) \subset \otimes_{j=1}^{i+1} H$ by the hypothesis and $m_i(\otimes_{j=1}^{i+1} H) \subset H$ because H is a K-algebra, we have that $\varepsilon_{K[G]}(h) \in \mathcal{O}_K$ and $S_{K[G]}(h) \in H$, which finishes the proof. □

Suppose L is an A-Galois extension of K. In general, the associated order $\mathfrak{A}_A$ of $\mathcal{O}_L$ is not an $\mathcal{O}_K$-Hopf order in A. In fact, we shall eventually see that this is a sufficient condition for the $\mathfrak{A}_{L/K}$-freeness of $\mathcal{O}_L$.

4.4 Maximal orders

Let K be the fraction field of a Dedekind domain $\mathcal{O}_K$ and let A be a K-algebra. We can achieve some properties for orders when we impose restrictions to A. In this section, we will deal with separable K-algebras and the information obtained for orders concerns the maximality for the inclusion. We follow the exposition at [Tru09, Section 2.1].

Definition 3.4.20 ([Tru09], Definition 2.1.2)**.** *Let K be a field and let A be a K-algebra. We say that A is:*

1. ***Semisimple**, if it is a finite direct sum of minimal left ideals of A.*
2. ***Separable**, if for all L extension field of K, $L \otimes_K A$ is a semisimple L-algebra.*

The next result give conditions so as to identify the maximal order in a K-algebra.

Proposition 3.4.21 ([CR87], (26.10))**.** *Let K be the fraction field of a Dedekind domain $\mathcal{O}_K$. Let A be a commutative separable K-algebra. Then, the integral closure $\mathcal{O}$ of $\mathcal{O}_K$ in A is the unique maximal $\mathcal{O}_K$-order in A.*

This is useful in our case because of the following.

Proposition 3.4.22 ([Tru09], Proposition 2.3.9)**.** *Let K be a field with* $\mathrm{char}(K) = 0$ *and let A be a finite commutative K-Hopf algebra. Then A is a separable K-algebra.*

In the case of a K-group algebra, it is actually possible to give a characterization for the maximality of $\mathcal{O}_K$-orders.

Proposition 3.4.23 ([CR87], (27.1))**.** *Let G be a finite group of order n. Let K be the fraction field of a Dedekind domain $\mathcal{O}_K$ and suppose that* $\mathrm{char}(K) \nmid n$*. Let $\mathcal{O}$ be an $\mathcal{O}_K$-order in $K[G]$ such that $\mathcal{O}_K[G] \subset \mathcal{O}$. Then, $\mathcal{O} \subset n^{-1}\mathcal{O}_K[G]$. In particular, $\mathcal{O}_K[G]$ is maximal if and only if $n \in \mathcal{O}_K^*$.*

Suppose that L is an A-Galois extension of K with A commutative. By Proposition 3.4.22, A is separable. Hence, using Proposition 3.4.21, there is a unique maximal $\mathcal{O}_K$-order in A. Note that a necessary and sufficient condition for A being commutative is that the corresponding permutation subgroup under the Greither-Pareigis correspondence is abelian. If in addition we assume that K is a p-adic field, we have the following sufficient condition for freeness.

Proposition 3.4.24 ([Tru09], Proposition 2.5.5)**.** *Let K be a p-adic field and let A be a commutative and separable K-algebra. Let $\mathfrak{M}$ be the unique maximal $\mathcal{O}_K$-order in A. Let S be a $\mathfrak{M}$-module which is finite as an $\mathcal{O}_K$-module and such that $S \otimes_{\mathcal{O}_K} K$ is A-free. Then S is $\mathfrak{M}$-free.*

From this result we can obtain a sufficient condition for freeness over the associated order.

Corollary 3.4.25. *Let L/K be an A-Galois extension of p-adic fields with A commutative. If $\mathfrak{A}_A$ is the maximal $\mathcal{O}_K$-order in A, then $\mathcal{O}_L$ is $\mathfrak{A}_A$-free.*

Proof. We show that this is a particular case of Proposition 3.4.24. Indeed, since A is commutative, it is separable by Proposition 3.4.22, and $\mathcal{O}_L$ is an $\mathfrak{A}_A$-module which is finite as an $\mathcal{O}_K$-module. Moreover, $\mathcal{O}_L \otimes_{\mathcal{O}_K} K = L$, which is A-free by Theorem 3.1.3. We obtain that $\mathcal{O}_L$ is $\mathfrak{A}_A$-free. □

4.5 H-tame extensions

We know that a Galois extension of p-adic fields L/K is tamely ramified if p does not divide the ramification index $e(L/K)$. In this section we generalize this notion to the Hopf-Galois setting.

First, we rewrite the tameness condition in such a way that it is natural to replace the classical Galois structure by an arbitrary Hopf-Galois structure (see [Mar69, Theoreme II.1]).

Proposition 3.4.26. *Let L/K be a Galois extension of p-adic fields. Then L/K is tamely ramified if and only if $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$.*

Let $G = \mathrm{Gal}(L/K)$. Given $\alpha \in L$, $\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha)$. Now, we can regard this definition as the element $\theta := \sum_{\sigma \in G} \sigma \in K[G]$ acting on the element α. Under this perspective, the condition that $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$ means that $\theta\mathcal{O}_L = \mathcal{O}_K$. Recall from Example 3.4.14 that θ generates the module of left integrals $\int_{\mathcal{O}_K[G]}^l$, so the characterization for tameness becomes $\int_{\mathcal{O}_K[G]}^l \cdot \mathcal{O}_L = \mathcal{O}_K$. This motivates the following definition:

Definition 3.4.27. *Let H be a cocommutative R-Hopf algebra and let S be a commutative R-algebra, both finite as R-modules. Suppose that S is a left H-module algebra and that $S^H = u_S(R)$. We say that S is H-**tame** if:*

1. $\mathrm{rank}_R(S) = \mathrm{rank}_R(H)$.

2. *S is faithful as an H-module.*

3. $\int_H^l \cdot S = u_S(R)$.

By construction, if L/K is a Galois tamely ramified extension of p-adic fields, then $\mathcal{O}_L$ is $\mathcal{O}_K[G]$-tame.

Recall that when S is H-Galois, we have that $S^H = u_S(R)$.

Proposition 3.4.28. *Let H be a finite cocommutative R-Hopf algebra and let S be an H-module algebra. Then, $\int_H^l \cdot S \subset S^H$.*

Proof. Let $\xi \in \int_H^l \cdot S$. Then, there are $\theta_i \in \int_H^l$, $s_i \in S$ such that $\xi = \sum \theta_i s_i$. Given $h \in H$,

$$h \cdot \xi = h \cdot \left(\sum \theta_i \cdot s_i\right) = \sum (h\theta_i) \cdot s_i = \sum \varepsilon(h)\theta_i \cdot s_i = \varepsilon(h)\,\xi.$$

This proves that $\xi \in S^H$. □

Proposition 3.4.28 yields the interpretation that H-tame extensions S are those for which $\int_H^l \cdot S$ are as large as possible.

4.6 Linking notions

We already know from Theorem 3.4.2 that if S is H-Galois then (under the suitable restrictions to R) S is H-free. In this section, we shall see further logical relations between the notions we have studied in this section.

4.6.1 H-tame implies H-free

The implication to the left side is proved in two parts, by proving as an intermediate step that S is H-projective. We need the following lemma about integrals.

Lemma 3.4.29. *Let H be an R-Hopf algebra and let $\theta \in \int_H^l$. Given $x \in H$,*

$$(x \otimes 1)((\mathrm{Id_H} \otimes S_H) \circ \Delta_H(\theta)) = ((\mathrm{Id_H} \otimes S_H) \circ \Delta_H(\theta))(1 \otimes x).$$

Proof. The result follows from the next chain of equalities:

$$\begin{aligned}
(x \otimes 1)((\mathrm{Id_H} \otimes S_H) \circ \Delta_H(\theta)) &= \sum_{(\theta)} x\theta_{(1)} \otimes S_H(\theta_{(2)}) \\
&= \sum_{(\theta,x)} x_{(1)}\varepsilon_H(x_{(2)})\theta_{(1)} \otimes S_H(\theta_{(2)}) \\
&= \sum_{(\theta,x)} x_{(1)}\theta_{(1)} \otimes S_H(\theta_{(2)})\varepsilon_H(x_{(2)}) \\
&= \sum_{(\theta,x)} x_{(1)}\theta_{(1)} \otimes S_H(\theta_{(2)})S_H(x_{(2)})x_{(3)} \\
&= \sum_{(\theta,x)} x_{(1)}\theta_{(1)} \otimes S_H(x_{(2)}\theta_{(2)})x_{(3)} \\
&= \sum_{(x)} (\mathrm{Id}_H \otimes S_H) \circ \Delta_H(x_{(1)}\theta)(1 \otimes x_{(2)}) \\
&= \sum_{(x)} (\mathrm{Id}_H \otimes S_H) \circ \Delta_H(\varepsilon_H(x_{(1)})\theta)(1 \otimes x_{(2)}) \\
&= \sum_{(x)} (\mathrm{Id}_H \otimes S_H) \circ \Delta_H(\theta)(1 \otimes \varepsilon_H(x_{(1)})x_{(2)}) \\
&= ((\mathrm{Id}_H \otimes S_H) \circ \Delta_H(\theta))(1 \otimes x).
\end{aligned}$$

$\square$

Theorem 3.4.30. *Suppose that R is a local ring. Let H be a cocommutative R-Hopf algebra and S an R-algebra, both finite as R-modules, and such that S is an H-module algebra. If S is H-tame, then S is H-projective.*

Proof. Since H is finite and R is local, $\int_H^l$ is R-free of rank one. Let θ be a generator of $\int_H^l$. Since S is H-tame, we have $\int_H^l S = R$, so $\theta \cdot S = R$. Then, there is $z \in S$ such that $\theta \cdot z = 1$. Now, we have that S is R-projective. This implies that $H \otimes_R S$ is H-projective. Indeed, S is direct summand of a free R-module, say $L = M \oplus S$. Then,

$$H \otimes_R L \cong (H \otimes_R M) \oplus (H \otimes_R S),$$

where $H \otimes_R L$ is a free H-module. That is, $H \otimes_R S$ is a direct summand of a free H-module, hence H-projective. Let $\mu\colon H \otimes_R S \longrightarrow S$, $\mu(h \otimes s) = h \cdot s$. Then, μ is clearly surjective and

$$\mu(h'(h \otimes s)) = \mu((h'h) \otimes s) = (h'h) \cdot s = h' \cdot (h \cdot s),$$

so μ is an epimorphism of H-modules. Then, there is a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Ker}(\mu) \arrow[r, "i"] & H \otimes_R S \arrow[r, "\mu"] & S \arrow[r] & 0 . \end{tikzcd}$$

It is enough to show that this sequence splits. Indeed, in that case, S is a direct summand of $H \otimes_R S$, and hence it is a direct summand of a free H-module, that is, S is H-projective.

Let $\nu\colon S \longrightarrow H \otimes_R S$, $\nu(s) = \sum_{(\theta)} \theta_{(1)} \otimes (z(S_H(\theta_{(2)}) \cdot s))$. First, we prove that ν is an homomorphism of H-modules. Let $h \in H$, $s \in S$. Then,

$$\begin{aligned} h \cdot (\nu(s)) &= h \cdot \left(\sum_{(\theta)} \theta_{(1)} \otimes z(S_H(\theta_2) \cdot s) \right) \\ &= \sum_{(\theta)} (h \cdot \theta_{(1)}) \otimes z(S_H(\theta_{(2)}) \cdot s) \\ &= (1 \otimes z) \left(\sum_{(\theta)} (h \cdot \theta_{(1)}) \otimes S_H(\theta_{(2)}) \right) (1 \otimes s) \end{aligned}$$

Now, we note that $\sum_{(\theta)} (h \cdot \theta_{(1)}) \otimes S_H(\theta_{(2)}) = (h \otimes 1)((1 \otimes S_H)\Delta(\theta))$. By the previous lemma, this coincides with $((1 \otimes S_H)\Delta(\theta))(1 \otimes h) = \sum_{(\theta)} \theta_{(1)} \otimes S_H(\theta_{(2)})h$. Then,

$$\begin{aligned} h \cdot (\nu(s)) &= (1 \otimes z) \left(\sum_{(\theta)} \theta_{(1)} \otimes S_H(\theta_{(2)})h \right) (1 \otimes s) \\ &= \sum_{(\theta)} \theta_{(1)} \otimes z(S_H(\theta_{(2)})(h \cdot s)) \\ &= \nu(h \cdot s), \end{aligned}$$

which proves that ν is an homomorphism of H-modules.

It remains to check that $\mu \circ \nu = \mathrm{Id}_S$. Let $s \in S$. Then,

$$\begin{aligned}
\mu \circ \nu(s) &= \sum_{(\theta)} \theta_{(1)}(z(S_H(\theta_{(2)}) \cdot s)) \\
&= \sum_{\theta} (\theta_{(1)} \cdot z)(\theta_{(2)} \cdot (S_H(\theta_{(3)}) \cdot s)) \\
&= \sum_{\theta} (\theta_{(1)} \cdot z)(\varepsilon(\theta_{(2)})\, s) \\
&= \sum_{(\theta)} ((\theta_{(1)}\varepsilon(\theta_{(2)})) \cdot z)\, s \\
&= (\theta \cdot z)\, s = s,
\end{aligned}$$

as we wanted to prove. □

Next, we prove that H-projective implies H-free of rank one. For proving this we need the following result (see [Sch77]).

Theorem 3.4.31 (Schneider)**.** *Let R be a local domain such that $K = \mathrm{Frac}(R)$ has charasteristic zero. Let H be a finite cocommutative R-Hopf algebra and let P, Q be finite left H-modules. If $K \otimes_R P \cong K \otimes_R Q$ as $K \otimes H$-modules, then $P \cong Q$ as H-modules.*

Proposition 3.4.32. *Let K be a p-adic field and let L be an A-Galois extension of K (in the sense of Definition 3.4.1). Let S be an $\mathcal{O}_K$-order in L. If H is an $\mathcal{O}_K$-Hopf order in A acting on S and S is H-projective, then S is H-free.*

Proof. We check that the situation given in the statement is actually a particular case of the one in Schneider's theorem.

The valuation ring $\mathcal{O}_K$ is a Dedekind domain and is local, in particular it is a local domain. Since K is p-adic, it has characteristic zero.

We have that A is cocommutative and finite dimensional because L is A-Galois. Since H is an $\mathcal{O}_K$-Hopf order and inherits the Hopf algebra structure of A, so H is cocommutative as an $\mathcal{O}_K$-Hopf algebra and finite as an $\mathcal{O}_K$-module. In addition, H is a finite module over itself.

On the other hand, since S is an $\mathcal{O}_K$-order in L, it is finitely generated as an $\mathcal{O}_K$-module. Now, we know by Theorem 3.4.30 that there is an epimorphism $\mu \colon H \otimes_R S \longrightarrow S$ of H-modules, so S is finitely generated as H-module. We also know by the hypothesis that S is H-projective, so S is finite as an H-module.

By Theorem 3.4.2, L is A-free of rank one, that is, $L \cong A$ as A-modules. Then,

$$K \otimes_R H \cong A \cong L \cong K \otimes_R S$$

as $K \otimes_R H$-modules. By Schneider's theorem, $S \cong H$ as H-modules, that is, S is H-free of rank one. □

Then, joining Theorem 3.4.30 and Proposition 3.4.32, we obtain the following:

Corollary 3.4.33. *Let K be a p-adic field and let L be an A-Galois extension of K. Let S be an $\mathcal{O}_K$-order in L. If H is an $\mathcal{O}_K$-Hopf order in A acting on S and S is H-tame, then S is H-free.*

In particular, when we take L to be a field extension of K and S to be its valuation ring $\mathcal{O}_L$, we obtain the desired implication.

Corollary 3.4.34. *Let L/K be an A-Galois extension of p-adic fields. Suppose that there is an $\mathcal{O}_K$-Hopf order H in A such that $\mathcal{O}_L$ is H-tame. Then, $\mathcal{O}_L$ is H-free (and hence, $H = \mathfrak{A}_A$).*

4.6.2 Hopf order implies freeness

Consider an A-Galois extension L/K of p-adic fields. Since the associated order in A is the only $\mathcal{O}_K$-order in A over which $\mathcal{O}_L$ can be free, is the object we work with in this section.

Theorem 3.4.35 ([Chi00], (13.3))**.** *Let L/K be an A-Galois extension of p-adic fields. If $\mathfrak{A}_A$ is an $\mathcal{O}_K$-Hopf order in A, then $\mathcal{O}_L$ is $\mathfrak{A}_A$-tame.*

Proof. Since $\mathcal{O}_K$ is local, $\int_{\mathfrak{A}_A}^{l}$ is $\mathcal{O}_K$-free of rank one. Let θ be an $\mathcal{O}_K$-generator of I. Since L/K is A-Galois, $L^A = K$. Then we can prove easily that $\mathcal{O}_L^{\mathfrak{A}_A} = u_{\mathcal{O}_L}(\mathcal{O}_K) = \mathcal{O}_K$. By Proposition 3.4.28, $\theta \cdot \mathcal{O}_L \subseteq \mathcal{O}_L^{\mathfrak{A}_A}$, whence $\theta \cdot \mathcal{O}_L$ is an ideal of $\mathcal{O}_K$. If π_K is an uniformizer of K, this means that $\theta \cdot \mathcal{O}_L = \pi_K^i \mathcal{O}_K$ for some $i \geq 0$, so $\frac{\theta}{\pi_K^i} \cdot \mathcal{O}_L = \mathcal{O}_L$. In particular, $\frac{\theta}{\pi_K^i} \in \mathfrak{A}_A$.

Let us check that $\frac{\theta}{\pi_K^i}$ is actually a left integral of $\mathfrak{A}_A$. Indeed, given $\alpha \in \mathfrak{A}_A$, since θ is a left integral, $\frac{\theta}{\pi_K^i}\alpha = \frac{\varepsilon_{\mathfrak{A}_A}(\theta)}{\pi_K^i}\alpha$. Now,

$$\varepsilon_{\mathfrak{A}_A}(\theta) = \varepsilon_{\mathfrak{A}_A}\left(\frac{\theta}{\pi_K^i}\pi_K^i\right) = \varepsilon_{\mathfrak{A}_A}\left(\frac{\theta}{\pi_K^i}\right)\varepsilon_{\mathfrak{A}_A}(\pi_K^i) = \varepsilon_{\mathfrak{A}_A}\left(\frac{\theta}{\pi_K^i}\right)\pi_K^i,$$

and joining this with the last expression gives $\frac{\theta}{\pi_K^i}\alpha = \varepsilon_{\mathfrak{A}_A}\left(\frac{\theta}{\pi_K^i}\right)\alpha$, as desired.

Then, we have proved that $\frac{\theta}{\pi_K^i} \in \int_{\mathfrak{A}_A}^{l}$, while θ is a generator of $\int_{\mathfrak{A}_A}^{l}$ as R-module. Then, $i = 0$ and $\theta\mathcal{O}_L = \mathcal{O}_K$, so $\mathcal{O}_L$ is $\mathfrak{A}_A$-tame. □

From Corollary 3.4.34, we get the following.

Corollary 3.4.36. *Let L/K be an A-Galois extension of p-adic fields. If the associated order $\mathfrak{A}_A$ is an $\mathcal{O}_K$-Hopf order, then $\mathcal{O}_L$ is $\mathfrak{A}_A$-free.*

4.6.3 H-Galois implies H-tame

We will use a result which is interesting by itself: H-Galois implies H-tame. To prove this we need the following technical result.

Proposition 3.4.37 ([Chi00], (14.3))**.** *Let H be a finite cocommutative R-Hopf algebra and let S be a finite R-algebra which is H-Galois. Let $E = \mathrm{End}_R(S)$. For any E-module M, consider the action of H on M induced by the isomorphism $M \cong S \otimes H$, and let M^H be the fixed submodule in the Hopf algebra sense. Then there is an isomorphism of R-modules*

$$M^H \cong \int_H^l \cdot M.$$

Now, the result that H-Galois implies H-tame is an easy corollary.

Corollary 3.4.38. *Let H be a finite cocommutative R-Hopf algebra and let S be an H-Galois extension of R. Then, S is H-tame.*

Proof. We must check the conditions of tameness. First, since S is an H-Galois extension of R, the isomorphism $H \otimes_R S \cong \mathrm{End}_R(S)$ yields that $\mathrm{rank}_R(H) = \mathrm{rank}_R(S)$. Moreover, since S is H-Galois, it is H-faithful. Finally, by applying the previous result to the E-module S, we obtain that $S^H \cong \int_H^l \cdot S$. Since S is H-Galois, $S^H = R$, so $\int_H^l \cdot S = R$. □

4.6.4 H-free implies H-tame

This follows easily from Corollary 3.4.38.

Corollary 3.4.39. *Suppose that R is local. Let H be a finite cocommutative R-Hopf algebra and let S be an H-module algebra with $S^H = R$. If S is H-free of rank one, then S is H-tame.*

Proof. Since H is finite, we have $H \cong H^*$ as H-modules. By the hypothesis, $S \cong H$ as H-modules, so we have that $S \cong H^*$ as H-modules. Now, we have that H^* is H-Galois, so by Corollary 3.4.38, H^* is H-tame. Hence $\int_H^l \cdot H^* = R$. The previous isomorphism maps this equality to $\int_H^l \cdot S = R$, proving that S is H-tame. □

From Corollaries 3.4.33 and 3.4.39, we obtain the following Hopf-Galois version of Noether's theorem.

Theorem 3.4.40. *Let L/K be an A-Galois extension of p-adic fields. Let S be an $\mathcal{O}_K$-order in A. For an $\mathcal{O}_K$-Hopf order H in A acting on S, S is H-tame if and only if S is H-free.*

4.6.5 Equivalence between notions

If the Hopf algebra we are working with is a local ring, then the three notions of H-Galois, H-tame and H-free are equivalent. Namely:

Theorem 3.4.41 ([Chi00], (14.7))**.** *Suppose that R is local. Let H be a local cocommutative R-Hopf algebra, and let S be a finite R-algebra which is also a faithful H-module algebra. The following are equivalent:*

1. *S is H-tame.*
2. *S is H-free.*
3. *S is H-Galois.*

5 The ring of integers in extensions of p-adic fields

In this part we focus in Problem 3.3.12 for extensions of p-adic fields. Namely, for an H-Galois extension L/K of p-adic fields, we are interested in criteria so as to characterize the freeness of $\mathcal{O}_L$ as an $\mathfrak{A}_H$-module. The available results in literature will show that the behavior of such a module depends heavily on the ramification of the extension.

5.1 Further notions of ramification theory

We present here the notions from ramification theory on extensions of p-adic fields that will be needed in what follows. Namely, we consider higher ramification group and ramification breaks, whose study is commonly known as higher ramification theory. The main reference is [Ser79, Chapter IV].

5.1.1 Higher ramification groups

Let L/K be a Galois extension of p-adic fields with group G.

Definition 3.5.1. *For an integer $i \geq -1$, the i-th ramification group of L/K is defined as $G_{-1} := G$ if $i = -1$ and, for $i \geq 0$,*

$$G_i := \{g \in G \mid v_L(g(x) - x) \geq i + 1 \text{ for all } x \in \mathcal{O}_L\}.$$

The condition that $v_L(g(x) - x) \geq i + 1$ for all $x \in \mathcal{O}_L$ can be rewritten in several equivalent ways:

1. $v_L(g(a) - a) \geq i + 1$, where $\mathcal{O}_L = \mathcal{O}_K[a]$.
2. g acts trivially on $\mathcal{O}_L/\mathfrak{p}_L^{i+1}$.

Note that if L/K is tamely ramified, π_L is an $\mathcal{O}_K$-algebra generator of $\mathcal{O}_K$.

It is clear that $G_i \supseteq G_{i+1}$ for every $i \geq -1$ and that G_i is trivial for i large enough (namely, $i \geq \max_{g \in G}(g(x) - x)$; see [Ser79, Chapter IV, Proposition 1]). Therefore, $\{G_i\}_{i=-1}^{\infty}$ is a filtration of G, called the **chain of ramification groups** of L/K.

5.1.2 Relationship with the ramification

The group

$$G_0 = \{g \in G \mid v_L(g(x) - x) \geq 1 \text{ for all } x \in L\}$$

is called the **inertia group** of L/K. Accordingly, the fixed subfield L^{G_0} is called the **inertia field** of L/K. Given $g \in G$, $g \in G_0$ if and only if g acts trivially on the residue field κ_L. Hence, the natural group epimorphism $G \longrightarrow \mathrm{Gal}(\kappa_L/\kappa_K)$ has kernel G_0. Consequently, $|G_0| = e(L/K)$.

Corollary 3.5.2. *The extension L/K is:*

1. *Unramified, if and only if G_0 is trivial.*
2. *Totally ramified, if and only if $G_0 = G$.*
3. *Tamely ramified, if and only if $p \nmid |G_0|$.*

We list further properties of the ramification groups.

Proposition 3.5.3 ([Ser79], Chapter IV, Corollaries 3 and 4)**.** *Let L/K be a Galois extension of p-adic fields with group G.*

1. *For each $i \geq 0$, G_{i+1} is a normal subgroup of G_i, and G_i/G_{i+1} is a direct product of cyclic groups of order p.*

2. *G_1 is a p-group.*

3. *G_0 is a semidirect product of G_1 and a subgroup of G whose order is coprime to p.*

Moreover, we have the following important result on G.

Proposition 3.5.4 ([Ser79], Corollary 5)**.** *The Galois group of a Galois extension of p-adic fields is solvable.*

From the result that G_1 is a p-group it follows immediately that $G_1 = \{1\}$ if and only if L/K is tamely ramified.

Definition 3.5.5. *We say that L/K is weakly ramified if $G_2 = \{1\}$.*

When we are working with Galois subextensions of L/K, we have the following useful result:

Proposition 3.5.6 ([Ser79], Chapter IV, Proposition 2)**.** *Let H be a subgroup of G. Then $H_i = G_i \cap H$ for all $i \geq -1$.*

5.1.3 Ramification breaks

Let E/K be a Galois extension of p-adic fields with group G and consider its chain of ramification groups $\{G_i\}_{i=0}^{\infty}$.

Definition 3.5.7. *A ramification break (or jump, or number) of E/K is a positive integer t such that $G_{t+1} \subsetneq G_t$.*

If L/K is totally ramified, then $G_0 = G$, and on the other hand G_1 is a p-group. Thus, if in addition G is not a p-group, we have that $G_1 \subsetneq G_0$. Since this jump is of a different nature of the other ones, we do not accept it as a ramification break. Moreover, since the chain of ramification groups stabilize, the ramification breaks exist and are finitely many.

Suppose that $v_p([E : K]) = 1$. Then, E/K admits a single ramification break t. We shall denote it by $t(E/K)$ if ramification breaks of other extensions arise in the context. If H is a subgroup of G and $L = E^H$, from Proposition 3.5.6 we have that $t(E/K) = t(E/L)$.

Proposition 3.5.8. *Let E/K be a Galois extension of p-adic fields with $[E : K] = rp$, $p \nmid r$. Then:*

1. *$1 \leq t \leq \frac{rpe}{p-1}$.*

2. *$p \mid t$ if and only if $t = \frac{rpe}{p-1}$.*

Our next goal is to define the notion of ramification break for a non-necessarily Galois extension. We do it by means of the Herbrand function (see [Ser79, Chapter IV, §3]).

Definition 3.5.9. *The **Herbrand function** of a Galois extension E/K is the function $\varphi_{E/K} \colon \mathbb{R}_{\geq -1} \longrightarrow \mathbb{R}_{\geq -1}$ defined as*

$$\varphi_{E/K}(u) = \int_0^u \frac{1}{[G_0 : G_t]} dt,$$

where $G_u = G_{\lfloor u \rfloor}$ for all $u \in \mathbb{R}$.

Theorem 3.5.10 (Hasse-Arf). *If G is an abelian group and t is a ramification break, then $\varphi_{E/K}(t)$ is an integer.*

It holds that $\varphi_{E/K}$ is continuous and strictly increasing (see [Ser79, Chapter IV, §3, Proposition 12 a)]), therefore bijective; call $\psi_{E/K}$ its inverse. If L is an intermediate field of E/K, by [Ser79, Chapter IV, §3, Proposition 15], we have transitivity formulas

$$\varphi_{E/K} = \varphi_{L/K} \circ \varphi_{E/L}, \quad \psi_{E/K} = \psi_{E/L} \circ \psi_{L/K}. \tag{3.4}$$

Now, let L/K be any extension of p-adic fields. The definition of Herbrand function is translated naturally to this setting.

Definition 3.5.11. *The Herbrand function for L/K is the function*

$$\varphi_{L/K} \coloneqq \varphi_{E/K} \circ \psi_{E/L},$$

where E is a field Galois extension of K such that $L \subset E$.

Note that if E is any Galois field extension of K with $L \subset E$, we have

$$\varphi_{E/K} \circ \psi_{E/L} = \varphi_{L/K} \circ \varphi_{E/L} \circ \psi_{E/L} = \varphi_{L/K},$$

which is independent of E. Then Definition 3.5.11 is correct.

Definition 3.5.12. *Let $\widetilde{L}$ be the normal closure of L/K. A ramification break for L/K is defined as the image of a ramification break of $\widetilde{L}$ by $\varphi_{L/K}$.*

A ramification break for a non-Galois extension is not necessarily an integer number, but in any case it is a p-adic integer.

5.2 The case of tamely ramified extensions

Recall that tamely ramified extensions of p-adic fields are those whose ramification index is not divisible by p. We shall prove that for abelian Hopf-Galois structures (those whose corresponding permutation subgroup is abelian), there is freeness over the associated order.

We start with the most simple case of tameness: the one of unramified extensions, defined by the condition that the ramification index is 1.

Let L/K be an unramified extension of p-adic fields. Recall from Proposition 3.2.28 that L/K is Galois. In this section, we see that $\mathcal{O}_L$ is $\mathfrak{A}_H$-free for any Hopf-Galois structure H on L/K.

Proposition 3.5.13 ([Chi+21], Proposition 11.24). *Let L/K be an unramified extension of p-adic fields with Galois group G and let $H = L[N]^G$ be a Hopf-Galois structure on L/K. Then $\mathfrak{A}_H = \mathcal{O}_L[N]^G$ and $\mathcal{O}_L$ is $\mathfrak{A}_H$-free.*

Proof. From [Tru13, Theorem 2.1], we have that $\mathcal{O}_L[N]^G$ is an $\mathcal{O}_K$-Hopf order if and only if $G_0 \subseteq \mathrm{Stab}_G(N)$. Since L/K is unramified, we have that G_0 is trivial, so the criterion is fulfilled. Then, we get that $\mathcal{O}_L[N]^G$ is indeed an $\mathcal{O}_K$-Hopf order of H. Now, $\theta \coloneqq \sum_{\eta\in N} \eta$ is a left integral of $\mathcal{O}_L[N]^G$, and given $x \in \mathcal{O}_L$, $\theta \cdot x = \mathrm{Tr}_{L/K}(x)$. Using once again that L/K is unramified, in particular it is tamely ramified, and then $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$ by Proposition 3.4.26. Hence there is some $z \in \mathcal{O}_L$ such that $\theta \cdot z = 1$. It follows that $\mathcal{O}_L$ is $\mathcal{O}_L[N]^G$-tame. By Corollary 3.4.33, we obtain that $\mathcal{O}_L$ is $\mathcal{O}_L[N]^G$-free, so $\mathfrak{A}_H = \mathcal{O}_L[N]^G$. □

Next, we see the result for a subclass of tamely ramified extensions of p-adic fields.

Proposition 3.5.14 ([Chi+21], Proposition 11.25)**.** *Let L/K be an extension of p-adic fields such that $p \nmid [L:K]$ and let $H = \widetilde{L}[N]^G$ be an abelian Hopf-Galois structure on L/K. Then $\mathfrak{A}_H = \mathcal{O}_{\widetilde{L}}[N]^G$ and $\mathcal{O}_L$ is $\mathfrak{A}_H$-free.*

Proof. We know that H is separable by Proposition 3.4.22 and commutative because N is abelian. By Proposition 3.4.21, H contains a unique maximal $\mathcal{O}_K$-order, which is the integral closure of $\mathcal{O}_K$ in H. Given $z \in \mathfrak{M}$, z is integral over $\mathcal{O}_K$ in H. Since $\widetilde{L}[N] = \widetilde{L} \otimes_K H$, z is also integral over $\mathcal{O}_{\widetilde{L}}$ in $\widetilde{L}[N]$. Then, z belongs to the maximal $\mathcal{O}_{\widetilde{L}}$-order in $\widetilde{L}[N]$. Now, since $|N| = [L:K]$, the hypothesis gives that $p \nmid |N|$. By Proposition 3.4.23, the maximal $\mathcal{O}_{\widetilde{L}}$-order of $\widetilde{L}[N]$ is $\mathcal{O}_{\widetilde{L}}[N]$, which therefore contains z. Thus, $z \in \mathcal{O}_{\widetilde{L}}[N] \cap H = \mathcal{O}_{\widetilde{L}}[N]^G$. This proves that $\mathfrak{M} \subseteq \mathcal{O}_{\widetilde{L}}[N]^G$. Since in addition $\mathcal{O}_{\widetilde{L}}[N]^G \subseteq \mathfrak{A}_H$ from Exercise 4, the maximality of $\mathfrak{M}$ yields that $\mathfrak{M} = \mathcal{O}_{\widetilde{L}}[N]^G = \mathfrak{A}_H$. By Corollary 3.4.25, $\mathcal{O}_L$ is $\mathfrak{A}_H$-free. □

Recall from Exercise 8 at Section 6.2 that the induced Hopf-Galois structure from two classical Galois structures is a classical Galois structure. For Galois tamely ramified extensions of p-adic fields, we have the following more general result.

Proposition 3.5.15. *Let E/K be a Galois tamely ramified extension of p-adic fields with group G. Let $H = E[N]^G$ be an abelian Hopf-Galois structure. Write $|N| = p^r m$ with* $\gcd(p, m) = 1$ *and $N = N_1 \times N_2$ with $|N_1| = p^r$ and $|N_2| = m$. Let L/K (resp. M/K) be the degree p^r (resp. m) subextension of E/K. Then N_1 (resp. N_2) gives L/K (resp. M/K) a Hopf-Galois structure such that H is induced from H_1 and H_2.*

The proof is beyond the scope of what we have seen so far, and can be consulted at [Chi+21, Proposition 8.22].

Now, we can prove freeness for Galois tamely ramified extensions.

Theorem 3.5.16. *Let E/K be a Galois tamely ramified extension of p-adic fields with group G and let $H = E[N]^G$ be an abelian Hopf-Galois structure on E/K. Then $\mathfrak{A}_H = \mathcal{O}_E[N]^G$ and $\mathcal{O}_E$ is $\mathfrak{A}_H$-free.*

Proof. Write $|N| = p^r m$ with $\gcd(p, m) = 1$ and $N = N_1 \times N_2$ with $|N_1| = p^r$ and $|N_2| = m$, and let L/K (resp. M/K) be the degree p^r (resp. m) subextension of E/K. By Proposition 3.5.15, H is the induced Hopf-Galois structure on E/K from the Hopf-Galois structure on L/K given by N_1 and the Hopf-Galois structure on M/K given by N_2. Since N is abelian, all the subextensions of E/K are Galois. Since in addition $L \cap M = K$ (because their degrees are coprime), we have that $E = LM$. Since E/K is tamely ramified and $[L:K] = p^r$, we see that L/K is unramified. Hence, L/K and M/K are arithmetically disjoint. Now, $\mathcal{O}_L$ is $\mathfrak{A}_{H_1}$-free by Proposition 3.5.13 and $\mathcal{O}_M$ is $\mathfrak{A}_{H_2}$-free by Proposition 3.5.14. Applying Theorem 3.3.17 2, we get that $\mathcal{O}_E$ is $\mathfrak{A}_H$-free. Finally, the same propositions at each case give $\mathfrak{A}_{H_1} = \mathcal{O}_L[N_1]^{\mathrm{Gal}(L/K)} = \mathcal{O}_E[N_1]^G$ and $\mathfrak{A}_{H_2} = \mathcal{O}_M[N_2]^{\mathrm{Gal}(M/K)} = \mathcal{O}_E[N_2]^G$, and Theorem 3.3.17 1 yields $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2} = \mathcal{O}_E[N]^G$, finishing the proof. □

Now, we consider non-necessarily Galois tamely ramified extensions of p-adic fields. Hence, now there is a non-necessarily trivial normal closure, but it turns out to be unramified over the original extension.

Lemma 3.5.17 ([Tru18], Proposition 5.2)**.** *Let L/K be a tamely ramified extension of p-adic fields with normal closure $\widetilde{L}$. Then $\widetilde{L}/L$ is unramified, so $\widetilde{L}/K$ is tamely ramified.*

Proof. Call $e := e(L/K)$. Let L_0/K be the maximal unramified subextension of L/K, so that L/L_0 is totally ramified. Then, $e = [L : L_0]$ and $\pi_L^e = v\pi_K$ for some $v \in \mathcal{O}_{L_0}^{\times}$. Let ζ_e be a primitive e-th root of unity and $u \in \overline{L}$ such that $u^e = v$, and call $L' = L(\zeta_e, u)$. Since $p \nmid e$, L'/L is an unramified extension, and hence Galois. Let $\pi_L' := u^{-1}\pi_L \in L'$. Then $(\pi_L')^e = u^{-e}\pi_L^e = \pi_K$, so the polynomial $x^e - \pi_K \in K[x]$ splits over L'. Let $f \in K[x]$ be a polynomial whose splitting field is the maximal unramified subextension of L'/K. By definition of normal closure, $\widetilde{L}$ is the smallest Galois extension of K containing L over which both $x^e - \pi_K$ and f split. In addition, L'/L is unramified. Necessarily, $\widetilde{L} \subset L'$, whence $\widetilde{L}/L$ is unramified. □

On the other hand, there is the result that for induced Hopf-Galois structures, freeness over the associated order can be projected to a subextension if the extension in the middle is tamely ramified.

Proposition 3.5.18. *Let E/K be a Galois extension of number or p-adic fields with group $G = J \rtimes G'$, where J, G' are subgroups of G and J is normal. Call $L = E^{G'}$, $M = E^J$, and let H be an induced Hopf-Galois structure on E/K from a Hopf-Galois structure H_1 on L/K and a Hopf-Galois structure H_2 on M/K. Suppose that E/L is tamely ramified.*

1. *$\mathfrak{A}_{H_1} = \pi(\mathfrak{A}_H)$, where π is projection onto the first component at the level of groups and extended by linearity.*

2. *If $\mathcal{O}_E$ is $\mathfrak{A}_H$-free, then $\mathcal{O}_L$ is $\mathfrak{A}_{H_1}$-free.*

This result was originally proved by Truman in [Tru18, Proposition 5.1]. In [Chi+21, Proposition 11.18], a slightly more general result appears, with a much shorter proof.

Combining Theorem 3.5.16, Lemma 3.5.17 and Proposition 3.5.18, we can prove the main result of this section.

Theorem 3.5.19 ([Tru18], Theorem 5.3)**.** *Let L/K be a tamely ramified almost classically Galois extension of p-adic fields. Let $H = \widetilde{L}[N]^G$ be a Hopf-Galois structure with N abelian. Then $\mathfrak{A}_H = \mathcal{O}_{\widetilde{L}}[N]^G$ and $\mathcal{O}_L$ is $\mathfrak{A}_H$-free.*

Proof. Let M/K be the complement of L/K as an almost classically Galois extension. Since L/K is tamely ramified, by Lemma 3.5.17, $\widetilde{L}/L$ is unramified. Hence, $G' := \mathrm{Gal}(\widetilde{L}/L)$ is cyclic, so the classical Galois structure on $\widetilde{L}/L$ is abelian. Now, from the Hopf-Galois structure H on L/K and the classical Galois structure on $\widetilde{L}/L$, we induce a Hopf-Galois structure H' on $\widetilde{L}/K$ whose corresponding permutation subgroup is $N \times \Lambda_{G'}$, where $\Lambda_{G'}$ is the set of left translations by elements of G'. This is an abelian group, so H' is an abelian Hopf-Galois structure. By Theorem 3.5.16, $\mathcal{O}_E$ is $\mathfrak{A}_{H'}$-free. Finally, since $\widetilde{L}/L$ is unramified, in particular it is tamely ramified, so Proposition 3.5.18 yields that $\mathcal{O}_L$ is $\mathfrak{A}_H$-free. □

It is currently unknown if Theorem 3.5.19 holds for arbitrary Hopf-Galois structures, with no restriction on the type.

5.3 The case of wildly ramified extensions

Now, we consider wildly ramified extensions of p-adic fields. The available results in literature show that their behavior is much more chaotic than in the tame case, even if we stick to Galois extensions.

5.3.1 Freeness for Galois extensions of p-adic fields

The main advances for the question of the freeness over the associated order at the classical Galois structure for Galois extensions of p-adic fields have been nicely summarized in [Tho10, Section 3]. We list here some of the results therein. We omit instead what is known on this question for extensions of local fields with positive characteristic; the interested reader can consult [Tho10, Section 4].

Much of what is known in this area lies in Galois extensions of $\mathbb{Q}_p$. For many subfamilies of such extensions, an affirmative answer to Problem 3.3.12 for the classical Galois structure on $L/\mathbb{Q}_p$ is known. One of these subfamilies is that of abelian extensions.

Theorem 3.5.20 (Leopoldt, 1959). *Let $L/\mathbb{Q}_p$ be an abelian extension of p-adic fields. Then $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}_p}$-free.*

The proof of this result is beyond the scope of these notes and can be consulted in [Leo59]. Actually, the following generalization holds (see [Let98, Theorem 1]).

Theorem 3.5.21 (Lettl, 1998). *Let L/K be an extension of p-adic fields and suppose that $L/\mathbb{Q}_p$ is abelian. Then $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.*

As for families of non-abelian extensions of p-adic fields, an example of affirmative result is as follows:

Theorem 3.5.22 (Bergé, 1972). *Let $L/\mathbb{Q}_p$ be a Galois extension of p-adic fields with Galois group $G \cong D_p$, the dihedral group of order $2p$. Then $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}_p}$-free.*

This is the main result at [Ber72].

Let us weaken the restriction on the ground field K to the condition that $K/\mathbb{Q}_p$ is unramified. In this situation, also Bergé proved the following criterion.

Theorem 3.5.23 (Bergé, 1978). *Let L/K be a totally ramified cyclic extension of p-adic fields with $K/\mathbb{Q}_p$ unramified. Write $[L:K] = rp^n$ with $p \nmid r$ and $n \in \mathbb{Z}_{\geq 1}$. Let t_1 be the first ramification break of L/K.*

1. *If $n = 1$, $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.*
2. *Otherwise, $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free if and only if*

$$\frac{rp}{p-1} - t_1 < \frac{p^n}{p^{n-1}-1}.$$

The situation is much trickier when no restriction is imposed on K. One of the most impressive results in this situation is the following on weakly ramified extensions (see [Joh15, Theorem 1.2]).

Theorem 3.5.24 (Johnston, 2015)**.** *Let L/K be a weakly ramified extension of p-adic fields with group G. Then $\mathfrak{A}_{L/K} = \mathcal{O}_K[G][\pi_K^{-1}\mathrm{Tr}_{G_0}]$ and $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.*

In the case of a cyclic degree p extension L/K of p-adic fields, the freeness is completely characterized in terms of the ramification break of L/K. This traces back to the works by F. Bertrandias, J.-P. Bertrandrias and M.-J. Ferton [BBF72; BF72]. We shall see, however, a more general result in the setting of Hopf-Galois theory.

5.3.2 Degree p extensions of p-adic fields

Let L/K be a ramified degree p extension of p-adic fields. Let $\widetilde{L}$ be the normal closure of L/K and let $G = \mathrm{Gal}(\widetilde{L}/K)$. First, note from Proposition 3.5.4 that G is solvable. By Theorem 2.3.10, L/K is Hopf-Galois. Thus, we can apply Corollary 2.5.15, obtaining that L/K admits a unique Hopf-Galois structure H, which is almost classically Galois. If L/K is Galois, H is just the classical Galois structure. The problem of characterizing the $\mathfrak{A}_H$-freeness of $\mathcal{O}_L$ in the general case was solved by the first author at [Gil24b]. We proceed to sketch the result providing a general criterion.

The first remark is that we can assume without loss of generality that $\widetilde{L}/K$ is totally ramified.

Proposition 3.5.25 ([Gil24b], Proposition 3.4)**.** *Let L/K be a ramified degree p extension of p-adic fields with normal closure $\widetilde{L}$ and Hopf-Galois structure H. Let L' (resp. K') be the inertia field of $\widetilde{L}/L$ (resp. $\widetilde{L}/K$). Let $H' := H \otimes_K K'$. Then:*

1. *L'/K' is a degree p extension of p-adic fields with normal closure $\widetilde{L}$ and Hopf-Galois structure H'.*
2. *$\mathcal{O}_L$ is $\mathfrak{A}_H$-free if and only if $\mathcal{O}_{L'}$ is $\mathfrak{A}_{H'}$-free.*

Note that, since L' is the inertia field of $\widetilde{L}/L$, the degree of $\widetilde{L}/L'$ is the order of the inertia group of $\widetilde{L}/L$, that is, the ramification index of $\widetilde{L}/L$. Necessarily, $\widetilde{L}/L'$ is totally ramified. On the other hand, L'/K' is ramified because L/K is. Thus, $\widetilde{L}/K'$ is totally ramified. Hence, Proposition 3.5.25 means that if the normal closure of our degree p extension is not totally ramified, we can take instead the extension of inertia fields, whose behavior is exactly the same.

From now on, we assume that $\widetilde{L}/K$ is totally ramified. Let $\ell := t(L/K)$ be the ramification break of L/K. Following Definition 3.5.12, it can be checked that

$$\ell = \frac{t(\widetilde{L}/K)}{r},$$

where $r = [\widetilde{L} : L]$. By Proposition 3.5.8, we have that $1 \leq t(\widetilde{L}/K) \leq \frac{rpe}{p-1}$, where $e := e(K/\mathbb{Q}_p)$, and $t(\widetilde{L}/K) = \frac{rpe}{p-1}$ if and only if it is divisible by p. As a consequence,

$$0 < \ell \leq \frac{pe}{p-1},$$

and $\ell = \frac{pe}{p-1}$ if and only if $\ell \equiv 0 \pmod{p}$ in $\mathbb{Z}_p/p\mathbb{Z}_p$.

Theorem 3.5.26 ([Gil24b], Theorem 1.2). *Let L/K be a degree p extension of p-adic fields whose normal closure $\widetilde{L}$ is totally ramified over K. Let H be the unique Hopf-Galois structure on L/K. Write e for the ramification index of $K/\mathbb{Q}_p$, and a for the residue class mod p of the ramification jump ℓ of L/K.*

1. *If $a = 0$, then $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.*
2. *If $\ell < \frac{pe}{p-1} - 1$, then $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free if and only if $a \mid p-1$.*
3. *If $\ell \geq \frac{pe}{p-1} - 1$, then $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free if and only if the length of the continued fraction expansion of $\frac{a}{p}$ is upper bounded by 4.*

If we impose that L/K is a Galois extension, then $r = 1$ and $\ell = t$. Replacing these in Theorem 3.5.26, we recover the result from [BBF72; BF72]:

Theorem 3.5.27 (F. Bertrandias, J. P. Bertrandias, M. J. Ferton, 1972). *Let L/K be a cyclic degree p extension of p-adic fields. Write e for the ramification index of $K/\mathbb{Q}$ and a for the remainder of the ramification jump t of L/K.*

1. *If $a = 0$, then $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.*
2. *If $t < \frac{pe}{p-1} - 1$, then $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free if and only if $a \mid p-1$.*
3. *If $t \geq \frac{pe}{p-1} - 1$, then $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free if and only if the length of the continued fraction expansion of $\frac{a}{p}$ is upper bounded by 4.*

6 The ring of integers in extensions of number fields

In this chapter we consider Problem 3.3.12 for extensions of number fields. Recall that this only makes sense when there is some integral basis, which is achieved by imposing that the ground ring of integers is a PID, or equivalently, the ground number field has class number 1.

6.1 Freeness for Galois extensions of number fields

We review what is known on the freeness for the ring of integers for Galois extensions of number fields.

As in the case of extensions of p-adic fields, we start with those results for extensions of $\mathbb{Q}$. There is an analogue of Theorem 3.5.20 for this case, also found by Leopoldt.

Theorem 3.6.1 (Leopoldt, 1959). *Let $L/\mathbb{Q}$ be an abelian extension of number fields. Then $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}}$-free.*

Let $G = \mathrm{Gal}(L/\mathbb{Q})$. We know that $\mathfrak{A}_{L/\mathbb{Q}} = \mathbb{Z}[G]$ if and only if $L/\mathbb{Q}$ is tamely ramified. In such case, it follows that every tamely ramified abelian extension of number fields admits a normal integral basis. Unfortunately, $\mathbb{Q}$ is the only number field with this property, due to the following result.

Theorem 3.6.2 ([Gre+99]). *Suppose that K is a number field such that every tamely ramified abelian extension of number fields admits a normal integral basis. Then $K = \mathbb{Q}$.*

There is also an affirmative answer for families of non-abelian extensions of $\mathbb{Q}$.

Theorem 3.6.3 (Bergé, 1972)**.** *Let $L/\mathbb{Q}$ be a Galois extension of number fields with group $G \cong D_p$ for a prime p. Then $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}}$-free.*

Theorem 3.6.4 (Martinet, 1972)**.** *Let $L/\mathbb{Q}$ be a Galois extension of number fields with group $G \cong Q_8$. Then $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}}$-free.*

Very recently, Ferri [Fer24] found characterizations of freeness for the families of Galois extensions with group isomorphic to A_4, S_4 and A_5.

As for families of number fields with arbitrary ground field, to the best knowledge of the author, the most complete criteria available is on families of Kummer extensions, which are those Galois extensions whose ground field contain a primitive n-th root of unity and the exponent of the Galois group divides n. In this direction, Gómez Ayala [Aya94] found a criterion for the existence of a NIB for tamely ramified Kummer extensions of number fields with prime degree. Later on, Del Corso and Rossi generalized such criterion, first for tamely ramified, cyclic and Kummer extensions of number fields [DR10], and afterwards for tamely ramified and Kummer extensions of number fields [DR13].

The reader is welcome to consult [Tho10, Section 1] for further results on normal integral bases of tamely ramified extensions of number fields.

6.2 Local freeness of the ring of integers

The complexity of the behavior of the ring of integers at a number field is considerably greater than in its p-adic analogue. For this reason, it is usual to translate the problem to the p-adic setting, by localizing by primes at the ground ring of integers. The notion of local freeness is a generalization of the $\mathcal{O}_K[G]$-local freeness of $\mathcal{O}_L$, for a Galois extension L/K of number fields (see Definition 3.3.4).

Let L/K be an H-Galois extension of number fields. For a prime $\mathfrak{p}$ of K, recall that we defined $\mathcal{O}_{L,\mathfrak{p}} := \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_{K,\mathfrak{p}}$. Likewise, let us define

$$\mathfrak{A}_{H,\mathfrak{p}} := \mathfrak{A}_H \otimes_{\mathcal{O}_K} \mathcal{O}_{K,\mathfrak{p}}.$$

This is an $\mathcal{O}_K$-order in $H_\mathfrak{p} \cong H \otimes_K K_\mathfrak{p}$, where $K_\mathfrak{p}$ is the completion of K by $\mathfrak{p}$. On the other hand, there is a natural $\mathfrak{A}_{H,\mathfrak{p}}$-module structure for $\mathcal{O}_{L,\mathfrak{p}}$. Thus, we can wonder whether this module structure is free.

Definition 3.6.5. *We say that $\mathcal{O}_L$ is $\mathfrak{A}_H$-**locally free** if $\mathcal{O}_{L,\mathfrak{p}}$ is $\mathfrak{A}_{H,\mathfrak{p}}$-free for every prime $\mathfrak{p}$ of K.*

As in the Galois case, since $\mathcal{O}_{K,\mathfrak{p}}$ is $\mathcal{O}_K$-flat, we have that local freeness is implied by freeness.

Proposition 3.6.6. *If $\mathcal{O}_L$ is $\mathfrak{A}_H$-free, then $\mathcal{O}_L$ is $\mathfrak{A}_H$-locally free.*

6.2.1 Translation of local criteria

We can translate some of the criteria for freeness at extensions of p-adic fields from Section 4 to this setting. For the following results, fix a prime $\mathfrak{p}$ of K.

Proposition 3.6.7 ([Tru11], Proposition 5.1). *If $\mathfrak{A}_{H,\mathfrak{p}}$ is the only maximal $\mathcal{O}_{K,\mathfrak{p}}$-order in $H_{\mathfrak{p}}$, then $\mathcal{O}_{L,\mathfrak{p}}$ is $\mathfrak{A}_{H,\mathfrak{p}}$-free.*

Proof. Since L is H-free by Theorem 3.1.3, we have that $L_{\mathfrak{p}}$ is $H_{\mathfrak{p}}$-free. Now, we apply Proposition 3.4.24 with $S = \mathcal{O}_{L,\mathfrak{p}}$ and $A = H_{\mathfrak{p}}$, and the result follows. □

Proposition 3.6.8 ([Tru11], Proposition 5.2). *If $\mathfrak{A}_{H,\mathfrak{p}}$ is an $\mathcal{O}_{K,\mathfrak{p}}$-Hopf order in $H_{\mathfrak{p}}$ and $\mathcal{O}_{L,\mathfrak{p}}$ is $\mathfrak{A}_{H,\mathfrak{p}}$-tame, then $\mathcal{O}_{L,\mathfrak{p}}$ is $\mathfrak{A}_{H,\mathfrak{p}}$-free.*

Proof. We have that $K_{\mathfrak{p}}$ is a p-adic field, $L_{\mathfrak{p}}$ is an $H_{\mathfrak{p}}$-Galois extension of $K_{\mathfrak{p}}$ and $\mathcal{O}_{L,\mathfrak{p}}$ is an $\mathcal{O}_{K,\mathfrak{p}}$-order of $L_{\mathfrak{p}}$. Under the given hypotheses, we can apply Corollary 3.4.34, and the statement follows. □

We now use the results from Section 5.2 to obtain conclusions on completions by unramified and tamely ramified primes. We call N the permutation subgroup corresponding to the Hopf-Galois structure H on L/K.

First, we translate Proposition 3.5.13.

Proposition 3.6.9 ([Tru11], Proposition 5.3 and Theorem 5.4). *Suppose that L/K is abelian. If $\mathfrak{p}$ is unramified in L, then:*

1. *$\mathcal{O}_{L,\mathfrak{p}}[N]^G$ is an $\mathcal{O}_K$-Hopf order in H.*
2. *$\mathcal{O}_{L,\mathfrak{p}}$ is $\mathcal{O}_{L,\mathfrak{p}}[N]^G$-free.*

Proof. The proof of Proposition 1 by direct calculation as in [Tru11, Proposition 3.3]. As for 2, we proceed as in Proposition 3.5.13: the element $\theta := \sum_{\eta \in N} \eta$ is a left integral of $\mathcal{O}_{L,\mathfrak{p}}[N]^G$ and, since $\mathfrak{p}$ is unramified in L, there is $z \in \mathcal{O}_{L,\mathfrak{p}}$ such that $\theta \cdot z = 1$. Then $\mathcal{O}_{L,\mathfrak{p}}$ is $\mathcal{O}_{L,\mathfrak{p}}[N]^G$-tame, and hence $\mathcal{O}_{L,\mathfrak{p}}[N]^G$-free. □

Actually, the same holds without the restriction that L/K is abelian.

Proposition 3.6.10 ([Chi+21], Proposition 11.28). *If $\mathfrak{p}$ is unramified in $\widetilde{L}$, then $\mathcal{O}_{L,\mathfrak{p}}$ is $\mathcal{O}_{\widetilde{L},\mathfrak{p}}[N]^G$-free.*

Next, we consider Proposition 3.5.14.

Proposition 3.6.11. *Suppose that N is abelian. If the rational prime under $\mathfrak{p}$ does not divide $[L:K]$, then $\mathcal{O}_{L,\mathfrak{p}}$ is $\mathcal{O}_{\widetilde{L},\mathfrak{p}}[N]^G$-free.*

Proof. Let $\mathfrak{M}$ be the only maximal $\mathcal{O}_K$-order in H. Then, $\mathfrak{M}_{\mathfrak{p}}$ is the only maximal $\mathcal{O}_K$-order in $H_{\mathfrak{p}}$. Given $x \in \mathfrak{M}_{\mathfrak{p}}$, we have that $x \in \widetilde{L}_{\mathfrak{p}}[N]^G$, so $x \in \widetilde{L}_{\mathfrak{p}}[N]$. Now, we know that

$$\widetilde{L}_{\mathfrak{p}}[N] \cong \prod_{\mathfrak{P} | \mathfrak{p}\mathcal{O}_{\widetilde{L}}} \widetilde{L}_{\mathfrak{P}}[N].$$

In addition, by hypothesis $p \nmid |N|$, where p is the rational prime under $\mathfrak{p}$. Since $L_{\mathfrak{P}}$ is a p-adic field, Proposition 3.4.23 gives that $\mathcal{O}_{L,\mathfrak{P}}[N]$ is the integral closure of $\mathcal{O}_K$ in $\widetilde{L}_{\mathfrak{P}}[N]$. Then, the image of x under the isomorphism above lies in the product

$$\prod_{\mathfrak{P} | \mathfrak{p}\mathcal{O}_{\widetilde{L}}} \mathcal{O}_{\widetilde{L},\mathfrak{P}}[N] \cong \mathcal{O}_{\widetilde{L},\mathfrak{p}}[N].$$

Hence $x \in \mathcal{O}_{\widetilde{L},\mathfrak{p}}[N] \cap \widetilde{L}_p[N]^G = \mathcal{O}_{\widetilde{L},\mathfrak{p}}[N]^G$. We deduce that $\mathfrak{M}_{\mathfrak{p}} = \mathcal{O}_{\widetilde{L},\mathfrak{p}}[N]^G$. The result then follows from Proposition 3.4.24. □

There is a class of extensions for which local freeness is immediately deduced.

Definition 3.6.12. *Let L/K be a finite Galois extension of number fields. We say that L/K is* ***domestic*** *if every prime of K lying above a rational prime dividing $[L:K]$ is unramified in L.*

Corollary 3.6.13. *Let L/K be a domestic extension of number fields and let $H = \widetilde{L}[N]^G$ be an abelian Hopf-Galois structure on L/K. Then $\mathcal{O}_L$ is $\mathfrak{A}_H$-locally free.*

Proof. Let $\mathfrak{p}$ be a prime of K and let p be the rational prime under $\mathfrak{p}$. If $p \mid [L:K]$, then p is unramified in L. Thus, by Proposition 3.6.10, we have that $\mathcal{O}_{L,\mathfrak{p}}$ is $\mathfrak{A}_{H,\mathfrak{p}}$-free. Otherwise, if $p \nmid [L:K]$, we reach the same conclusion from Proposition 3.6.11. □

This situation simplifies even more for tame p-extensions.

Corollary 3.6.14. *Let L/K be a tamely ramified Galois p-extension of number fields and let $H = \widetilde{L}[N]^G$ be an abelian Hopf-Galois structure on L/K. Then $\mathcal{O}_L$ is $\mathfrak{A}_H$-locally free.*

Proof. Let $\mathfrak{p}$ be a prime of K. If p is not under $\mathfrak{p}$, then the prime under $\mathfrak{p}$ does not divide $[L:K]$, so $\mathcal{O}_{L,\mathfrak{p}}$ is $\mathfrak{A}_{H,\mathfrak{p}}$-free by Proposition 3.6.11. Otherwise, if p is under $\mathfrak{p}$, tameness yields that $\mathfrak{p}$ is unramified in L, and the $\mathfrak{A}_{H,\mathfrak{p}}$-freeness of $\mathcal{O}_{L,\mathfrak{p}}$ follows from Proposition 3.6.10. □

6.3 Global freeness over the ring of integers

Let L/K be an H-Galois extension of number fields and suppose that both $\mathcal{O}_L$ and $\mathfrak{A}_H$ are $\mathcal{O}_K$-free. We consider Problem 3.3.12 for this situation. This topic has been barely explored and most of the results available in this direction have arisen in the very recent years. So far, this problem has been attacked in two ways.

6.3.1 From local to global freeness through idèles theory

Suppose that $\mathcal{O}_L$ is $\mathfrak{A}_H$-locally free. In [Tru16], Truman introduced a strategy that involves the utilization of the theory of idèles in order to find a characterization for the $\mathfrak{A}_H$-freeness. Such a strategy is explained in all detail in [Tru09, Section 2.1.4]. We present here a summary of the strategy and the main results in literature obtained by this strategy.

The strategy

The customary setting is the one of $\mathcal{O}_K$-orders in a separable K-algebra, but we restrict to the case of the associated order $\mathfrak{A}_H$ in H.

Definition 3.6.15. *Let L/K be an H-Galois extension of number fields.*

1. *The* ***Grothendieck group*** *$\mathfrak{K}_0(\mathfrak{A}_H)$ of locally free $\mathfrak{A}_H$-modules is defined as the abelian group generated by $\mathfrak{A}_H$-isomorphism classes of locally free $\mathfrak{A}_H$-modules $[X]$ with the restrictions $[X \oplus Y] = [X] + [Y]$.*

2. *The* ***locally free class group*** *$\mathrm{Cl}(\mathfrak{A}_H)$ of $\mathfrak{A}_H$ is defined to be the cokernel of the map $\mathbb{Z} \longrightarrow \mathfrak{K}_0(\mathfrak{A}_H)$ defined by $n \mapsto [\mathfrak{A}_H^n]$.*

We can give a simple characterization for freeness in terms of the locally free class group of $\mathfrak{A}_H$.

Proposition 3.6.16 ([Tru09], Proposition 2.1.24)**.** *Let L/K be an H-Galois extension of number fields with H abelian and suppose that $\mathcal{O}_L$ is $\mathfrak{A}_H$-locally free. Then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free if and only if $\mathcal{O}_L$ has trivial class in* $\mathrm{Cl}(\mathfrak{A}_H)$*.*

Now, we may describe $\mathrm{Cl}(\mathfrak{A}_H)$ by means of the theory of idèles. All the products of the form $\prod_{\mathfrak{p}} f(\mathfrak{p})$ are taken in primes $\mathfrak{p}$ of K.

Definition 3.6.17. *Let L/K be an H-Galois extension of number fields*

1. *The **idèle group** of H is defined as*

$$\mathbb{J}(H) = \{(a_{\mathfrak{p}})_{\mathfrak{p}} \in \prod_{\mathfrak{p}} H_{\mathfrak{p}}^{\times} \mid a_{\mathfrak{p}} \in \mathfrak{A}_{H,\mathfrak{p}}^{\times} \textit{ for all but finitely many } \mathfrak{p}\}.$$

2. *The group of **principal idèles** is defined as the image of the diagonal embedding $H^{\times} \hookrightarrow \mathbb{J}(H)$ defined by $a \mapsto (a)_{\mathfrak{p}}$.*

3. *The group of **unit idèles** is defined by*

$$\mathbb{U}(H) = \{(a_{\mathfrak{p}})_{\mathfrak{p}} \in \prod_{\mathfrak{p}} H_{\mathfrak{p}}^{\times} \mid a_{\mathfrak{p}} \in \mathfrak{A}_{H,\mathfrak{p}}^{\times} \textit{ for all } \mathfrak{p}\}.$$

Proposition 3.6.18 ([Tru09], Proposition 2.1.25)**.** *Let L/K be an H-Galois extension of number fields with H abelian. Then there is a group isomorphism*

$$\mathrm{Cl}(\mathfrak{A}_H) \cong \mathbb{J}(H)/(H^*\mathbb{U}(H)).$$

In practice, one can follow this procedure:

1. Fix an H-normal basis generator x of L.

2. Fix a prime $\mathfrak{p}$ of K. Let $x_{\mathfrak{p}}$ be an $\mathfrak{A}_{H,\mathfrak{p}}$-generator of $\mathcal{O}_{L,\mathfrak{p}}$.

3. Let $h_{\mathfrak{p}}$ be such that $h_{\mathfrak{p}} \cdot x = x_{\mathfrak{p}}$.

4. We have $(h_{\mathfrak{p}})_{\mathfrak{p}}$. Study its class in the quotient $\mathbb{J}(H)/(H^*\mathbb{U}(H))$.

Results obtained

In the same reference [Tru16], Truman considered tamely ramified Galois extensions of number fields L/K with group $C_p \times C_p$. The Hopf-Galois structures on such an extension were determined and explicitly described at [Byo02]. Since every group of order p^2 is abelian, so is every Hopf-Galois structure on L/K. On the other hand, we know from Corollary 3.6.14 that $\mathcal{O}_L$ is $\mathfrak{A}_H$-locally free. Then, Proposition 3.6.16 applies in this situation. In [Tru16, Corollary 5.10], a necessary condition and a sufficient condition are stated for the $\mathfrak{A}_H$-freeness of $\mathcal{O}_L$ in terms of certain ideals having trivial class in certain ray class groups.

In [Tru12], Truman restricts to the case $p = 2$ and $K = \mathbb{Q}$, for which his characterization takes a very explicit form. This corresponds to the case in which L is a tamely ramified biquadratic number field. Write $L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ with $m, n \in \mathbb{Z}$

square-free. Let $k = \frac{mn}{d^2}$, where $d = \gcd(m, n)$. Then, $L/\mathbb{Q}$ admits three non-classical Hopf-Galois structures, each of which correspond to a quadratic subfield of L.

Tameness is equivalent to the congruences $m \equiv n \equiv 1 \pmod 4$. Then $k \equiv 1 \pmod 4$, and m, n and k can be exchanged indistinctly, and then so can we do with the non-classical Hopf-Galois structures on $L/\mathbb{Q}$.

Theorem 3.6.19 ([Tru12], Proposition 6.1)**.** *Let $L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ be a tamely ramified biquadratic number field and let H be the non-classical Hopf-Galois structure on L/K corresponding to $\mathbb{Q}(\sqrt{m})$. Then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free if and only if at least one of the generalized Pell equations*

$$x^2 + my^2 = \pm 2d$$

admits some solution $(x, y) \in \mathbb{Z}^2$.

The techniques presented in this section have been applied also to generalize the results on the Galois module structure for tamely ramified Kummer extensions of number fields to the setting of Hopf-Galois extensions. In this direction, Truman [Tru20] proved a characterization for freeness at tamely ramified extensions of the form $L = K(\sqrt[p]{a})$, $a \in \mathcal{O}_K$, such that $\zeta_p \notin K$. His result mimics the corresponding by Gómez Ayala [Aya94] for the Galois case.

Very recently, in his PhD thesis [Pre24], Prestidge used the same strategy to obtain a characterization for freeness at two classes of non-Galois extensions:

- $L = K(\sqrt[p]{a_1}, \dots, \sqrt[p]{a_r})$, p prime, $a_1, \dots, a_r \in \mathcal{O}_K$, $\zeta_p \notin K$.
- $L = K(\sqrt[m]{a})$, $m \in \mathbb{Z}$ odd and square-free, $a \in \mathcal{O}_K$, $\zeta_p \notin K$.

The these results are a Hopf-Galois analogue of the one by Del Corso and Rossi [DR13] for the Galois case.

6.3.2 An explicit method to describe the associated order

Let L/K be an H-Galois extension of number fields and suppose that $\mathcal{O}_K$ is a PID. Rio and the first author [GR22b] introduced an explicit method to produce a basis of the associated order $\mathfrak{A}_H$, thanks to which one can translate the question of the existence of an $\mathfrak{A}_H$-free generator for $\mathcal{O}_L$ to the solvability of a certain homogeneous equation. In some cases, this method is useful in some theoretical aspects; for instance, it gives rise to a proof of Theorem 3.3.17.

The strategy

Let $W = \{w_i\}_{i=1}^n$ be a K-basis of H. Suppose that one knows an integral basis $B = \{\gamma_j\}_{j=1}^n$ of L/K and the action of W on B, that is, the elements $m_{ij}^{(k)}(H, L) \in K$ such that

$$w_i \cdot \gamma_j = \sum_{k=1}^{n} m_{ij}^{(k)}(H, L)\gamma_k.$$

The matrix of the linear map $\rho_H \colon H \longrightarrow \mathrm{End}_K(L)$ defined by $\rho_H(h)(x) = h \cdot x$ is an $n^2 \times n$ matrix whose coefficients are the $m_{ij}^{(k)}(H, L)$ arranged in a suitable way.

Now, the assumption that $\mathcal{O}_K$ is a PID allow to reduce the matrix $M(H, L)$ by using linear transformations that correspond to isomorphisms of $\mathcal{O}_L^{n^2}$. This yields an $n \times n$ matrix, whose inverse provides an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$.

Let $V = \{v_i\}_{i=1}^n$ be an $\mathcal{O}_K$-basis of $\mathcal{O}_L$. For a given $\beta \in \mathcal{O}_L$, let $M_\beta(H,L)$ be the matrix whose i-th is formed by the coordinates of $v_i \cdot \beta$ with respect to B, where $1 \leq i \leq n$. Then, β is an $\mathfrak{A}_H$-free generator of $\mathcal{O}_L$ if and only if the determinant of $M_\beta(H,L)$ is an invertible element of $\mathcal{O}_L$. If one writes $\beta = \sum_{j=1}^n \beta_j\gamma_j$ with $\beta_j \in \mathcal{O}_K$, this reduces to the solvability of an homogeneous equation on the β_j.

Results obtained

In [GR22a], Rio and the first author used this method to provide a characterization for freeness at Galois quartic number fields.

In the case of tamely ramified biquadratic number fields, Theorem 3.6.19 is recovered. Acquire the notation therein. We state the criteria for wildly ramified biquadratic extensions. Up to reorderings of m, n and k, there are two possible cases (according to the form of an integral basis for L): $m \equiv 3 \pmod 4$ and $n,k \equiv 2 \pmod 4$ on the one hand, $m \equiv 1 \pmod 4$ and $n,k \not\equiv 1 \pmod 4$ on the other. For each $\gamma \in \{m,n,k\}$, let H_γ be the Hopf-Galois structure on $L/\mathbb{Q}$ associated to $\mathbb{Q}(\sqrt{\gamma})$.

Theorem 3.6.20 ([GR22a], Thoerem 5.9). *Let L be a wildly ramified biquadratic number field.*

1. *If $m \equiv 3 \pmod 4$ and $n,k \equiv 2 \pmod 4$, $\mathcal{O}_L$ is $\mathfrak{A}_{H_m}$-free (resp. $\mathfrak{A}_{H_n}$-free, resp. $\mathfrak{A}_{H_k}$-free) if and only if at least one of the equations $x^2 + my^2 = \pm 4d$ (resp. $x^2 + ny^2 = \pm 2d$, resp. $x^2 + ky^2 = \pm 2\frac{n}{d}$) is solvable.*

2. *If $m \equiv 1 \pmod 4$ and $n,k \not\equiv 1 \pmod 4$, $\mathcal{O}_L$ is $\mathfrak{A}_{H_m}$-free if and only if at least one of the equations $x^2 + my^2 = \pm 2d$ is solvable. Moreover, $\mathcal{O}_L$ is never $\mathfrak{A}_{H_n}$-free nor $\mathfrak{A}_{H_k}$-free.*

Now, suppose that L is a quartic cyclic number field. In this case, $L/\mathbb{Q}$ admits a unique non-classical Hopf-Galois structure H. Moreover, $L = \mathbb{Q}(\sqrt{a(d+b\sqrt{d})}$, where $a \in \mathbb{Z}$ is odd and square-free and d is square-free and coprime to a, and of the form $d = b^2 + c^2$ for some $c \in \mathbb{Z}_{>0}$.

Theorem 3.6.21 ([GR22a], Theorem 4.3). *Let $L = \mathbb{Q}(\sqrt{a(d+b\sqrt{d})}$ be a quartic cyclic number field and let H be its non-classical Hopf-Galois structure. Then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free if and only if the generalized Pell equation $x^2 - dy^2 = b$ has some integer solution $(x,y) \in \mathbb{Z}^2$ such that $b \mid x - cy$.*

In [Gil24a], the first author considered the class of H-Galois extensions L/K for which there is some finite set $S \subset L$ with $L = K(S)$ such that for every $h \in H$ and every $\alpha \in L$, $h \cdot \alpha = \lambda\alpha$ for some $\lambda \in K$. An element $\alpha \in L$ with that property is called an H-eigenvector. In the case that L/K is Galois and $H = H_c$, the extension L/K is Kummer and the elements of S are Kummer generators (see [Gil24a, Theorem 4.7]). Consequently, an extension L/K as above is called H-Kummer. It turns out that a subclass of those are related with almost classically Galois extensions L/K with normal closure $\widetilde{L}$ such that $\widetilde{L}/M$ is Kummer in the classical sense (see [Gil24a, Theorem 1.1]). On the other hand, the method above yields the following criterion.

Theorem 3.6.22 ([Gil24a], Theorem 1.2). *Let L/K be an H-Kummer extension associated to Dedekind domains. If L admits some integral basis which in addition is a generating system of H-eigenvectors, then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free.*

We finish our exposition by stating an application of this result to a concrete family of number fields. Note that if L/K is an almost classically Galois extension with complement M and normal closure $\widetilde{L}$, then for $J = \mathrm{Gal}(\widetilde{L}/K)$, $\lambda(J)$ gives $\widetilde{L}/M$ an almost classically Galois structure. We shall refer to this as the almost classically Galois structure for M.

Corollary 3.6.23 ([Gil24a], Proposition 7.3)**.** *Let $L = \mathbb{Q}(\sqrt[n]{a})$ with $n \in \mathbb{Z}_{\geq 2}$ and $a \in \mathbb{Z}$ square-free. Assume that $L \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ and that $\mathcal{O}_L = \mathbb{Z}[\sqrt[n]{a}]$. Then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free, where H is the almost classically Galois structure on $L/\mathbb{Q}$ for $\mathbb{Q}(\zeta_n)$.*

7 Exercises

1. Let n be a square-free integer and let $L = \mathbb{Q}(\sqrt{n})$.

   (a) Find a necessary and sufficient condition for L to possess a normal integral basis. Prove its validity.

   (b) Justify that $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}}$-free.

2. Let L/K be a Galois extension of p-adic fields with group G. Prove that L/K is tamely ramified if and only if $\mathcal{O}_K[G] = \mathfrak{A}_{L/K}$.

3. Let $L = \mathbb{Q}(\sqrt[3]{2})$ and let H be the only Hopf-Galois structure on $L/\mathbb{Q}$.

   (a) Let $\alpha \in L - \mathbb{Q}$ and let $f(x) = x^3 + a_1x^2 + a_2x + a_3$ be its minimal polynomial over $\mathbb{Q}$. Prove that α is an H-normal basis generator for L if and only if $a_1 \neq 0$ and $a_1^2 \neq 3a_2$.
   Hint: Let $(\alpha_i)_{i=1}^3$ be the roots of f with $\alpha_1 = \alpha$. Use the symmetric identities of the roots to prove that $\sum_{i=1}^3 \alpha_i^2 = a_1^2 - 2a_2^2$.

   (b) Determine explicitly $\int_H^l$. Is H unimodular?
   Hint: Find a generator w of H as a K-algebra and work with the K-basis $\{\mathrm{Id}, w, w^2\}$ of H. When considering products, use a degree 3 identity satisfied by w.

4. Let L/K be a (G, G')-separable H-Galois extension of p-adic fields with normal closure $\widetilde{L}$ and let N be the regular and G-stable subgroup of $\mathrm{Perm}(G/G')$ such that $H = \widetilde{L}[N]^G$. Prove that $\mathcal{O}_{\widetilde{L}}[N]^G \subseteq \mathfrak{A}_H$.

5. Let K be a p-adic field with valuation ring $\mathcal{O}_K$ and let G be a cyclic group with generator σ. Call $f = \sigma - 1_G$. Prove that $\mathcal{O}_K[f]$ is an $\mathcal{O}_K$-Hopf order in $K[G]$[1].

6. For the following extensions of number or p-adic fields L/K and Hopf-Galois structure H on L/K, determine whether $\mathcal{O}_L$ is $\mathfrak{A}_H$-free or not. In the case that L/K admits a unique Hopf-Galois structure, H is not specified. You are allowed to use any information at the LMFDB database.

   (a) $L = \mathbb{Q}(\sqrt[3]{2})$ and $K = \mathbb{Q}$; Number field 3.1.108.1.

[1] In fact, the $\mathcal{O}_K$-Hopf orders of $K[G]$ are $\mathcal{O}_K[\pi_K^{-i} f]$ for $0 \leq i \leq \lfloor \frac{e}{p-1} \rfloor$.

(b) $L = \mathbb{Q}(\sqrt{3}, \sqrt{2})$, $K = \mathbb{Q}$ and $H = H_3$ with the notation of Theorem 3.6.20; Number field 4.4.2304.1.

(c) $L = \mathbb{Q}_5(\alpha)$ and $K = \mathbb{Q}_5$, where $\alpha^3 + 5 = 0$; p-adic field 5.1.3.2a1.1.

(d) $L = \mathbb{Q}_5(\alpha)$ and $K = \mathbb{Q}_3$, where $\alpha^6 + 6\alpha^2 + 3 = 0$; p-adic field 3.1.6.7a2.1.

Bibliography

[Aya94] E. J. Gómez Ayala. “Bases normales d’entiers dans les extensions de Kummer de degré premier”. In: *Journal de Théorie des Nombres de Bordeaux* 6.1 [1994], pp. 95–116.

[Bac16] D. Bachiller. “Counterexample to a conjecture about braces”. In: *Journal of algebra* 453 [2016], pp. 160–176.

[BBF72] F. Bertrandias, J.-P. Bertrandias, and M.-J. Ferton. “Sur l’anneau des entiers d’une extension cyclique de degré premier d’un corps local.” In: *C. R. Acad. Sc. Paris* 274 [1972], pp. 1388–1391.

[Ber72] A.-M. Bergé. “Sur l’arithmétique d’une extension diédrale”. In: *Ann. Inst. Fourier* 22.2 [1972], pp. 31–59.

[BF72] F. Bertrandias and M.-J. Ferton. “Sur l’anneau des entiers d’une extension cyclique de degré premier d’un corps local.” In: *C. R. Acad. Sc. Paris* 274 [1972], pp. 1330–1333.

[BL96] Nigel P. Byott and Günter Lettl. “Relative Galois module structure of integers of abelian fields”. In: *Journal de Théorie des Nombres de Bordeaux* 8 [Oct. 1996], pp. 125–141. DOI: 10.5802/jtnb.160.

[Bou72] N. Bourbaki. *Commutative Algebra*. Elements of Mathematics. Hermann, Addison-Wesley, 1972.

[Byo02] N. P. Byott. “Integral Hopf–Galois Structures on Degree p^2 Extensions of p-adic Fields”. In: *Journal of Algebra* 248 [2002], pp. 334–365.

[Byo96] N. P. Byott. “Uniqueness of Hopf Galois Structure for Separable Field Extensions”. In: *Communications in Algebra* 24.10 [1996], pp. 3217–3228.

[Chi+21] L. N. Childs, C. Greither, K. P. Keating, A. Koch, T. Kohl, P. J. Truman, and R. G. Underwood. *Hopf Algebras and Galois Module Theory*. 1st ed. Mathematical Surveys and Monographs 260. American Mathematical Society, 2021.

[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.

[Coh91] P. M. Cohn. *Algebra*. 2nd ed. Vol. 3. John Wiley & Sons, 1991.

[Coh93] Henri Cohen. *A course in computational algebraic number theory*. 3rd, Corr. Print. Graduate Texts in Mathematics. Springer, 1993.

[CR87] Charles W. Curtis and Irving Reiner. *Methods of representation theory. With applications to finite groups and orders*. Revised. Vol. Vol.2. Pure & Applied Mathematics. Wiley-Interscience, 1987. ISBN: 9780471888710,0471888710.

[CRV16] T. Crespo, A. Rio, and M. Vela. “Induced Hopf Galois structures”. In: *Journal of Algebra* 457 [2016], pp. 312–322. ISSN: 0021-8693.

[DR10] I. Del Corso and L. P. Rossi. “Normal integral basis for cyclic Kummer extensions”. In: *Journal of Pure and Applied Algebra* 214 [2010], pp. 385–391.

[DR13] I. Del Corso and L. P. Rossi. “Normal integral bases and tameness conditions for Kummer extensions”. In: *Acta Arithmetica* 160 [Jan. 2013].

[Fer24] F. Ferri. “Leopoldt-type theorems for non-abelian extensions of $\mathbb{Q}$”. In: *Glasgow Mathematical Journal* 66.2 [2024], pp. 308–337. DOI: 10.1017/S0017089523000460.

[FT92] A. Fröhlich and M. J. Taylor. *Algebraic number theory*. CUP. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1992.

[Gil24a] D. Gil-Muñoz. “A generalization of Kummer Theory to Hopf-Galois extensions”. In: *Journal of Algebra* 660 [2024], pp. 190–235.

[Gil24b] D. Gil-Muñoz. “Hopf-Galois module structure of degree p extensions of p-adic fields”. Preprint. 2024.

[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.

[GR22a] D. Gil-Muñoz and A. Rio. “Hopf-Galois module structure of quartic Galois extensions of $\mathbb{Q}$”. In: *Journal of Pure and Applied Algebra* 266 [2022].

[GR22b] D. Gil-Muñoz and A. Rio. “Induced Hopf Galois structures and their Local Hopf Galois Modules”. In: *Publicacions Matemàtiques* 66.1 [2022].

[Gre+99] C. Greither, D. R. Replogle, K. Rubin, and A. Srivastav. “Swan modules and Hilbert-Speiser number fields”. In: *J. Number Theory* 79.1 [1999], pp. 164–173.

[Joh15] H. Johnston. “Explicit integral Galois module structure of weakly ramified extensions of local fields”. In: *Proceedings of the American Mathematical Society* 143 [Dec. 2015], pp. 5059–5071.

[Leo59] H.-W. Leopoldt. “Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers”. In: *Journal für die reine und angewandte Mathematik* 1959.201 [1959], pp. 119–149.

[Let98] G. Lettl. “Relative Galois module structure of integers of local abelian fields”. In: *Acta Arithmetica* 85 [1998], pp. 235–238.

[LL07] F. Lorenz and S. Levy. *Algebra. Fields with structure, algebras and advanced topics Volume 2*. 1st ed. Universitext. Springer, 2007. ISBN: 0387724877; 9780387724874.

[Mar69] J. Martinet. “Sur l’arithmétique des extensions galoisiennes à groupe de Galois diédral d’ordre 2p”. In: *Annales de l’institut Fourier* 19.1 [1969], pp. 1–80.

[Mar77] D. A. Marcus. *Number fields*. Universitext. Springer, 1977.

[MR89] H. Matsumura and M. Reid. *Commutative ring theory*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1989. ISBN: 9780521367646; 0521367646.

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

[Noe32] E. Noether. "Normalbasis bei Körpern ohne höhere Verzweigung." In: 1932.167 [1932], pp. 147–152. DOI: doi:10.1515/crll.1932.167.147. URL: https://doi.org/10.1515/crll.1932.167.147.

[Pre24] G. Prestidge. "Hopf-Galois module structure of some non-normal extensions". PhD thesis. University of Keele, 2024.

[Rib72] P. Ribenboim. *Algebraic Numbers (Pure & Applied Mathematics Monograph)*. 1972. ISBN: 9780471718048; 0471718041.

[Sch77] H. J. Schneider. "Cartan matrix of liftable finite group schemes". In: *Communications in algebra* 5 [1977], pp. 795–819.

[Ser79] J.-P. Serre. *Local Fields*. Graduate Texts in Mathematics. Springer, 1979.

[SV18] A. Smoktunowicz and L. Vendramin. "On skew braces (with an appendix by N. Byott and L. Vendramin)". In: *J. Comb. Algebra* 2.4 [2018], pp. 47–86.

[Tho10] L. Thomas. "On the Galois module structure of extensions of local fields". In: *Publications mathématiques de Besançon* [2010], pp. 157–194.

[Tru09] P. J. Truman. "Hopf-Galois Module Structure of Some Tamely Ramified Extensions". PhD thesis. University of Exeter, 2009.

[Tru11] P. J. Truman. "Towards a Generalisation of Noether's Theorem to Nonclassical Hopf-Galois Structures". In: *New York Journal of Mathematics* 17 [2011], pp. 799–810.

[Tru12] Paul J. Truman. "Hopf-Galois module structure of tame biquadratic extensions". In: *Journal de Théorie des Nombres de Bordeaux* 24.1 [Mar. 2012], pp. 173–199. URL: http://eudml.org/doc/251057.

[Tru13] P. J. Truman. "Integral Hopf-Galois structures for tame extensions". In: *New York Journal of Mathematics* 19 [2013], pp. 647–655.

[Tru16] P. J. Truman. "Hopf-Galois module structure of tame $C_p \times C_p$ extensions". In: *Journal de Theorie des Nombres de Bordeaux* 28.2 [2016], pp. 557–582.

[Tru18] P. J. Truman. "Commutative Hopf–Galois module structure of tame extensions". In: *Journal of Algebra* 503 [2018], pp. 389–408. ISSN: 0021-8693. DOI: https://doi.org/10.1016/j.jalgebra.2018.01.047.

[Tru20] Paul J. Truman. "Hopf-Galois module structure of tamely ramified radical extensions of prime degree". In: *Journal of Pure and Applied Algebra* 224.5 [2020]. ISSN: 0022-4049. DOI: https://doi.org/10.1016/j.jpaa.2019.106231.

[Tru25] P. J. Truman. "On some semidirect products of skew braces arising in Hopf-Galois theory". Preprint. 2025.

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