ULB FACULTÉ DES SCIENCES

UNIVERSITÉ LIBRE DE BRUXELLES

Correspondence theorems in Hopf-Galois theory for separable field extensions

Thesis submitted by Hoan-Phung BUI

in fulfilment of the requirements of the PhD Degree in Science ("Docteur en Sciences")

Academic year 2019-2020

Supervisor: Professor Joost VERCRUYSSE
Université Libre de Bruxelles
Co-supervisor: Professor Gabor WIESE
Université du Luxembourg

Correspondence theorems in Hopf-Galois theory for separable field extensions

Hoan-Phung Bui

Remerciements

Je voudrais commencer par remercier du fond du coeur mes promoteurs, Joost Vercruysse et Gabor Wiese, pour ces 6 années passées à leurs côtés. J'aimerais leur témoigner ma reconnaissance pour n'avoir jamais cessé de croire en moi et pour m'avoir toujours soutenu même lorsque ma motivation faiblissait. Je les remercie pour leur patience et leur bienveillance ainsi que pour leur disponibilité.

En plus de leurs qualités humaines, j'ai sincèrement aimé les échanges que j'ai eus avec eux. Chaque réunion fut toujours très enrichissante pour moi. Leur expertise différente en mathématiques leur a permis d'être très complémentaires dans la supervision de cette thèse à mi-chemin entre plusieurs domaines. Je leur suis reconnaissant pour toutes les réunions organisées à Bruxelles comme au Luxembourg et pour les déplacements effectués (merci, en particulier, à Gabor pour l'accueil que j'ai reçu à chacune de mes visites au Luxembourg). Je tiens également à leur témoigner ma gratitude pour la relecture attentive de ce document, pour leurs commentaires très pertinents et pour les nombreuses réunions en vidéoconférence qui m'ont donné la force nécessaire pour finaliser ce travail.

I would also like to thank Michele D'Adderio, Simone Gutt, Nigel Byott and Christian Lomp for their careful review. Their relevant comments helped improve my thesis.

Je remercie sincèrement mes parents qui m'ont toujours encouragé et poussé dans les études. Ils ont travaillé dur durant toute leur vie afin que mes frères et moi ne manquions de rien et puissons aller à l'université. Sans leur soutien et leur amour, je n'aurais probablement pas été si loin. Je suis aussi reconnaissant envers mon frère Hoan Long qui est toujours présent pour moi lorsque j'ai besoin de lui et envers mon

frère Hoan-Vuong qui m'a tiré vers le haut quand j'étais petit. Je tiens aussi à remercier mon oncle Chu Hong, ma tante Di Be et mes cousins Minh Tuan et Minh Tai pour les moments passés ensemble lors des réunions de famille. Ces moments ont toujours été pour moi de vrais instants de bonheur et m'ont aidé à tenir tout au long de ma thèse.

Je tiens également à faire part de ma gratitude envers mes amis mathématiciens et physiciens pour les moments de détente partagés ensemble. Merci à Thierry, Julie, Christine, François, Cédric, Nicolas, Thibaut, Jérémie, Keno, Mitia, Anna, Florence, Cédric, Jonathan, Samy, Tressy, Gaetan, Piotr, Claire, Jamina etc. Je pense en particulier aux moments passés à leurs côtés sur le campus lors de nos années d'étude et de thèse ainsi qu'aux soupers passés chez les uns et les autres, aux après-midi jeux de société, aux parties de badminton et plus antérieurement aux répétitions de chorale. Je les remercie pour ces moments de joie. Merci aussi à eux pour m'avoir écouté et rassuré dans mes moments de doute en partageant notamment leurs propres expériences de thèse.

Pour finir, j'aimerais remercier ma femme, Sylvie, qui m'a accompagné tout au long de cette aventure et avec qui je partage ma vie depuis 10 ans. A l'image de mes promoteurs, elle n'a jamais cessé de croire en moi. Je la remercie pour sa gentillesse et sa douceur ainsi que pour sa patience dans les périodes plus compliquées. Je lui suis infiniment reconnaissant pour tout l'amour qu'elle me donne et qui me porte au quotidien. Merci aussi à sa famille pour tous les encouragements et les gentils mots que j'ai reçus de leur part lors de ma fin de thèse ainsi que pour tous les bons moments passés à leurs côtés lors des réunions de famille.

Contents

Introduction

Let L/K be a finite Galois extension, i.e. a field extension which is both separable and normal, and let $G = \mathrm{Gal}(L/K)$ be its Galois group. Then the fundamental theorem of Galois theory says that there is a correspondence between the set of intermediate fields of L/K and the set of subgroups of G. Explicitly, if G_0 is a subgroup of G, we associate to G_0 the set of G_0-invariants

$$L^{G_0} := \big\{x \in L \,|\, \sigma(x) = x \quad \forall \sigma \in G_0\big\},$$

which is an intermediate field of L/K. On the other hand, if L_0 is an intermediate field of L/K, then L/L_0 is also a Galois extension. We then associate to L_0 the group $\mathrm{Gal}(L/L_0)$, which is a subgroup of G. We therefore get the correspondence theorem for finite Galois extensions: the maps

$$\begin{aligned} \big\{G_0 \subseteq G \text{ subgroup}\big\} &\rightleftarrows \big\{L/L_0/K \text{ intermediate field}\big\} : \\ G_0 &\longmapsto L^{G_0} \\ \mathrm{Gal}(L/L_0) &\longmapsfrom L_0 \end{aligned}$$

are bijections, which are inverse to each other and inclusion-reversing. It is natural to ask whether such a correspondence exists for a larger class of extensions.

For example, the Jacobson-Bourbaki theorem reformulates the correspondence theorem from (infinite) Galois theory as a bijection between subfields L_0 of finite codimension in a field L on the one hand, and their linear endomorphism rings $\mathrm{End}_{L_0}(L)$ on the other hand, and is also valid for division rings (i.e. "non-commutative fields") [Jac85]. Sweedler [Swe75] generalized this theorem further by using the language of

corings (which are coalgebras over a not necessarily commutative base).

In a different direction, Galois theory has been extended to commutative rings that are not necessarily fields by Auslander and Goldman [AG60] and by Chase, Harrison and Rosenberg [CHR65], see also [DI71].

Another possibility is to replace the group action by a Hopf algebra (co)action, leading to Hopf-Galois theory. One can motivate the use of Hopf algebras in Galois theory by the observation that, in a finite Galois extension L/K, all K-linear endomorphisms can be described as $L \otimes_K K[G]$. In fact, finite Galois extensions are exactly finite separable extensions L/K with $G = \mathrm{Aut}(L/K)$ such that the morphism of K-vector spaces

$$L \otimes_K K[G] \longrightarrow \mathrm{End}_K(L) : x \otimes \sigma \longmapsto \big(y \mapsto x\sigma(y)\big)$$

is bijective. Here, the finite group of automorphisms G appears in the Hopf algebra $K[G]$. Substituting $K[G]$ with another Hopf algebra leads to Definition 1.60 of Hopf-Galois extensions introduced by Chase and Sweedler [CS69].

The first step towards the generalization of the classical correspondence theorem is given by Chase and Sweedler.

Proposition 2.2. *[CS69, Thm. 7.6] Let L/K be a finite H-Galois extension. For a Hopf subalgebra $H_0 \subseteq H$ we define*

$$\mathit{Fix}(H_0) = \big\{x \in L \,|\, h \cdot x = \epsilon(h)x \quad \forall h \in H_0\big\}.$$

Then the map

$$\mathit{Fix} : \big\{H_0 \subseteq H \ \textit{Hopf subalgebra}\big\} \longrightarrow \big\{L/L_0/K \ \textit{intermediate field}\big\}$$

is injective and inclusion-reversing.

This map is not a correspondence in general because not every subfield lies in the image of Fix. A correspondence theorem, which is fully analogous to the classical one above, does not seem to be known.

This thesis aims at providing such a correspondence theorem for finite separable Hopf-Galois extensions. We will also describe a variant of this correspondence which

will be analogous, in classical Galois theory, to the correspondence between intermediate fields $L/L_0/K$ that are normal (hence Galois) over K and normal subgroups $G_0 \subseteq G$. To do this, we will characterize the image of Fix in a natural and intrinsic way. For that purpose, we introduce the notions of H-subextensions (Definition 2.16) and H-normal extensions (Definition 2.20), the latter being H-subextensions which are also H-stable (in the obvious sense $H \cdot L_0 \subseteq L_0$). We will also describe the inverse of Fix using several maps. First, we define the annihilator of an intermediate field L_0 (Definition 2.14) to be

$$\mathrm{Ann}_H(L_0) = \big\{h \in H \,|\, h \cdot x = 0 \quad \forall x \in L_0\big\}.$$

One should note that $\mathrm{Ann}_H(L_0)$ is not a Hopf subalgebra of H but it is a left ideal two-sided coideal of H if L_0 is an H-subextension (Proposition 2.23(b)) and it is a Hopf ideal of H if L_0 is H-normal (Proposition 2.23(d)). Secondly, we will be using a well-known correspondence between Hopf subalgebras of H and left ideals two-sided coideals of H (Definition 1.56):

1. if I is a left ideal two-sided coideal of H and if $\pi : H \twoheadrightarrow H/I$ is the natural projection, then we define

   $$\varphi(I) = \big\{h \in H \,|\, \pi(h_{(1)}) \otimes h_{(2)} = \pi(1_H) \otimes h\big\},$$

   which is a Hopf subalgebra of H (Theorem 1.57);

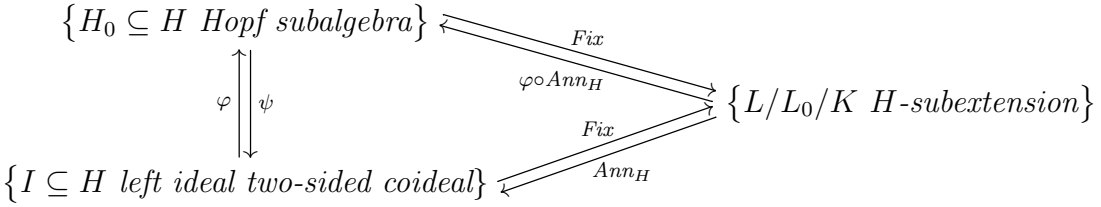
2. if $A \subseteq H$ is a Hopf subalgebra, then we define $A^+ = \big\{h \in A \,|\, \epsilon(h) = 0\big\}$ and

   $$\psi(A) = HA^+$$

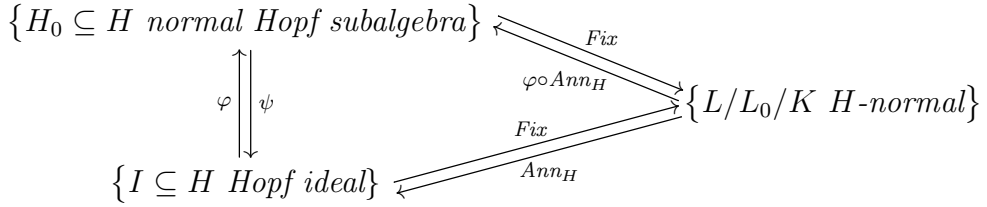
   which is a left ideal two-sided coideal of H (Theorem 1.57).

In this terminology, the main correspondence theorem for finite separable Hopf-Galois extensions proved in this thesis is the following.

Theorem 2.31. *Let L/K be a finite separable H-Galois extension, then the maps*



are inverse bijections. Moreover, the above correspondence restricts to the following inverse bijections:



The notions of H-subextensions and H-normal extensions behave exactly in the same way as in classical Galois theory. Indeed, if L_0 is an H-subextension, then L/L_0 is $L_0 \otimes_K H_0$-Galois with $H_0 = \big((\varphi \circ \mathrm{Ann}_H(L)\big)(L_0)$ (Proposition 2.33(b)). Also, if L_0 is H-normal, then L_0/K is $H/\mathrm{Ann}_H(L_0)$-Galois (Proposition 2.23(d)). Moreover, intersections and composita behave well (Proposition 2.54).

A key input of this thesis is provided by the work of Greither and Pareigis, to which also the title of the thesis pays reverence. In [GP87], they associated to a Hopf-Galois structure on a separable field extension a group, which we call the Greither-Pareigis group (Theorem 2.6). More precisely, if L/K is a finite separable H-Galois extension and if we define $\widetilde{L}/K$ a finite Galois extension containing L, $G = \mathrm{Gal}(\widetilde{L}/K)$, $G' = \mathrm{Gal}(\widetilde{L}/L)$ and $X = G/G'$, then the Greither-Pareigis group N can be seen as a subset of the permutation group $\mathrm{Perm}(X)$. The study of the group N (and more precisely, the study of the subgroups of N) is a way to better understand the correspondence theorem. A variant of our main correspondence theorem can be formulated in terms of the Greither-Pareigis group $N \subseteq \mathrm{Perm}(X)$.

Theorem 2.45. *Let L/K be a finite separable H-Galois extension and let $N \subseteq Perm(X)$ be its associated Greither-Pareigis group. Then the maps*

$$\big\{\mathcal{N} \subseteq N \text{ subgroup normalized by } \lambda(G)\big\} \underset{\mathcal{N}}{\overset{Fix \circ \mathcal{H}}{\rightleftarrows}} \big\{L/L_0/K \ H\text{-subextension}\big\}$$

are inverse bijections. Moreover, the above correspondence restricts to the following inverse bijections:

$$\big\{\mathcal{N} \subseteq N \text{ normal subgroup normalized by } \lambda(G)\big\} \underset{\mathcal{N}}{\overset{Fix \circ \mathcal{H}}{\rightleftarrows}} \big\{L/L_0/K \ H\text{-normal}\big\}$$

It is again a remarkably close analog of the classical theorem of Galois theory, now in the sense that H-subextensions and H-normal extensions correspond respectively to subgroups and normal subgroups of the Greither-Pareigis group, together with an

extra condition of normalization, which is inherent to the Greither-Pareigis group.

As said earlier, all the intermediate fields of a finite H-Galois extension do not arise as the set of invariants for some Hopf subalgebra. Equivalently, not all intermediate fields are H-subextensions. In [GP87], Greither and Pareigis say that the correspondence theorem holds in its *strong form* if the map Fix defined in Proposition 2.2 is surjective (and hence bijective). Obviously, this is the case for classical Galois extension. They also defined a larger class of extensions, called *almost classical Galois extensions*, for which they proved that the correspondence theorem holds in its strong form for a suitable Hopf-Galois structure. In [CRV16], Crespo, Rio and Vela showed that the class of Hopf-Galois extensions for which the correspondence is bijective is larger than the class of almost classically Galois extensions. Another approach for this problem is given in [KKTU19] where Koch, Kohl, Truman and Underwood translated the correspondence in Proposition 2.2 into a correspondence between the subgroups of the Greither-Pareigis group N normalized by $\lambda(G)$ and the subgroups of the Galois group $G = \mathrm{Gal}(\widetilde{L}/K)$.

One other interesting feature is that we can replace the Greither-Pareigis group N of a Hopf-Galois extension by its opposite N^{opp}, thus obtaining an opposite Hopf-Galois structure $H^\dagger$ on L/K (Lemmas 2.47 and 2.48). A further main result of this thesis is that H-subextensions and H-stable extensions correspond to each other under passage to the opposite Hopf-Galois structure. This makes the possibly technically not so elegant definition of H-subextension (Definition 2.16) appear very natural.

Theorem 2.51. *Let L/K be an H-Galois extension and let $H^\dagger$ be its opposite Hopf-Galois structure. Let L_0 be an intermediate field, then*

(a) L_0 is H-stable if and only if L_0 is an $H^\dagger$-subextension;

(b) L_0 is an H-subextension if and only if L_0 is $H^\dagger$-stable.

As pointed out above, H-normal extensions lead to quotient structures. It is thus possible to consider infinite towers of Hopf-Galois extensions as in classical Galois theory. As it turns out, the canonical Galois map which is used to define Hopf-Galois extensions in the finite case, is no longer bijective for infinite (classical) Galois extensions. Rather it is injective and has a dense image with respect to a suitably defined topology. Taking this point of view, we make first steps towards infinite Hopf-Galois extensions in chapter 3, and obtain a first correspondence theorem between intermediate H-normal subextensions and open Hopf ideals (Theorem 3.14). In the

final Chapter 4, we give some indications how this theory could be developed further.

We point out that, in the literature, a dual point of view on Hopf-Galois theory is often used. In this thesis, we were led to strive to obtain correspondence theorems as close as possible to the one of classical Galois theory. In the case of finite dimensional Hopf algebras (covering the main part of this thesis), both approaches are however completely equivalent. Moreover, in the literature, several variations of the correspondence theorem for Hopf-Galois theory have been discussed. Let us mention in particular [OZ94] and [Sch98], where a bijective correspondence is described between the Hopf subalgebras of H and the intermediate extensions that are stable under the action of a "transformed Hopf algebra". This result seems closely related to our characterization of H-subextensions as $H^\dagger$-stable extensions (see also Chapter 4).

We give a short outline of the thesis. Chapter 1 is a presentation of the background on Hopf algebras and Hopf-Galois extensions. Chapter 2 is the core of the thesis. After introducing the work of Greither and Pareigis in section 2.2, we will prove our correspondence theorem for Hopf-Galois theory in section 2.5 and its variant using the Greither-Pareigis group in section 2.6. Chapter 3 is devoted to first steps towards an infinite Hopf-Galois theory and finally in Chapter 4, we discuss some directions for future investigations.

1

Hopf algebras

1.1 Basic definitions

In this section, we will review some of the basic concepts and known results about Hopf algebras. All the proofs can be found in [DNR01] and [BW03].

Throughout this section, R will be a commutative ring with unity. Unadorned tensors are assumed to be taken over R unless specified otherwise.

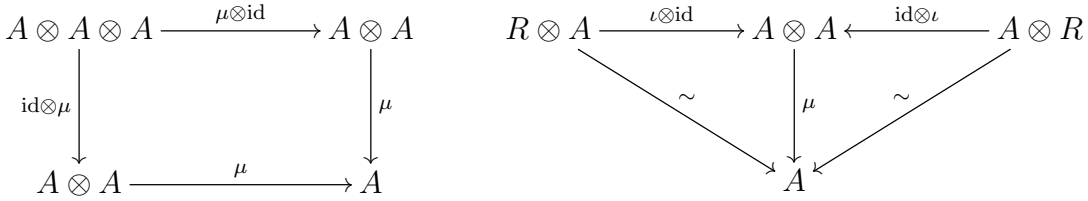
1.1.1 Algebras, coalgebras, bialgebras and Hopf algebras

We will first reformulate the classical definition of R-algebras using commutative diagrams. Then, we will define R-coalgebras whose structure is the dual of that of R-algebras.

Definition 1.1. An *R-algebra* A is an R-module together with

1. a multiplication map $\mu : A \otimes A \longrightarrow A$,
2. a unit map $\iota : R \longrightarrow A$,

such that both μ and ι are R-module morphisms and such that the following diagrams commute:



The left diagram describes the associativity of the multiplication and the right diagram describes the existence of a unit in A: $1_A = \iota(1_R)$.

Obviously, this is equivalent to the classical definition of an R-algebra, that is a ring A together with a ring morphism $R \longrightarrow Z(A)$ where $Z(A)$ is the center of A.

Definition 1.2. An R-algebra A is *commutative* if for all $a, a' \in A$ we have $\mu(a \otimes a') = \mu(a' \otimes a)$.

Alternatively, we can define the commutativity of an R-algebra by using the following map.

Definition 1.3. Let M and M' be two R-modules, we define the *switch map*

$$\sigma : M \otimes M' \longrightarrow M' \otimes M : m \otimes m' \longmapsto m' \otimes m.$$

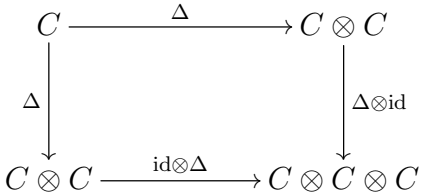
Therefore, an R-algebra A is commutative if and only if $\mu = \mu \circ \sigma$.

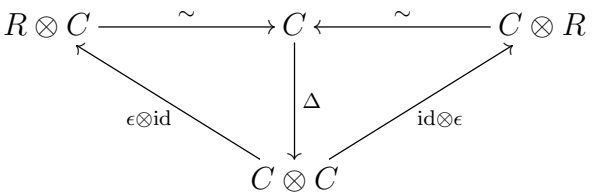
We will now take the dual of the diagrams of Definition 1.1 to obtain the following definition.

Definition 1.4. An *R-coalgebra* C is an R-module together with

1. a comultiplication map $\Delta : C \longrightarrow C \otimes C$,
2. a counit map $\epsilon : C \longrightarrow R$,

such that both Δ and ϵ are R-module morphisms and such that the following diagrams commute:





The left diagram describes the coassociativity of the comultiplication and the right diagram describes the counital condition.

Let $c \in C$, its image by the comultiplication lies in $C \otimes C$. Therefore, $\Delta(c)$ must be of the form $\sum_{i=1}^{n} c_{i1} \otimes c_{i2}$. To simplify the writing, we will adopt the Sweedler notation:

$$\Delta(c) = c_{(1)} \otimes c_{(2)} \in C \otimes C.$$

The diagrams of Definition 1.4 can thus be expressed by the equalities

$$c_{(1)(1)} \otimes c_{(1)(2)} \otimes c_{(2)} = c_{(1)} \otimes c_{(2)(1)} \otimes c_{(2)(2)} =: c_{(1)} \otimes c_{(2)} \otimes c_{(3)}$$

and

$$\epsilon\big(c_{(1)}\big)c_{(2)} = c = c_{(1)}\epsilon\big(c_{(2)}\big).$$

Definition 1.5. An R-coalgebra C is *cocommutative* if $\Delta = \sigma \circ \Delta$ where σ is the switch map defined in Definition 1.3. With the Sweedler notation, the cocommutativity of C can be expressed by the equality

$$c_{(1)} \otimes c_{(2)} = c_{(2)} \otimes c_{(1)}.$$

Example 1.6. Let S be any set and let $R[S]$ be the free R-module generated by S. Then $R[S]$ is a cocommutative R-coalgebra with comultiplication and counit defined by

1. $\Delta : R[S] \longrightarrow R[S] \otimes R[S] : s \longmapsto s \otimes s \quad \forall s \in S$,
2. $\epsilon : R[S] \longrightarrow R : s \longmapsto 1_R \quad \forall s \in S$.

Definition 1.7. Let C and C' be two R-coalgebras and let $f : C \longrightarrow C'$ be an R-module morphism. Then f is a *coalgebra morphism* if f preserves the comultiplication and the counit, i.e. if the following diagrams commute:

$$\begin{array}{ccc} C & \xrightarrow{\ f\ } & C' \\ {\scriptstyle \Delta_C}\downarrow & & \downarrow{\scriptstyle \Delta_{C'}} \\ C \otimes C & \xrightarrow{\ f \otimes f\ } & C' \otimes C' \end{array} \qquad \begin{array}{ccc} C & \xrightarrow{\ f\ } & C' \\ {\scriptstyle \epsilon_C}\downarrow & & \downarrow{\scriptstyle \epsilon_{C'}} \\ R & = & R \end{array}$$

With the Sweedler notation, the diagrams can be expressed by the equalities

$$f(c_{(1)}) \otimes f(c_{(2)}) = f(c)_{(1)} \otimes f(c)_{(2)} \ \text{ and } \ \epsilon_{C'}\big(f(c)\big) = \epsilon_C(c).$$

Definition 1.8. Let C be an R-coalgebra and let $I \subseteq C$ be an R-submodule. Then I is

1. a *right* (resp. *left*) *coideal* of C if $\Delta(I) \subseteq I \otimes C$ (resp. if $\Delta(I) \subseteq C \otimes I$),
2. a *coideal* (or a *two-sided coideal*) of C if $\Delta(I) \subseteq I \otimes C + C \otimes I$ and if $\epsilon(I) = 0$.

If I is a right (resp. left) coideal of C, then $\Delta(I) \subseteq I \otimes C \subseteq I \otimes C + C \otimes I$ (resp. $\Delta(I) \subseteq C \otimes I \subseteq I \otimes C + C \otimes I$). Therefore, any right (resp. left) coideal with $\epsilon(I) = 0$ is also a coideal. Conversely, a coideal is not necessarily a right or left coideal.

Proposition 1.9. *Let C be an R-coalgebra and let $I \subseteq C$ be a coideal. Then there is a canonical coalgebra structure on C/I such that the natural projection $C \twoheadrightarrow C/I$ is a coalgebra morphism.*

Definition 1.10. Let C be an R-coalgebra and let $C_0 \subseteq C$ be an R-submodule. Then C_0 is a *subcoalgebra* of C if $\Delta(C_0) \subseteq C_0 \otimes C_0$.

Proposition 1.11. *Suppose C is flat over R. Let C and C' be two R-coalgebras and let $f : C \longrightarrow C'$ be a coalgebra morphism. Then $\operatorname{Ker} f$ is a coideal of C and $\operatorname{Im} f$ is a subcoalgebra of C'.*

We would like to work with R-modules that have the structures of R-algebra and R-coalgebra simultaneously. However, if the two structures are not compatible in some way, we would not be able to say anything more than if we just looked at them separately. This motivates the following definition.

Definition 1.12. An *R-bialgebra* B is an R-module which is both an R-algebra and an R-coalgebra and which satisfy the following compatibility conditions:

1. $\Delta(bb') = b_{(1)}b'_{(1)} \otimes b_{(2)}b'_{(2)} \quad \forall b, b' \in B$ (μ and Δ are compatible),
2. $\epsilon(bb') = \epsilon(b)\epsilon(b') \quad \forall b, b' \in B$ (μ and ϵ are compatible),
3. $\Delta(1_B) = 1_B \otimes 1_B$ (ι and Δ are compatible),
4. $\epsilon(1_B) = 1_R$ (ι and ϵ are compatible).

Remark 1.13. If we endow $B \otimes B$ with a structure of R-algebra given by

$$\mu_{B\otimes B}\big((b_1 \otimes b'_1) \otimes (b_2 \otimes b'_2)\big) = b_1b_2 \otimes b'_1b'_2 \text{ and } \iota_{B\otimes B}(1_R) = 1_B \otimes 1_B$$

and with a structure of R-coalgebra given by

$$\Delta_{B\otimes B}(b \otimes b') = (b_{(1)} \otimes b'_{(1)}) \otimes (b_{(2)} \otimes b'_{(2)}) \text{ and } \epsilon_{B\otimes B}(b \otimes b') = \epsilon(b)\epsilon(b'),$$

then the compatibility conditions can be reformulated by either of the following equivalent statements:

1. Δ and ϵ are algebra morphisms,

2. μ and ι are coalgebra morphisms.

Example 1.14. Let S be a monoid (that is, a set with an associative operation and a unit), then the R-algebra $R[S]$ is also a cocommutative R-bialgebra if we endow $R[S]$ with the R-coalgebra structure as in Example 1.6.

Definition 1.15. Let B and B' be two R-bialgebras and let $f : B \longrightarrow B'$ be an R-module morphism. Then f is a *bialgebra morphism* if f is both an algebra morphism and a coalgebra morphism.

Definition 1.16. Let B be an R-bialgebra and let $I \subseteq B$ be an R-submodule. Then I is a *biideal* of B if I is both an ideal and a coideal of B.

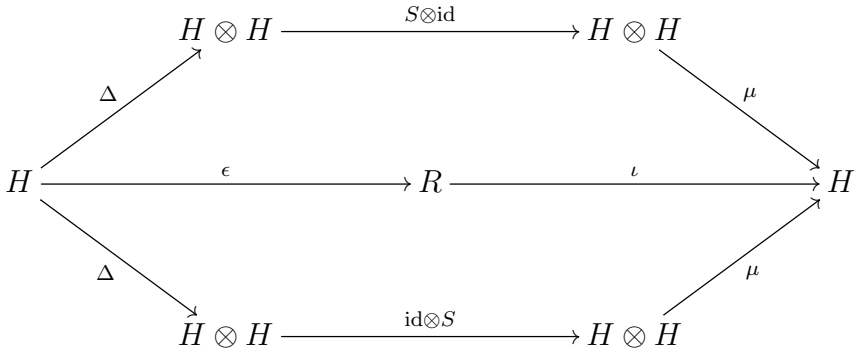
Proposition 1.17. *Let B be an R-bialgebra and let $I \subseteq B$ be a biideal. Then there is a canonical bialgebra structure on B/I such that the natural projection $B \twoheadrightarrow B/I$ is a bialgebra morphism.*

Definition 1.18. Let B be an R-bialgebra and let $B_0 \subseteq B$ be an R-submodule. Then B_0 is a *subbialgebra* of B if B_0 is both a subalgebra and a subcoalgebra of B.

Proposition 1.19. *Suppose B is flat over R. Let B and B' be two R-bialgebras and let $f : B \longrightarrow B'$ be a bialgebra morphism. Then $\operatorname{Ker} f$ is a biideal of B and $\operatorname{Im} f$ is a subbialgebra of B'.*

We will now define a special class of R-bialgebras which have an additional map that will, in a way, play the role of the inversion in a group.

Definition 1.20. An *R-Hopf algebra H* is an R-bialgebra for which there exists an R-module morphism $S : H \longrightarrow H$, called the antipode, such that the following diagram commutes:



With the Sweedler notation, this diagram can be expressed by the equality

$$S(h_{(1)})h_{(2)} = \iota\big(\epsilon(h)\big) = h_{(1)}S\big(h_{(2)}\big).$$

Example 1.21. Let G be a group. By Example 1.14, we already know that the group algebra $R[G]$ is a cocommutative R-bialgebra. $R[G]$ is also a cocommutative R-Hopf algebra with antipode S defined by

$$S : R[G] \longrightarrow R[G] : \sigma \longmapsto \sigma^{-1} \quad \forall \sigma \in G.$$

We will now see that the antipode of an R-Hopf algebra can alternatively be seen as the inverse of an element in some ring.

Proposition 1.22. *Let A be an R-algebra and let C be an R-coalgebra. Then we can endow $Hom_R(C, A)$, the set of R-linear maps from C to A, with a ring structure with multiplication $*$ defined by*

$$(f * g)(x) = f(c_{(1)})g(c_{(2)}) \quad \forall f, g \in Hom_R(C, A), \forall c \in C.$$

The identity of $*$ is given by $\iota \circ \epsilon \in Hom_R(C, A)$.

Definition 1.23. The multiplication $*$ is called the *convolution product*.

Proposition 1.24. *Let H be an R-bialgebra, then H is an R-Hopf algebra with antipode S if and only if S is the inverse of the identity map $id_H \in Hom_R(H, H)$ with respect to the convolution product $*$, i.e. if and only if $S * id_H = \iota \circ \epsilon = id_H * S$.*

Corollary 1.25. *If H is an R-Hopf algebra, then the antipode is unique.*

Proposition 1.26. *Let H be an R-Hopf algebra, then*

(a) $S(hh') = S(h')S(h) \quad \forall h, h' \in H$,

(b) $S(1_H) = 1_H$,

(c) $\Delta\big(S(h)\big) = S(h_{(2)}) \otimes S(h_{(1)}) \quad \forall h \in H$,

(d) $\epsilon\big(S(h)\big) = \epsilon(h) \quad \forall h \in H$.

Definition 1.27. Let H and H' be two R-Hopf algebras and let $f : H \longrightarrow H'$ be an R-module morphism. Then f is a *Hopf algebra morphism* if f is a bialgebra morphism.

Proposition 1.28. *Let H, H' and f be defined as in the previous definition. Then $f \circ S_H = S_{H'} \circ f$.*

Definition 1.29. Let H be an R-Hopf algebra and let $I \subseteq H$ be an R-submodule. Then I is a *Hopf ideal* of H if I is a biideal and if $S(I) \subseteq I$.

Proposition 1.30. *Let H be an R-Hopf algebra and let $I \subseteq H$ be a Hopf ideal. Then there is a canonical Hopf algebra structure on H/I such that the natural projection $H \twoheadrightarrow H/I$ is a Hopf algebra morphism.*

Definition 1.31. Let H be an R-Hopf algebra and let $H_0 \subseteq H$ be an R-submodule. Then H_0 is a *Hopf subalgebra* of H if H_0 is both a subbialgebra of H and if $S(H_0) \subseteq H_0$. We say that H_0 is a *normal Hopf subalgebra* if $h_{(1)}h'S(h_{(2)}) \in H_0 \quad \forall h \in H, \forall h' \in H_0$.

Proposition 1.32. *Suppose H is flat over R. Let H and H' be two R-Hopf algebras and let $f : H \longrightarrow H'$ be a Hopf algebra morphism. Then $\mathrm{Ker}\, f$ is a Hopf ideal of H and $\mathrm{Im}\, f$ is a Hopf subalgebra of H'.*

We end this section with some properties that we will need later.

Definition 1.33. Let C be an R-coalgebra. An element $c \in C$ is called *grouplike* if $\Delta(c) = c \otimes c$ and if $\epsilon(c) = 1_R$.

Lemma 1.34. *Let K be a field and let C be a K-coalgebra.*

(a) The set of grouplike elements of C is K-linearly independent. Moreover, if $C = H$ is a K-Hopf algebra, then the set of grouplike elements of H forms a group.

(b) If C has a K-basis of grouplike elements, then any subcoalgebra and any quotient coalgebra of C also has a basis of grouplike elements.

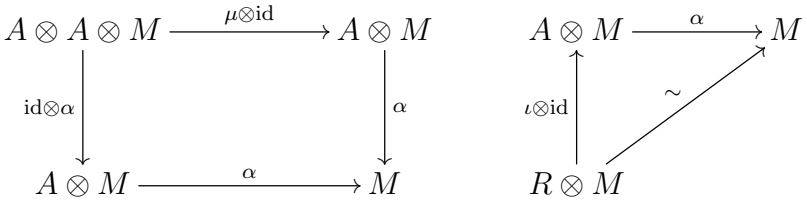
Lemma 1.35. *Let K be a field and let H be a K-Hopf algebra. Let I_1 and I_2 be two Hopf ideals of H, then $I_1 + I_2$ is also a Hopf ideal of H. The same result holds for (left and/or right) ideals and (left and/or right) coideals.*

Lemma 1.36. *Let K be a field and let H be a K-Hopf algebra. Let H_1 and H_2 be two Hopf subalgebras of H, then $H_1 \cap H_2$ is also a Hopf subalgebra of H. The same result holds for subalgebras, subcoalgebras, subbialgebras and normal Hopf subalgebras.*

1.1.2 Action and coaction

In the same spirit as for Definition 1.1, we will reformulate the classical definition of left (resp. right) modules over an R-algebra using diagrams. We will then define right (resp. left) comodules over an R-coalgebra whose structure is the dual of that of left (resp. right) modules.

Definition 1.37. Let A be an R-algebra. A *left A-module M* is an R-module together with an action $\alpha : A \otimes M \longrightarrow M$ such that α is an R-module morphism and such that the following diagrams commute:



We define a *right A-module* in a similar way.

If $A = H$ is an R-bialgebra and if the H-module $M = S$ is an R-algebra, we define a special case of H-modules for which the comultiplication (resp. counit) of H is compatible with the multiplication (resp. unit) of S.

Definition 1.38. Let S be an R-algebra and let H be an R-bialgebra. Then S is a *left H-module algebra* if

1. S is a left H-module (we will denote the action of $h \in H$ on $s \in S$ by $h \cdot s$),
2. $h \cdot (ss') = (h_{(1)} \cdot s)(h_{(2)} \cdot s') \quad \forall h \in H, \forall s, s' \in S$,
3. $h \cdot 1_S = \epsilon(h)1_S \quad \forall h \in H$.

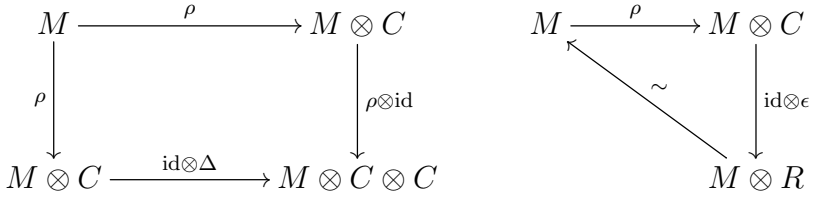
We define a *right H-module algebra* in a similar way.

Example 1.39. Let L/K be a Galois extension with Galois group $G = \mathrm{Gal}(L/K)$ and let $H = K[G]$, then L is a left $K[G]$-module algebra. Indeed, L is obviously a left $K[G]$-module. Moreover,

$$\sigma(xy) = \sigma(x)\sigma(y) \text{ and } \sigma(1) = 1 \quad \forall \sigma \in G, \forall x, y \in L.$$

We will now take the duals of the diagrams of Definition 1.37 and Definition 1.38 to obtain the following definitions.

Definition 1.40. Let C be an R-coalgebra. A *right C-comodule M* is an R-module together with a coaction $\rho : M \longrightarrow M \otimes C$ such that ρ is an R-module morphism and such that the following diagrams commute:



We define a *left C-comodule* in a similar way.

Example 1.41. Let C be an R-coalgebra. We can easily see that C is a left and right C-comodule with coaction given by Δ.

As for the comultiplication, we will use the Sweedler notation for the image of an element $m \in M$ by the coaction ρ:

$$\begin{aligned}\rho(m) &= m_{[0]} \otimes m_{[1]} \in M \otimes C \text{ for a right } C\text{-comodule,}\\ \rho(m) &= m_{[-1]} \otimes m_{[0]} \in C \otimes M \text{ for a left } C\text{-comodule.}\end{aligned}$$

The diagrams of Definition 1.40 (for a right C-comodule) can thus be expressed by the equalities

$$m_{[0][0]} \otimes m_{[0][1]} \otimes m_{[1]} = m_{[0]} \otimes m_{[1](1)} \otimes m_{[1](2)} \quad \forall m \in M$$

and

$$m = m_{[0]}\epsilon(m_{[1]}) \quad \forall m \in M.$$

Just like we did with H-modules, if $C = H$ is an R-bialgebra and if the H-comodule $M = S$ is an R-algebra, we define a special case for which the multiplication (resp. unit) of H is compatible with the multiplication (resp. unit) of S.

Definition 1.42. Let S be an R-algebra and let H be an R-bialgebra. Then S is a *right H-comodule algebra* if

1. S is a right H-comodule,
2. $(ss')_{[0]} \otimes (ss')_{[1]} = s_{[0]}s'_{[1]} \otimes s_{[0]}s'_{[1]} \quad \forall s, s' \in S$,
3. $\rho(1_S) = 1_S \otimes 1_H$.

We define a *left H-comodule algebra* in a similar way.

1.1.3 Duality

Let H be an R-Hopf algebra and let $H^* := \mathrm{Hom}_R(H, R)$ be its dual. The dual of the multiplication and the dual of the comultiplication are respectively

$$\mu^* : H^* \longrightarrow (H \otimes H)^* \text{ and } \Delta^* : (H \otimes H)^* \longrightarrow H^*.$$

As we can see, μ^* and Δ^* do not give a comultiplication and a multiplication on H^*. To properly define a structure of Hopf algebra on H^*, we need the R-module morphism

$$\varphi : M^* \otimes M^* \longrightarrow (M \otimes M)^* : f \otimes f' \longmapsto \big(m \otimes m' \mapsto f(m)f'(m')\big) \tag{1.1}$$

where M is any R-module. Note that, in general, φ is not bijective. However, there are cases where φ is bijective, for example if M is a finitely generated projective R-module. Also note that we have a natural R-module isomorphism

$$R \xrightarrow{\cong} R^* : a \longmapsto \big(b \mapsto ab\big).$$

Proposition 1.43. *Let C be an R-coalgebra, then its dual C^* can be endowed with a structure of R-algebra:*

1. *the multiplication map is given by $\Delta^* \circ \varphi : C^* \otimes C^* \longrightarrow (C \otimes C)^* \longrightarrow C^*$ where φ is defined as in (1.1),*
2. *the unit map is given by $\epsilon^* : R \xrightarrow{\cong} R^* \longrightarrow C^*$.*

Remark 1.44. The algebra C^* is commutative if and only if the coalgebra C is cocommutative.

Let A be an R-algebra. Its dual A^* is not, in general, an R-coalgebra because the dual of the multiplication $\mu^* : A^* \longrightarrow (A \otimes A)^*$ cannot be made into a comultiplication. However, if A is finitely generated and projective as an R-module, then the map φ is a bijection. We can thus define a comultiplication on A^*.

Proposition 1.45. *Let A be an R-algebra that is finitely generated and projective as an R-module, then its dual A^* can be endowed with a structure of R-coalgebra:*

1. *the comultiplication map is given by $\varphi^{-1} \circ \mu^* : A^* \longrightarrow (A \otimes A)^* \longrightarrow A^* \otimes A^*$ where φ is defined as in (1.1),*
2. *the counit map is given by $\iota^* : A^* \longrightarrow R^* \xrightarrow{\cong} R$.*

Remark 1.46. If A is an R-algebra that is finitely generated and projective as an R-module, then its double dual A^{**} is naturally isomorphic to A. By Remark 1.44, the coalgebra A^* is cocommutative if and only if the algebra A is commutative.

Proposition 1.47. *Let H be an R-Hopf algebra that is finitely generated and projective as an R-module., then its dual H^* is also an R-Hopf algebra that is finitely generated and projective as an R-module. Moreover, its double dual H^{**} is naturally isomorphic to H as R-Hopf algebras.*

We will now look at the dual of C-comodules, H-comodule algebras, A-modules and H-module algebras.

Proposition 1.48. *Let C be an R-coalgebra and let M be a right C-comodule with coaction $\rho : M \longrightarrow M \otimes C$. Then M becomes a left C^*-module with action*

$$\begin{array}{c} C^* \otimes M \xrightarrow{id\otimes\rho} C^* \otimes M \otimes C \xrightarrow{\sigma\otimes id} M \otimes C^* \otimes C \longrightarrow M \otimes R \xrightarrow{\cong} M : \\ f \otimes m \longmapsto m_{[0]} f(m_{[1]}) \end{array}$$

where σ is the switch map defined in Definition 1.3. Moreover, if $C = H$ is also an R-bialgebra and if $M = S$ is also a right H-comodule algebra, then this action endows S with a structure of left H^*-module algebra.

Proposition 1.49. *Let A be an R-algebra that is finitely generated and projective as an R-module and let M be a left A-module. Then M can be endowed with a structure of right A^*-comodule. Let $\{(f_i, a_i)\}_{i=1}^n \subseteq A^* \times A$ be a projective coordinate system, so that for every $a \in A$ we have $a = \sum_{i=1}^n f_i(a)a_i$. Then M becomes a right A^*-comodule with coaction*

$$\rho : M \longrightarrow M \otimes A^* : m \longmapsto \sum_{i=1}^{n} (a_i \cdot m) \otimes f_i. \tag{1.2}$$

Moreover, if $A = H$ is also an R-bialgebra and if $M = S$ is also a left H-module algebra, then this coaction endows S with a structure of right H^*-comodule algebra.

We end this subsection with the definition of an alternative dual for an arbitrary K-algebra when $R = K$ is a field. This definition is due to Sweedler [Swe69].

Definition 1.50. Let A be a K-algebra. We say that an ideal $I \subseteq A$ is *cofinite* if A/I is finite dimensional. The *Sweedler dual* of a K-algebra A is

$$A^\circ = \{ f \in A^* \mid \operatorname{Ker} f \text{ contains a cofinite ideal} \}.$$

Remark 1.51. The inclusion $A^\circ \subseteq A^*$ is an equality if A is finite dimensional.

Lemma 1.52. *Let A_1 and A_2 be two K-algebras, then $A_1^\circ \otimes A_2^\circ = (A_1 \otimes A_2)^\circ$. Moreover, if $f : A_1 \longrightarrow A_2$ is a morphism of K-algebras, then $f^*(A_2^\circ) \subseteq A_1^\circ$.*

Proposition 1.53. *Let A be a K-algebra, then A° can be endowed with a structure of K-coalgebra:*

1. *the comultiplication map is given by $\mu^*|_{A^\circ} : A^\circ \longrightarrow (A \otimes A)^\circ = A^\circ \otimes A^\circ$,*

2. the counit map is given by $\iota^*|_{A^\circ} : A^\circ \longrightarrow K^\circ = K^* \xrightarrow{\cong} K$.

Moreover, if $A = H$ *is a* K*-bialgebra (resp.* K*-Hopf algebra), then* H° *is also a* K*-bialgebra (resp.* K*-Hopf algebra).*

1.1.4 Limits and colimits

Let K be a field. It is well-known that the category Alg_K of K-algebras is complete and cocomplete, meaning that all categorical limits (such as products, equalizers, pullbacks and inverse (or projective) limits) and all categorical colimits (such as coproducts, coequalizers, pushouts and inductive (or direct) limits) exist in Alg_K. Since the forgetful functor $\mathsf{Alg}_K \to \mathsf{Set}$ preserves and creates limits, all limits can be computed in set-theoretical terms, and be endowed with a suitable K-algebra structure. Colimits, on the other hand, are more complicated to describe (the construction of coproducts, for example is similar the construction of *free products* of groups). However, when we restrict to the category of commutative algebras, then the situation becomes easier. Indeed, the categorical coproduct of two K-algebras A and B is just the K-tensor product $A \otimes B$. More generally, the categorical pushout of morphisms of commutative algebras $f : E \to A$ and $g : E \to B$ is given by the balanced tensor product $A \otimes_E B$.

The situation for coalgebras is maybe less known, although it is -as one could expect- exactly dual to the situation of algebras. Indeed, any category of coalgebras Coalg_K has all colimits which can be computed in the underlying category of sets. At least in the case when K is a field (or even more generally, when K is a regular commutative ring, see e.g. [Por08] and [Ago11]) the category Coalg_K also has all limits. In case we restrict to the cocommutative coalgebras, then the categorical product of two coalgebras C and D can be computed as the tensor product $C \otimes D$, which becomes a coalgebra by the following comultiplication

$$\Delta : C \otimes D \to C \otimes D \otimes C \otimes D,\ \Delta(c \otimes d) = c_{(1)} \otimes d_{(1)} \otimes c_{(2)} \otimes d_{(2)}$$

and counit

$$\epsilon : C \otimes D \to K,\ \epsilon(c \otimes d) = \epsilon_C(c)\epsilon_D(d).$$

In this case, the natural projections $\pi_C : C \otimes D \to C$ and $\pi_D : C \otimes D \to D$ are given by

$$\pi_C(c \otimes d) = c\epsilon_D(d) \ \text{ and } \ \pi_D(c \otimes d) = \epsilon_C(c)d,$$

for all $c \otimes d \in C \otimes D$. The pullback of two morphisms of cocommutative coalgebras $p_1 : C \to E$ and $p_2 : D \to E$, is given by the following subset of the product

$$C \otimes^E D := \{c \otimes d \in C \otimes D \mid c_{(1)} \otimes p_1(c_{(2)}) \otimes d = c \otimes p_2(d_{(1)}) \otimes d_{(2)} \in C \otimes E \otimes D\}.$$

Also the category of Hopf algebras Hopf_K is complete and cocomplete (see e.g. [Por11] and [Ago11]). In fact, limits in Hopf_K can be computed in the same way as limits in the category of coalgebras; colimits in Hopf_K can be computed on the underlying algebras. In view of the above however, limits nor colimits of Hopf algebras can in general be computed on their underlying sets. When we consider commutative (respectively cocommutative) Hopf algebras, then coproducts and pushouts (respectively, products and pullbacks) have the same simplified description as in the underlying category of commutative algebras (respectively cocommutative coalgebras), as given above.

1.2 Invariants and coinvariants

In this section, we will state an important correspondence between ideals and subalgebras of a Hopf algebra.

Throughout this section, K will be a field and H will be a K-Hopf algebra. Unadorned tensors are assumed to be taken over K unless specified otherwise.

Definition 1.54. Let L be a left H-module and let $F \subseteq H$ be a subset. We define the set of *left F-invariants* of L by

$$L^F = \big\{x \in L \,|\, h \cdot x = \epsilon(h)x \quad \forall h \in F\big\}.$$

If L is a right H-module, we define the set of *right F-invariants* in a similar way.

Definition 1.55. Let L be a right H-comodule, let V be a K-vector space and let $f : H \longrightarrow V$ be a morphism of K-vector spaces. We define the set of *right V-coinvariants* of L by

$$L^{\mathrm{co}\,V} = \big\{x \in L \,|\, x_{[0]} \otimes f(x_{[1]}) = x \otimes f(1_H)\big\}.$$

If L is a left H-module, we define the set of *left V-coinvariants* in a similar way but it will be noted ${}^{\mathrm{co}\,V}L$.

Definition 1.56. Let H be a K-Hopf algebra. We define the pair of maps

$$\big\{I \subseteq H \text{ left ideal two-sided coideal}\big\} \underset{\psi}{\overset{\varphi}{\rightleftarrows}} \big\{A \subseteq H \text{ right coideal subalgebra}\big\}$$

in the following way:

1. let $I \subseteq H$ be a left ideal two-sided coideal and let $\pi : H \twoheadrightarrow H/I$ be the natural projection, then $\varphi(I)$ is the set of left H/I-coinvariants of H:

$$\varphi(I) = {}^{\mathrm{co}\,H/I}H := \big\{h \in H \,|\, \pi(h_{(1)}) \otimes h_{(2)} = \pi(1_H) \otimes h\big\};$$

2. let $A \subseteq H$ be a right coideal subalgebra, then $\psi(A)$ is the left H-module generated by $A^+ := \big\{a \in A \,|\, \epsilon(a) = 0\big\}$:

$$\psi(A) = HA^+.$$

In general, the maps φ and ψ are not inverse bijections but they satisfy the following property:

$$A \subseteq \varphi(I) \iff I \subseteq \psi(A).$$

In some particular cases, φ and ψ are known to be inverse bijections.

Theorem 1.57. *([New75], [Sch90, Thm. 4.15]) Let H be a cocommutative K-Hopf algebra, then the pair of maps*

$$\big\{I \subseteq H \text{ left ideal two-sided coideal}\big\} \underset{\psi}{\overset{\varphi}{\rightleftarrows}} \big\{A \subseteq H \text{ Hopf subalgebra}\big\},$$

where φ and ψ are defined as in Definition 1.56, are inverse bijections.

Theorem 1.58. *([Mon93, Thm. 3.4.6]) The bijective correspondence from Theorem 1.57 can be restricted to a bijective correspondence between the Hopf ideals and the normal Hopf subalgebras of a cocommutative K-Hopf algebra H:*

$$\big\{I \subseteq H \text{ Hopf ideal}\big\} \underset{\psi}{\overset{\varphi}{\rightleftarrows}} \big\{A \subseteq H \text{ normal Hopf subalgebra}\big\}.$$

1.3 Hopf-Galois extensions

Let L/K be a finite separable field extension and let $G = \mathrm{Aut}(L/K)$. From the linear independence of characters, the morphism of K-vector spaces defined by

$$\underline{\mathrm{can}} : L[G] \longrightarrow \mathrm{End}_K(L) : x\sigma \longmapsto \big(y \mapsto x\sigma(y)\big) \tag{1.3}$$

from the group algebra $K[G]$ to the ring of K-linear endomorphisms $\mathrm{End}_K(L)$ is injective. Furthermore, $\underline{\mathrm{can}}$ is bijective if and only if $L[G]$ and $\mathrm{End}_K(L)$ have the same dimension as L-vector spaces, i.e. if and only if $\#G = [L : K]$. We thus have the following result.

Proposition 1.59. *Let L/K be a finite separable field extension and let $\underline{can}$ be the map defined in (1.3). Then $\underline{can}$ is bijective if and only if L/K is Galois.*

We can thereby substitute the normality of the finite separable field extension L/K in Galois theory by the bijectivity of $\underline{can}$. Chase and Sweedler [CS69] used this result to extend Galois theory to commutative rings with action given by a Hopf algebra.

Definition 1.60. Let R be a commutative ring with unity, let S be a commutative R-algebra that is finitely generated and projective as an R-module and let H be an R-Hopf algebra. Then S/R is a *Hopf-Galois extension with Hopf algebra H*, or simply *H-Galois*, if S is a left H-module algebra and if the map

$$\underline{can} : S \otimes H \longrightarrow \mathrm{End}_R(S) : s \otimes h \longmapsto \big(t \mapsto s(h \cdot t)\big) \tag{1.4}$$

is an isomorphism of R-modules.

Remark 1.61. Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. Taking $R = K$, $S = L$ and $H = K[G]$ in the previous definition recovers Proposition 1.59. Therefore, every finite Galois extension of fields L/K is $K[G]$-Galois.

In [GP87], Greither and Pareigis showed an example of a finite non-Galois extension that is Hopf-Galois.

Example 1.62. Let $K = \mathbb{Q}$, $\omega = \sqrt[3]{2}$ and $L = \mathbb{Q}(\omega)$. Let us define the following linear maps $c, s : L \to L$ by

$$\begin{array}{lll} c(1) = 1, & c(\omega) = \frac{-1}{2}\omega, & c(\omega^2) = \frac{-1}{2}\omega^2, \\ s(1) = 0, & s(\omega) = \frac{1}{2}\omega, & s(\omega^2) = \frac{-1}{2}\omega^2. \end{array}$$

Straightforward calculations show that, for all $x, y \in \mathbb{Q}(\omega)$, we have

$$c(xy) = c(x)c(y) - 3s(x)s(y) \text{ and } s(xy) = c(x)s(y) + s(x)c(y).$$

Let $H = \mathbb{Q}[c,s]/\big(3s^2 + c^2 - 1, (2c+1)s, (2c+1)(c-1)\big)$, $\Delta(c) = c \otimes c - 3s \otimes s$, $\Delta(s) = c \otimes s + s \otimes c$, $\epsilon(c) = 1$ and $\epsilon(s) = 0$, then L/K is a finite H-Galois extension.

It is possible to make the isomorphism of R-modules $\underline{can}$ into an isomorphism of R-algebras if we define a suitable multiplication on $S \otimes H$.

Definition 1.63. Let S be a left H-module algebra. We define the *smash product* $S\#H$ to be the R-algebra which as R-module is $S \otimes H$ (we will write $s\#h \in S\#H$ for the element corresponding to $s \otimes h \in S \otimes H$) and with multiplication defined by

$$(s\#h)(s'\#h') = s(h_{(1)} \cdot s')\#h_{(2)}h' \quad \forall s, s' \in S, \forall h, h' \in H$$

and with unit $1_S\#1_H$.

Corollary 1.64. *Let S/R be an H-Galois extension, then $\underline{can} : S\#H \longrightarrow End_R(S)$ is an isomorphism of R-algebras.*

Proof. Let $s, s', t \in S$ and $h, h' \in H$, then

$$\begin{aligned}\underline{\mathrm{can}}\big((s\#h)(s'\#h')\big)(t) &= \underline{\mathrm{can}}\big(s(h_{(1)}\cdot s')\#h_{(2)}h'\big)(t) = s(h_{(1)}\cdot s')(h_{(2)}h'\cdot t)\\ &= s\Big(h\cdot\big(s'(h'\cdot t)\big)\Big) = \underline{\mathrm{can}}(s\#h)\underline{\mathrm{can}}(s'\#h')(t)\end{aligned}$$

and

$$\underline{\mathrm{can}}(1_S\#1_H)(t) = 1_S(1_H\cdot t) = t.$$

□

We end this section with some useful results on H-Galois extensions.

Proposition 1.65. *Let S/R be an H-Galois extension, then $S^H = R$.*

Proof. For all $h \in H$ and for all $s \in R$, we have $h \cdot s = \epsilon(h)s$. Thus, $R \subseteq S^H$. Conversely, let $s \in S^H$, then for all $t \in S$ and for all $h \in H$ we have

$$(t\#h)(s\#1_H) = \big(t(h_{(1)}\cdot s)\big)\#h_{(2)} = \big(t\epsilon(h_{(1)})s\big)\#h_{(2)} = st\#h = (s\#1_H)(t\#h).$$

Therefore, $\underline{\mathrm{can}}(s\#1_H)$ commutes with $\underline{\mathrm{can}}(t\#h)$ for all $t \in S$ and for all $h \in H$. By the bijectivity of $\underline{\mathrm{can}}$, we can conclude that $\underline{\mathrm{can}}(s\#1_H)$ is in the center of $\mathrm{End}_R(S)$, which is R. So, $s \in R$. □

Proposition 1.66. *[Chi89, Prop. 2.9] Let K be a field and let H be a K-bialgebra. Suppose that L/K is a finite field extension such that L is a left H-module algebra and define $\underline{can} : L \otimes H \longrightarrow End_K(L)$ as in (1.4). Let $\rho : L \longrightarrow L \otimes H^* : x \longmapsto x_{[0]} \otimes x_{[1]}$ be the right coaction as defined in (1.2) and define*

$$j : L \otimes L \longrightarrow L \otimes H^* : x \otimes y \longmapsto xy_{[0]} \otimes y_{[1]}.$$

Then $\underline{can}$ is bijective if and only if j is bijective.

Proposition 1.67. *[Sch97] Let L/K be a finite field extension and let H be a K-bialgebra. Suppose L is a left H-module algebra such that $\underline{can} : L \otimes H \longrightarrow End_K(L)$, as defined in (1.4), is bijective. Then H is a K-Hopf algebra.*

Proposition 1.68. *Let H be a K-Hopf algebra and let L/K be a finite field extension that is H-Galois. Then H is cocommutative.*

Proof. Using the fact that L/K is H-Galois in the first and third isomorphism, the fact that L/K is finite in the second isomorphism and the Hom-tensor relations in the last isomorphism, we obtain a natural isomorphism

$$\begin{aligned} L \otimes H \otimes H &\cong \mathrm{Hom}_K(L, L) \otimes H \cong \mathrm{Hom}_K(L, L \otimes H) \\ &\cong \mathrm{Hom}_K\big(L, \mathrm{Hom}_K(L, L)\big) \cong \mathrm{Hom}_K(L \otimes L, L). \end{aligned}$$

The composed isomorphism $\alpha : L \otimes H \otimes H \longrightarrow \mathrm{Hom}_K(L \otimes L, L)$ is given explicitly by $\alpha(x \otimes h \otimes h')(y \otimes z) = x(h \cdot y)(h' \cdot z)$.
By the commutativity of L, it is clear that for all $x, y, z \in L$ and for all $h \in H$,

$$\begin{aligned} x(h_{(1)} \cdot y)((h_{(2)} \cdot z) &= xh \cdot (yz) = xh \cdot (zy) \\ &= x(h_{(1)} \cdot z)((h_{(2)} \cdot y) = x(h_{(2)} \cdot y)((h_{(1)} \cdot z). \end{aligned}$$

This means that $\alpha(x \otimes h_{(1)} \otimes h_{(2)}) = \alpha(x \otimes h_{(2)} \otimes h_{(1)})$ and since α is an isomorphism we also have that $x \otimes h_{(1)} \otimes h_{(2)} = x \otimes h_{(2)} \otimes h_{(1)}$. Since K is a field, it follows that $h_{(1)} \otimes h_{(2)} = h_{(2)} \otimes h_{(1)}$, hence H is cocommutative. □

1.4 Hopf-Galois descent

Let L/K be a field extension, we can consider the extension-of-scalars functor

$$L \otimes - : \mathsf{Vect}_K \longrightarrow \mathsf{Vect}_L : V \longmapsto L \otimes V$$

from the category of K-vector spaces to the category of L-vector spaces. The action of L on $L \otimes V$ is given by

$$x(y \otimes v) = xy \otimes v \quad \forall x, y \in L, \forall v \in V.$$

Let H be a K-Hopf algebra and suppose that L is a left H-module algebra. Consider the K-algebra $L\#H$. Then a left $L\#H$-module M is an L-vector space which is also a left H-module and such that the actions of L and H on M satisfy the following compatibility condition:

$$h \cdot (xm) = (h_{(1)} \cdot x)(h_{(2)} \cdot m) \quad \forall h \in H, \forall x \in L, \forall m \in M. \tag{1.5}$$

Lemma 1.69. *Let L/K be a field extension, let V be a K-vector space and let H be a K-Hopf algebra. Suppose that L is a left H-module algebra. Define the action of H on $L \otimes V$ by*

$$h \cdot (y \otimes v) = (h \cdot y) \otimes v \quad \forall h \in H, \forall y \in L, \forall v \in V.$$

Then $L \otimes V$ is a left $L\#H$-module.

Proof. Let $h \in H$, $x, y \in L$ and $v \in V$, then

$$\begin{aligned} h \cdot \big(x(y \otimes v)\big) &= h \cdot (xy \otimes v) = (h \cdot xy) \otimes v = (h_{(1)} \cdot x)(h_{(2)} \cdot y) \otimes v \\ &= (h_{(1)} \cdot x)\big((h_{(2)} \cdot y) \otimes v\big) = (h_{(1)} \cdot x)\big(h_{(2)} \cdot (y \otimes v)\big). \end{aligned}$$

Hence (1.5) is satisfied. □

Therefore, the extension-of-scalars functor can be written as

$$L \otimes - : \mathsf{Vect}_K \longrightarrow {}_{L\#H}\mathsf{Mod} : V \longmapsto L \otimes V$$

from the category of K-vector spaces to the category of left $L\#H$-modules.

Suppose now that M is a left $L\#H$-module, is it possible to find a K-vector space V such that $L \otimes V \cong M$ as $L\#H$-modules? The following proposition answers this question in the case where L/K is a finite dimensional H-Galois extension.

Proposition 1.70. *[CS69, Thm. 9.6] Let L/K be a field extension and let H be a finite dimensional K-Hopf algebra. Suppose that L is a left H-module algebra. Then L/K is an H-Galois extension if and only if the pair of functors*

$$L \otimes - : \mathsf{Vect}_K \rightleftarrows {}_{L\#H}\mathsf{Mod} : (-)^H$$

defines an equivalence of categories.

In fact, the above equivalence of categories has a richer structure. The category ${}_{L\#H}\mathsf{Mod}$ is monoidal by means of the tensor product over L. Indeed, let M and N be two left $L\#H$-modules, then we can define the following action of H on the tensor product $M \otimes_L N$:

$$h \cdot (m \otimes n) = (h_{(1)} \cdot m) \otimes (h_{(2)} \cdot n) \quad \forall h \in H, \forall m \in M, \forall n \in N.$$

This action is well-defined because for any $x \in L$ we have

$$\begin{aligned} h \cdot (xm \otimes n) &= \big(h_{(1)} \cdot (xm)\big) \otimes (h_{(2)} \cdot n) = (h_{(1)} \cdot x)(h_{(2)} \cdot m) \otimes (h_{(3)} \cdot n) \\ &= (h_{(2)} \cdot m) \otimes (h_{(1)} \cdot x)(h_{(3)} \cdot n) = (h_{(1)} \cdot m) \otimes (h_{(2)} \cdot x)(h_{(3)} \cdot n) \\ &= (h_{(1)} \cdot m) \otimes (h_{(2)} \cdot xn) = h \cdot (m \otimes xn) \end{aligned}$$

where we used the cocommutativity of H (Proposition 1.68) in the 4^{th} equality. A similar computation shows that the actions of L and H on $M \otimes_L N$ satisfy the compatibility condition (1.5). With this monoidal structure, the extension-of-scalars functor

$L \otimes - : \mathsf{Vect}_K \longrightarrow {}_{L\#H}\mathsf{Mod}$ is a strict monoidal functor (with the usual tensor product in Vect_K). Indeed, let V and W be two K-vector spaces, then there is an isomorphism of L-vector spaces

$$\alpha : L \otimes (V \otimes W) \xrightarrow{\cong} (L \otimes V) \otimes_L (L \otimes W) : x \otimes (v \otimes w) \longmapsto (x \otimes v) \otimes (1 \otimes w).$$

It is an isomorphism of H-modules because

$$\alpha\Big(h \cdot \big(x \otimes (v \otimes w)\big)\Big) = \alpha\big((h \cdot x) \otimes (v \otimes w)\big) = \big((h \cdot x) \otimes v\big) \otimes (1 \otimes w)$$

and

$$\begin{aligned} &h \cdot \alpha\big(x \otimes (v \otimes w)\big) = h \cdot \big((x \otimes v) \otimes (1 \otimes w)\big) = \big(h_{(1)} \cdot (x \otimes v)\big) \otimes \big(h_{(2)} \cdot (1 \otimes w)\big) \\ &= \big((h_{(1)} \cdot x) \otimes v\big) \otimes \big((h_{(2)} \cdot 1) \otimes w\big) = \big((h_{(1)} \cdot x) \otimes v\big) \otimes \big(\epsilon(h_{(2)})1 \otimes w\big) \\ &= \big(\epsilon(h_{(2)})(h_{(1)} \cdot x) \otimes v\big) \otimes (1 \otimes w) = \big((h \cdot x) \otimes v\big) \otimes (1 \otimes w). \end{aligned}$$

We can therefore conclude the following proposition.

Proposition 1.71. *Let L/K be a finite dimensional H-Galois extension, then the equivalence of categories given in Proposition 1.70 is a monoidal equivalence.*

Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$ and let M be a left $L\#K[G]$-module. Then the set of left $K[G]$-invariants of M is

$$\begin{aligned} M^{K[G]} &:= \big\{m \in M \,|\, h \cdot m = \epsilon(h)m \quad \forall h \in K[G]\big\} \\ &= \big\{m \in M \,|\, \sigma(m) = m \quad \forall \sigma \in G\big\}. \end{aligned}$$

We can thus reformulate the equivalence of monoidal categories in the following way.

Definition 1.72. Let G be a group and let M be a left G-module. We define the set of left *G-invariants* of M by

$$M^G = \big\{m \in M \,|\, \sigma(m) = m \quad \forall \sigma \in G\big\}.$$

Corollary 1.73. *Let L/K be a finite Galois extension with Galois group $G = Gal(L/K)$, then the pair of functors*

$$L \otimes - : \mathsf{Vect}_K \rightleftarrows {}_{L\#K[G]}\mathsf{Mod} : (-)^G$$

defines an equivalence of monoidal categories.

2

Finite Hopf-Galois theory for separable field extensions

2.1 Introduction

Let L/K be a finite field extension. We start by recalling the Fundamental Theorem of Galois Theory.

Theorem 2.1. *(Fundamental Theorem of Galois Theory) Let L/K be a finite Galois extension with Galois group $Gal(L/K) = G$, then the maps*

$$\{G_0 \subseteq G \text{ subgroup}\} \underset{ann}{\overset{fix}{\rightleftarrows}} \{L/L_0/K \text{ intermediate field}\}$$

defined by

$$fix(G_0) = \{x \in L \mid \sigma(x) = x \quad \forall \sigma \in G_0\} =: L^{G_0}$$

and

$$ann(L_0) = \{\sigma \in G \mid \sigma(x) = x \quad \forall x \in L_0\} = Gal(L/L_0)$$

are inverse bijections and inclusion reversing. Moreover, L_0/K is Galois if and only if $Gal(L/L_0)$ is a normal subgroup of G.

It is natural to ask whether it is possible to generalize Theorem 2.1 to Hopf-Galois extensions. The following proposition, due to Chase and Sweedler [CS69], gives a beginning of an answer.

Proposition 2.2. *Let L/K be a finite H-Galois extension. For a Hopf subalgebra $H_0 \subseteq H$ we define*

$$Fix(H_0) = \{x \in L \mid h \cdot x = \epsilon(h)x \quad \forall h \in H_0\} =: L^{H_0}.$$

Then the map

$$\big\{H_0 \subseteq H \ \textit{Hopf subalgebra}\big\} \longrightarrow \big\{L/L_0/K \ \textit{intermediate field}\big\}$$

is injective and inclusion-reversing.

If L/K is a finite Galois extension with Galois group $Gal(L/K) = G$, then it is also H-Galois with $H = K[G]$. Recall that, in this case, every Hopf subalgebra $H_0 \subseteq H$ is of the form $K[G_0]$ for some subgroup $G_0 \subseteq G$ (see Lemma 1.34). Conversely, $K[G_0]$ is a Hopf subalgebra for every subgroup $G_0 \subseteq G$. In this context, the maps fix defined in Theorem 2.1 and Fix defined in Proposition 2.2 coincide: for every subgroup $G_0 \subseteq G$ we have

$$\begin{aligned}
\mathrm{Fix}\big(K[G_0]\big) &= \big\{x \in L \,|\, h \cdot x = \epsilon(h)x \quad \forall h \in K[G_0]\big\} \\
&= \big\{x \in L \,|\, \sigma \cdot x = \epsilon(\sigma)x \quad \forall \sigma \in G_0\big\} \\
&= \big\{x \in L \,|\, \sigma(x) = x \quad \forall \sigma \in G_0\big\} = \mathrm{fix}(G_0).
\end{aligned}$$

The map Fix is therefore bijective.

A major difference between Galois theory and Hopf-Galois theory is that Fix may not be bijective.

In this chapter, we will give a characterization of the intermediate fields of the form $\mathrm{Fix}(H_0)$ for some Hopf subalgebra $H_0 \subseteq H$. We will also characterize the intermediate fields of the form $\mathrm{Fix}(I)$ for some Hopf ideal $I \subseteq H$. We will then state and prove the Fundamental Theorem of Hopf-Galois Theory (Theorem 2.31) which is the generalization of Theorem 2.1 for Hopf-Galois extensions.

Throughout this chapter, L/K will be a finite separable H-Galois extension. Unadorned tensors are assumed to be taken over K unless specified otherwise.

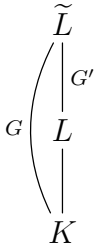
2.2 The Greither-Pareigis group

In this section, we introduce an important group associated to a finite separable H-Galois extension L/K. This group, due to Greither and Pareigis [GP87], will allow us to work with Hopf-Galois extensions using classical Galois theory.

Throughout this section, we will adopt the following notations:

1. L/K is a finite separable H-Galois extension;
2. $\widetilde{L}/K$ is a finite Galois extension containing L/K;
3. $G = \mathrm{Gal}(\widetilde{L}/K)$, $G' = \mathrm{Gal}(\widetilde{L}/L)$;
4. $X = G/G'$ is the set of G'-cosets of G (elements of X are of the form $\sigma G'$ with $\sigma \in G$).

The field extensions and Galois groups are summarized in the following diagram:



Definition 2.3. We define the *left translation map* by the action of G on X:

$$\lambda : G \longrightarrow \mathrm{Perm}(X) : \sigma \longmapsto \left(\tau G' \mapsto \sigma\tau G'\right)$$

where $\mathrm{Perm}(X)$ is the group of permutations of X.

Definition 2.4. Let A be a set. A subgroup $N \subseteq \mathrm{Perm}(A)$ is called *regular* if, for every $a, b \in A$, there exists a unique $\nu \in N$ such that $\nu(a) = b$.

Remark 2.5. If A is a finite set, then $N \subseteq \mathrm{Perm}(A)$ is regular if and only if N is transitive and $\#N = \#A$.

Theorem 2.6. *[GP87, Thm. 2.1] Let L/K be a finite separable field extension. Then there is a correspondence between the Hopf-Galois structures on L/K and the subgroups $N \subseteq Perm(X)$ that are regular and normalized by $\lambda(G)$.*

To better understand this theorem, we need the following results. Complete proofs of these results can be found in [Chi89].

Let $X\widetilde{L} = Map(X, \widetilde{L})$ be the set of maps from X to $\widetilde{L}$. For every $\sigma G' \in X$, we define the map

$$u_{\sigma G'} : X \longrightarrow \widetilde{L} : \tau G' \longmapsto \begin{cases} 1 & \text{if } \sigma G' = \tau G', \\ 0 & \text{if } \sigma G' \neq \tau G'. \end{cases} \tag{2.1}$$

Then, $X\widetilde{L}$ is generated as an $\widetilde{L}$-vector space by the set $\{u_{\sigma G'} \,|\, \sigma G' \in X\}$. Moreover, $X\widetilde{L}$ is an $\widetilde{L}$-algebra whose multiplication is

$$X\widetilde{L} \otimes X\widetilde{L} \longrightarrow X\widetilde{L} : u_{\sigma G'} \otimes u_{\tau G'} \longmapsto \begin{cases} u_{\sigma G'} & \text{if } \sigma G' = \tau G', \\ 0 & \text{if } \sigma G' \neq \tau G', \end{cases}$$

and whose unit element is

$$1_{X\widetilde{L}} = \sum_{\sigma G' \in X} u_{\sigma G'}.$$

If we define an action of G on $X\widetilde{L}$ by

$$\sigma(x.u_{\tau G'}) = \sigma(x).u_{\sigma\tau G'} \quad \forall \sigma \in G, \forall x \in \widetilde{L}, \forall \tau G' \in X, \tag{2.2}$$

then $X\widetilde{L}$ becomes a G-module.

The following lemma shows how, from an H-Galois extension L/K, we obtain a subgroup $N \subseteq \mathrm{Perm}(X)$.

Lemma 2.7. *(a) The map*

$$\beta_L : \widetilde{L} \otimes L \xrightarrow{\cong} X\widetilde{L} : x \otimes y \longmapsto \sum_{\sigma G' \in X} x\sigma(y).u_{\sigma G'} \tag{2.3}$$

is an isomorphism of $\widetilde{L}$-algebras and G-modules where G acts on $\widetilde{L} \otimes L$ via the left factor.

(b) There is an isomorphism of $\widetilde{L}$-Hopf algebras

$$\beta_H : \widetilde{L} \otimes H \xrightarrow{\cong} \widetilde{L}[N] \tag{2.4}$$

where N is a group of order $[L : K]$.

(c) Define the action $\widetilde{\alpha} : \widetilde{L}[N] \underset{\widetilde{L}}{\otimes} X\widetilde{L} \to X\widetilde{L}$ by the diagram

$$\begin{array}{ccccc} \widetilde{L}[N] \underset{\widetilde{L}}{\otimes} X\widetilde{L} & & \xrightarrow{\quad\quad\widetilde{\alpha}\quad\quad} & & X\widetilde{L} \\ {\scriptstyle \beta_H \underset{\widetilde{L}}{\otimes} \beta_L} \uparrow \cong & & & & \uparrow {\scriptstyle \beta_L} \cong \\ (\widetilde{L} \otimes H) \underset{\widetilde{L}}{\otimes} (\widetilde{L} \otimes L) & \xrightarrow{\cong} & \widetilde{L} \otimes (H \otimes L) & \xrightarrow{id \otimes \alpha} & \widetilde{L} \otimes L \end{array}$$

Then, the extension $X\widetilde{L}/\widetilde{L}$ is $\widetilde{L}[N]$-Galois and the action $\widetilde{\alpha}$ identifies N as a subgroup of Perm(X) which is regular and normalized by $\lambda(G)$.

Proof. See [GP87] Lemma 1.2, Proposition 1.3 and Theorem 3.1. □

Remark 2.8. If $N \subseteq \mathrm{Perm}(X)$ is normalized by $\lambda(G)$, then $\widetilde{L}[N]$ becomes a G-module with action given by

$$G \times \widetilde{L}[N] \longrightarrow \widetilde{L}[N] : (\sigma, x.\nu) \longmapsto \sigma(x.\nu) = \sigma(x).\big(\lambda(\sigma)\nu\lambda(\sigma^{-1})\big) \tag{2.5}$$

for all $\sigma \in G$, $x \in \widetilde{L}$ and $\nu \in N$. With this action, β_H becomes a morphism of G-modules.

Conversely, let N be any subgroup of $\mathrm{Perm}(X)$. We define the action

$$\hat{\alpha} : \widetilde{L}[N] \underset{\widetilde{L}}{\otimes} X\widetilde{L} \longrightarrow X\widetilde{L} : (x.\nu) \otimes (y.u_{\sigma G'}) \longmapsto (xy).u_{\nu(\sigma G')}. \tag{2.6}$$

Lemma 2.9. *(a) The action $\hat{\alpha}$ endows $X\widetilde{L}$ with a structure of left $\widetilde{L}[N]$-module algebra.*

(b) If $N \subseteq Perm(X)$ is regular, then $X\widetilde{L}/\widetilde{L}$ is an $\widetilde{L}[N]$-Galois extension.

(c) Additionally, if N is normalized by $\lambda(G)$, then $\widetilde{L}[N]$ is a G-module with action given by (2.5). Recall that $X\widetilde{L}$ is also a G-module with action defined by (2.2). Restricting $\hat{\alpha}$ to the set of G-invariants gives the action

$$\hat{\alpha}^G : \big(\widetilde{L}[N]\big)^G \otimes (X\widetilde{L})^G \longrightarrow (X\widetilde{L})^G$$

making $(X\widetilde{L})^G/K$ into an $\big(\widetilde{L}[N]\big)^G$-Galois extension. Moreover, $H = \big(\widetilde{L}[N]\big)^G$ is a K-Hopf algebra and the restriction of β_L on $1_{\widetilde{L}} \otimes L$ gives the isomorphism $L \cong (X\widetilde{L})^G$.

Proof. See [GP87] Theorem 3.1. □

Example 2.10. Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. Let $\widetilde{L} = L$, then $G = \mathrm{Gal}(\widetilde{L}/K)$ and $G' = \mathrm{Gal}(\widetilde{L}/L) = \{\mathrm{id}\}$, so $X = G/G' = G$.

(1) Define $N_\rho = \rho(G) \subseteq \mathrm{Perm}(G)$ where

$$\rho : G \longrightarrow \mathrm{Perm}(G) : \sigma \longmapsto \big(\tau \mapsto \tau\sigma^{-1}\big)$$

is the *right translation map*. Obviously, $N_\rho \subseteq \mathrm{Perm}(G)$ is regular and normalized by $\lambda(G)$ (it is even centralized by $\lambda(G)$). Its associated Hopf algebra $H = \big(L[N_\rho]\big)^G$ is the set of $\sum_{\sigma\in G} x_\sigma.\sigma \in L[N_\rho]$ such that for every $\tau \in G$:

$$\tau\Big(\sum_{\sigma\in G} x_\sigma.\sigma\Big) = \sum_{\sigma\in G} \tau(x_\sigma).\sigma = \sum_{\sigma\in G} x_\sigma.\sigma \iff \tau(x_\sigma) = x_\sigma \quad \forall \sigma \in G.$$

Thus, $H = K[G]$. By (2.3) and (2.6), the action of $\tau \in G$ on $x \in L$ is given by

$$\tau \underbrace{\Big(\sum_{\sigma\in G} \sigma(x).u_\sigma\Big)}_{=\beta_L(1_{\widetilde{L}}\otimes x)} = \sum_{\sigma\in G} \sigma(x).u_{\sigma\tau^{-1}} = \underbrace{\sum_{\sigma\in G} \sigma\tau(x).u_\sigma}_{=\beta_L(1_{\widetilde{L}}\otimes \tau(x))}.$$

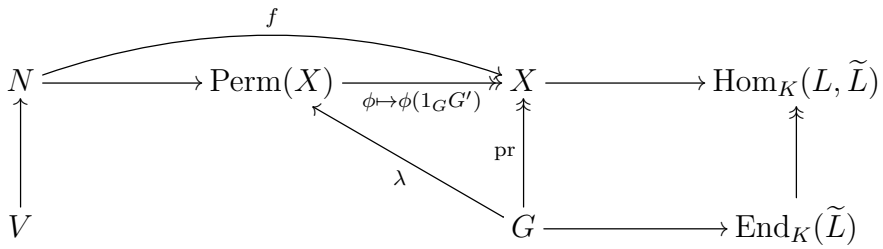
Therefore, the action of $K[G]$ on L is just given by the action of G on L.

(2) Define $N_\lambda = \lambda(G) \subseteq \mathrm{Perm}(G)$. Obviously, $N_\lambda \subseteq \mathrm{Perm}(G)$ is regular and normalized by $\lambda(G)$. Its associated Hopf algebra is $H = \big(L[N_\lambda]\big)^G$. If G is an abelian group, then $H = \big(L[N_\lambda]\big)^G = \big(L[N_\rho]\big)^G = K[G]$. Otherwise, this is another Hopf-Galois structure on L/K.

Definition 2.11. The Hopf-Galois structure on L/K given by N_ρ is called the *canonical classical Hopf-Galois structure* and the one given by N_λ is called the *canonical nonclassical Hopf-Galois structure*. These two structures coincide if and only if L/K is an abelian extension.

We will study in more detail the canonical classical and nonclassical Hopf-Galois structures in section §2.9.

We continue this section with a result that will be important later. Consider the diagram



Then, any subgroup V of N can be seen as a subset of $\mathrm{Hom}_K(L, \widetilde{L})$. The next lemma shows that there exists a subgroup of G whose image in $\mathrm{Hom}_K(L, \widetilde{L})$ is the same as the image of V in $\mathrm{Hom}_K(L, \widetilde{L})$.

Lemma 2.12. *Let $V \subseteq N \subseteq Perm(X)$ be a subgroup which is normalized by $\lambda(G)$. Define*

$$S = pr^{-1}\big(f(V)\big) = \big\{\sigma \in G \,|\, \exists v \in V : v(1_G G') = \sigma G'\big\}.$$

Then S is a subgroup of G containing G' and $\#S = \#G'.\#V$. Moreover, the images of V and S in $Hom_K(L, \widetilde{L})$ coincide.

Proof. As $1_N \in V$, it follows that $G' \subseteq S$.

1. Let $\sigma \in S$ and take $v \in V$ such that $v(1_G G') = \sigma G'$. Since V is normalized by $\lambda(G)$, we know that $\lambda(\sigma^{-1})v^{-1}\lambda(\sigma) \in V$. Applying it to G', we get

$$\big(\lambda(\sigma^{-1})v^{-1}\lambda(\sigma)\big)(1_G G') = \big(\lambda(\sigma^{-1})v^{-1}\big)(\sigma G') = \lambda(\sigma^{-1})(1_G G') = \sigma^{-1}G'.$$

   So, $\sigma^{-1} \in S$.

2. Let $\sigma_1, \sigma_2 \in S$ and take $v_1, v_2 \in V$ such that $v_1(1_G G') = \sigma_1 G', v_2(1_G G') = \sigma_2 G'$. We have $\lambda(\sigma_1)v_2\lambda(\sigma_1^{-1})v_1 \in V$. So,

$$\begin{aligned}\big(\lambda(\sigma_1)v_2\lambda(\sigma_1^{-1})v_1\big)(1_G G') &= \big(\lambda(\sigma_1)v_2\lambda(\sigma_1^{-1})\big)(\sigma_1 G') \\ &= \big(\lambda(\sigma_1)v_2\big)(1_G G') = \lambda(\sigma_1)(\sigma_2 G') = \sigma_1\sigma_2 G'.\end{aligned}$$

   This shows that $\sigma_1\sigma_2 \in S$.

To prove that $\#S = \#G'.\#V$, just remark that the map $f|_V : V \to X$ is injective and that the kernel of $\mathrm{pr} : G \twoheadrightarrow X$ is G'. Finally, $f(V) = \mathrm{pr}(S)$ so V and S must have the same image in $\mathrm{Hom}_K(L, \widetilde{L})$. □

The problem of determining all the possible Hopf-Galois structures on a finite separable extension L/K using Theorem 2.6 is a difficult one since the number of regular subgroups of $\mathrm{Perm}(X)$ grows quickly as the dimension $[L : K]$ increases. In [Byo96], Byott translated the search of subgroups $N \subseteq \mathrm{Perm}(X)$ regular and normalized by $\lambda(G)$ into a search of embeddings $G \to N \rtimes \mathrm{Aut}(N)$ satisfying some stability condition. An application of this result is given by Byott's Uniqueness Theorem.

Theorem 2.13 ([Byo96])**.** *A finite Galois field extension L/K with Galois group G has unique Hopf-Galois structure (the one given by $K[G]$) if and only if $\#G$ is a Burnside number.*

2.3 H-subextensions and H-stable extensions

Throughout this section, let L/K be a finite H-Galois extension where H is a K-Hopf algebra and let L_0 be an intermediate field of L/K. We will introduce the notion of H-subextension (Definition 2.16) and H-stable intermediate field (Definition 2.20).

Definition 2.14. The *annihilator* of L_0 is the K-vector space defined by

$$\mathrm{Ann}_H(L_0) = \big\{h \in H \,|\, h \cdot x = 0 \quad \forall x \in L_0\big\}.$$

We can see $\mathrm{Ann}_H(L_0)$ as the kernel of the morphism of K-vector space

$$\alpha_0 : H \longrightarrow \mathrm{Hom}_K(L_0, L) : h \longmapsto \big(x \mapsto h \cdot x\big). \tag{2.7}$$

If we denote by $\overline{h}$ the image of $h \in H$ by the natural projection $H \twoheadrightarrow H/\mathrm{Ann}_H(L_0)$, then the morphism of K-vector spaces

$$\alpha_0' : H/\mathrm{Ann}_H(L_0) \longrightarrow \mathrm{Hom}_K(L_0, L) : \overline{h} \longmapsto \big(x \mapsto h \cdot x\big) \tag{2.8}$$

is injective.

Lemma 2.15. *The morphism of L-vector spaces*

$$\underline{can}_0 : L \otimes H/Ann_H(L_0) \longrightarrow Hom_K(L_0, L) : x \otimes \overline{h} \longmapsto \big(y \mapsto x(h \cdot y)\big) \tag{2.9}$$

is surjective.

Proof. This follows from the commutative diagram

$$\begin{array}{ccc} L \otimes H & \xrightarrow[\sim]{\underline{\mathrm{can}}} & \mathrm{End}_K(L) \\ \downarrow & & \downarrow \\ L \otimes H/\mathrm{Ann}_H(L_0) & \xrightarrow{\underline{\mathrm{can}}_0} & \mathrm{Hom}_K(L_0, L) \end{array}$$

where the vertical maps are the obvious surjection. □

Definition 2.16. We say that L_0 is an *H-subextension* if the following property holds: if $F \subseteq H$ is a subset whose image under α_0 (as defined in (2.7)) is K-linearly independent, then $\alpha_0(F)$ is also L-linearly independent.

Example 2.17. Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$ and let $H = K[G]$, then it is clear that any intermediate extension is an H-subextension.

Lemma 2.18. *The following statements are equivalent:*

(a) L_0 is an H-subextension;

(b) there is a subset $F \subseteq H$ whose image under α_0 (as defined in (2.7)) is L-linearly independent and generates $\alpha_0(H)$ as a K-vector space;

(c) the map $\underline{can}_0$ (as defined in (2.9)) is injective (and hence bijective by Lemma 2.15).

Proof. (a) $\Rightarrow$ (b): Let B be a K-basis of H, then there exists a subset $B_0 \subseteq B$ such that $\alpha_0(B_0)$ is a K-basis of $\alpha_0(H)$. Since L_0 is an H-subextension, $\alpha_0(B_0)$ is also L-linearly independent in $\mathrm{Hom}_K(L_0, L)$.
(b) $\Rightarrow$ (c): Let $\overline{F}$ be the image of F under the natural projection $H \twoheadrightarrow H/\mathrm{Ann}_H(L_0)$. Then any element u in $L \otimes H/\mathrm{Ann}_H(L_0)$ can be written in the form $u = \sum_{\overline{h}\in\overline{F}} x_{\overline{h}} \otimes \overline{h}$ for some $x_{\overline{h}} \in L$. Since the set $\alpha_0(F)$ is L-linearly independent, if $\underline{\mathrm{can}}_0(u) = 0$, then all $x_{\overline{h}} = 0$ and therefore $u = 0$. Hence $\underline{\mathrm{can}}_0$ is injective.
(c) $\Rightarrow$ (a): Let $F \subseteq H$ be a subset whose image under α_0 is K-linearly independent. The injectivity of the map $\underline{\mathrm{can}}_0$ implies that any K-linearly independent subset of $\alpha_0'\big(H/\mathrm{Ann}_H(L_0)\big)$ is L-linearly independent. Since $\alpha_0(F)$ lies in $\alpha_0'\big(H/\mathrm{Ann}_H(L_0)\big)$, this proves that $\alpha_0(F)$ is L-linearly independent. □

Remark 2.19. By Lemma 2.15, for any intermediate field L_0 of L/K we always have $\dim_K\big(L \otimes H/\mathrm{Ann}_H(L_0)\big) \geq \dim_K\big(\mathrm{Hom}_K(L_0, L)\big)$ or equivalently $\dim_K\big(\mathrm{Ann}_H(L_0)\big) \leq [L : K] - [L_0 : K]$, and by Lemma 2.18, the equality holds if and only if L_0 is an H-subextension. Thus the H-subextensions are the intermediate fields L_0 whose annihilator $\mathrm{Ann}_H(L_0)$ is "big enough".

Definition 2.20. We say that L_0 is *H-stable* if $H \cdot L_0 \subseteq L_0$. If, furthermore, L_0 is an H-subextension, we say that L_0 is *H-normal*.

Example 2.21. Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$ and let $H = K[G]$, then an intermediate field L_0 is H-stable if and only if L_0/K is Galois. By Example 2.17, L_0 is H-normal if and only if L_0/K is Galois. Hence, L_0 is H-normal if and only if it is normal in the classical sense.

Lemma 2.22. *If L_0 is H-stable, then the map $\underline{can}_0$ (as defined in (2.9)) induces a well-defined morphism of K-vector spaces*

$$\underline{can}_0' : L_0 \otimes H/Ann_H(L_0) \longrightarrow End_K(L_0) : x \otimes \overline{h} \longmapsto \big(y \mapsto (x(h \cdot y))\big) \tag{2.10}$$

which is surjective. If, furthermore, L_0 is an H-subextension, then $\underline{can}_0'$ is a bijection.

Proof. By the definition of H-stable, the map $L_0 \otimes H/\mathrm{Ann}_H(L_0) \to \mathrm{End}_K(L_0)$ is well-defined. To see that it is surjective, recall $\underline{\mathrm{can}}_0$ from Lemma 2.15 and consider the following surjective morphism of L-vector spaces:

$$\begin{array}{l} L \underset{L_0}{\otimes} \big(L_0 \otimes H/\mathrm{Ann}_H(L_0)\big) \cong L \otimes H/\mathrm{Ann}_H(L_0) \xrightarrow{\mathrm{can}_0} \mathrm{Hom}_K(L_0, L) \cong L \underset{L_0}{\otimes} \mathrm{End}_K(L_0) : \\ x \underset{L_0}{\otimes} u \longmapsto x \underset{L_0}{\otimes} \underline{\mathrm{can}}_0'(u). \end{array}$$

As $L_0 \to L$ is faithfully flat, the surjectivity of can'_0 follows. If, furthermore, L_0 is also an H-subextension, then the above map is a bijection by Lemma 2.18. Therefore, $\underline{\mathrm{can}}'_0$ is also a bijection. □

The next proposition is the first key result of the correspondence theorem for finite separable Hopf-Galois extensions 2.31.

Proposition 2.23. *(a) If L_0 is any intermediate field, then $Ann_H(L_0)$ is a left ideal in H such that $\epsilon\big(Ann_H(L_0)\big) = 0$.*

(b) If L_0 is an H-subextension, then $Ann_H(L_0)$ is a left ideal two-sided coideal in H.

(c) If L_0 is H-stable, then $Ann_H(L_0)$ is a (two-sided) ideal in H.

(d) If L_0 is H-normal, then L_0/K is $H/Ann_H(L_0)$-Galois and $Ann_H(L_0)$ is a Hopf ideal in H.

Proof. (a) For any $h \in H$, $h' \in \mathrm{Ann}_H(L_0)$ and $x \in L_0$ we have

$$(hh') \cdot x = h \cdot (h' \cdot x) = h \cdot 0 = 0.$$

Therefore, $hh' \in \mathrm{Ann}_H(L_0)$. Moreover, since $1 \in L_0$,

$$0 = h' \cdot 1 = \epsilon(h')1.$$

So, $\epsilon(h') = 0$.

(b) We need to prove that $\Delta\big(\mathrm{Ann}_H(L_0)\big) \subseteq H \otimes \mathrm{Ann}_H(L_0) + \mathrm{Ann}_H(L_0) \otimes H$. We note

$$\pi : H \longrightarrow\!\!\!\!\!\rightarrow H/\mathrm{Ann}_H(L_0) : h \longmapsto \overline{h}$$

the natural projection. Let $h \in \mathrm{Ann}_H(L_0)$ and let $\{\overline{h}_1, ..., \overline{h}_m\}$ be any K-basis of $H/\mathrm{Ann}_H(L_0)$. Then there exist elements $\overline{h}'_1, ..., \overline{h}'_m \in H/\mathrm{Ann}_H(L_0)$ such that $(\pi \otimes \pi)\Delta(h) = \overline{h}_{(1)} \otimes \overline{h}_{(2)} = \sum_{i=1}^m \overline{h}'_i \otimes \overline{h}_i$. For any $x, y \in L_0$, we find

$$\underline{\mathrm{can}}_0\Big(\sum_{i=1}^m (\overline{h}'_i \cdot x) \otimes \overline{h}_i\Big)(y) = \sum_{i=1}^m (\overline{h}'_i \cdot x)(\overline{h}_i \cdot y) = h \cdot (xy) = 0.$$

Since $\underline{\mathrm{can}}_0$ is injective by Lemma 2.18, we obtain that $\sum_{i=1}^m (\overline{h}'_i \cdot x) \otimes \overline{h}_i = 0$. Because the elements $\overline{h}_i$ form a K-basis of $H/\mathrm{Ann}_H(L_0)$, it follows that $\overline{h}'_i \cdot x = 0$ $\forall x \in L_0$, hence (since α'_0 from (2.8) is injective) $\overline{h}'_i = 0$ for all indices i. We can thus conclude that $(\pi \otimes \pi)\Delta(h) = 0$ and therefore

$$\Delta(h) \in \mathrm{Ker}(\pi \otimes \pi) = H \otimes \mathrm{Ann}_H(L_0) + \mathrm{Ann}_H(L_0) \otimes H.$$

(c) We already know by (a) that $\mathrm{Ann}_H(L_0)$ is a left ideal. For any $h \in H$, $h' \in \mathrm{Ann}_H(L_0)$ and $x \in L_0$ we have

$$h \cdot x \in L_0 \implies (h'h) \cdot x = h' \cdot (h \cdot x) = 0.$$

Therefore, $h'h \in \mathrm{Ann}_H(L_0)$.

(d) We already know that $\mathrm{Ann}_H(L_0)$ is a biideal, so $H/\mathrm{Ann}_H(L_0)$ is a bialgebra. By Lemma 2.22, the map $\underline{\mathrm{can}}'_0$ is bijective and hence L_0/K is $H/\mathrm{Ann}_H(L_0)$-Galois. By Proposition 1.67, the bialgebra $H/\mathrm{Ann}_H(L_0)$ is Hopf algebra. Therefore, $\mathrm{Ann}_H(L_0)$ is a Hopf ideal.

□

2.4 The space of invariants of a Hopf-Galois extension

In this section, we study the space of invariants of the finite separable H-Galois extension L/K.

Lemma 2.24. *Let $I \subseteq H$ and let L^I be the space of I-invariants as defined in Definition 1.54.*

(a) If I is a left ideal two-sided coideal of H, then L^I is an intermediate field of L/K.

(b) If I is a right ideal of H and if $\epsilon(I) = 0$, then L^I is H-stable.

Proof. (a) Let $h' \in I$ and $x \in K$, then, by Definition 1.38.2., $h' \cdot x = \epsilon(h')x = 0$. Thus, L^I contains K. For any $y, z \in L^I$, we have $h' \cdot (y + z) = 0$ and, since $\Delta(h') \in H \otimes I + I \otimes H$, $h' \cdot (xy) = (h'_{(1)} \cdot y)(h'_{(2)} \cdot z) = 0$ by Definition 1.38.3. So, L^I is a ring containing K and it is a field because L/K is an algebraic extension.

(b) Let $h \in H$, $h' \in I$ and $x \in L^I$, then

$$h'h \in I \implies h' \cdot (h \cdot x) = (h'h) \cdot x = \epsilon(h'h)x = 0.$$

So, $h \cdot x \in L^I$.

□

We will now state the second key proposition of the correspondence theorem for separable Hopf-Galois extensions 2.31.

Proposition 2.25. *Let $I \subseteq H$ be a left ideal two-sided coideal, then L^I is an H-subextension and $Ann_H(L^I) = I$.*

We will postpone the proof of this proposition to later in this section.

Let $\widetilde{L}/K$ be a finite Galois extension containing L and let $I \subseteq H$ be a left ideal two-sided coideal. Then the natural projection

$$\widetilde{p} : \widetilde{L} \otimes H \longrightarrow\!\!\!\!\!\rightarrow \widetilde{L} \otimes H/I \tag{2.11}$$

is a morphism of left $\widetilde{L} \otimes H$-modules and $\widetilde{L}$-coalgebras. Combining it with the morphism $\beta_H : \widetilde{L} \otimes H \cong \widetilde{L}[N]$ defined in (2.4), we get

$$\widetilde{\pi} : \widetilde{L}[N] \longrightarrow\!\!\!\!\!\rightarrow \widetilde{L} \otimes H/I \tag{2.12}$$

which is a surjective morphism of left $\widetilde{L}[N]$-modules and $\widetilde{L}$-coalgebras.
Let

$$\mathrm{HKer}(\widetilde{\pi}) = {}^{\mathrm{co}\,\widetilde{L}\otimes H/I}\big(\widetilde{L}[N]\big) := \big\{ l \in \widetilde{L}[N] \,|\, \widetilde{\pi}(l_{(1)}) \otimes l_{(2)} = \widetilde{\pi}(1_{\widetilde{L}[N]}) \otimes l \big\} \tag{2.13}$$

be the set of left $\widetilde{L}\otimes H/I$-coinvariants. By Theorem 1.57, $\mathrm{HKer}(\widetilde{\pi})$ is a Hopf subalgebra of $\widetilde{L}[N]$ so, by Lemma 1.34, $\mathrm{HKer}(\widetilde{\pi})$ must be of the form $\widetilde{L}[V]$ for some subgroup $V \subseteq N$. As $V = \mathrm{HKer} \cap N$ and because N is the set of grouplike elements of $\widetilde{L}[N]$, we obtain the following explicit description:

$$V = \big\{ n \in N \,|\, \widetilde{\pi}(n) \otimes n = \widetilde{\pi}(1_N) \otimes n \big\} \tag{2.14}$$

$$= \big\{ n \in N \,|\, \widetilde{\pi}(n) = \widetilde{\pi}(1_N) \big\}. \tag{2.15}$$

Lemma 2.26. *Let $n, m \in N$, we have the equivalence $\widetilde{\pi}(n) = \widetilde{\pi}(m) \Leftrightarrow nV = mV$ and the isomorphism of $\widetilde{L}$-coalgebras $\widetilde{L} \otimes H/I \cong \widetilde{L}[N/V]$.*

Proof. Let $n, m \in N$ such that $nV = mV$. Then $m = nv$ for some $v \in V$. Because $\widetilde{\pi}$ is a morphism of left $\widetilde{L}[N]$-modules, we have $\widetilde{\pi}(ll') = l.\widetilde{\pi}(l')$ for every $l, l' \in \widetilde{L}[N]$. In particular,

$$\widetilde{\pi}(m) = \widetilde{\pi}(nv) = n.\widetilde{\pi}(v) = n.\widetilde{\pi}(\mathrm{id}_N) = \widetilde{\pi}(n).$$

The map $\widetilde{\pi}$ can thus be defined on N/V and induces a surjective map $\widetilde{L}[N/V] \twoheadrightarrow \widetilde{L} \otimes H/I$.

This last map is also injective: let $n, m \in N$ such that $\widetilde{\pi}(n) = \widetilde{\pi}(m)$, then

$$\widetilde{\pi}(m^{-1}n) = m^{-1}.\widetilde{\pi}(n) = m^{-1}.\widetilde{\pi}(m) = \widetilde{\pi}(m^{-1}m) = \widetilde{\pi}(\mathrm{id}_N),$$

so $m^{-1}n \in V$ and $mV = nV$. □

Remark 2.27. The subgroup $V \subseteq N$ is not normal in general. More precisely, V is normal if and only if the coalgebra $\widetilde{L}[N/V]$ is a Hopf algebra, i.e. if and only if I is a Hopf ideal of H.

Let us consider the morphism of $\widetilde{L}$-coalgebras $\widetilde{\pi} : \widetilde{L}[N] \to \widetilde{L} \otimes H/I \cong \widetilde{L}[N/V]$. An element $\sum_{n\in N} x_n n \in \widetilde{L}[N]$ is in the kernel of $\widetilde{\pi}$ if and only if for each coset $mV \in N/V$ we have

$$\sum_{n\in mV} x_n = 0.$$

Therefore, the kernel of $\widetilde{\pi}$ is generated as an $\widetilde{L}$-vector space by the elements $n - m$ with $n, m \in N$ such that $nV = mV$. This leads to the equality:

$$\begin{aligned} L^{\mathrm{Ker}(\widetilde{\pi})} &= \big\{x \in L \,|\, l.x = 0 \quad \forall l \in \mathrm{Ker}(\widetilde{\pi})\big\} \\ &= \big\{x \in L \,|\, n.x = m.x \quad \forall n, m \in N \text{ such that } nV = mV\big\} \\ &= \big\{x \in L \,|\, v.x = x \quad \forall v \in V\big\} = L^V. \end{aligned}$$

Let $\beta_H : \widetilde{L} \otimes H \cong \widetilde{L}[N]$ be the map defined in (2.4). Then β_H is a morphism of G-modules with actions defined by

$$\sigma(x \otimes h) = \sigma(x) \otimes h \quad \forall \sigma \in G, x \in \widetilde{L}, h \in H$$

and

$$\sigma(x.\nu) = \sigma(x).\big(\lambda(\sigma)\nu\lambda(\sigma^{-1})\big) \quad \forall \sigma \in G, x \in \widetilde{L}, \nu \in N.$$

Since G acts on $\widetilde{L} \otimes H$ only via the left factor $\widetilde{L}$, the map $\widetilde{\pi} : \widetilde{L}[N] \cong \widetilde{L} \otimes H \twoheadrightarrow \widetilde{L} \otimes H/I$ is also a morphism of G-modules.

Lemma 2.28. *The subgroup $V \subseteq N \subseteq Perm(X)$ is normalized by $\lambda(G)$.*

Proof. For $\sigma \in G$ and $\nu \in N$, we will write $\sigma.\nu$ for $\lambda(\sigma)\nu\lambda(\sigma^{-1})$. Because $\widetilde{\pi} : \widetilde{L}[N] \twoheadrightarrow \widetilde{L} \otimes H/I$ is a morphism of G-modules, we have for every $\sigma \in G$ and $v \in V$:

$$\widetilde{\pi}(\sigma.v) = \sigma.\widetilde{\pi}(v) = \sigma.\widetilde{\pi}(1_N) = \widetilde{\pi}(\sigma.1_N) = \widetilde{\pi}(1_N).$$

So, $\sigma.v \in V$, i.e. V is normalized by $\lambda(G)$. □

Proof of Proposition 2.25. Let $S = \mathrm{pr}^{-1}\big(f(V)\big)$ be the subgroup of G associated to V as defined in Lemma 2.12. Since the images of S and V in $\mathrm{Hom}_K(L, \widetilde{L})$ coincide, we obtain $L^V = L^S$. Furthermore, as G' is contained in S, we also have $L^S = \widetilde{L}^S$. Now we can apply classical Galois theory to compute dimensions:

$$[L^{\mathrm{Ker}(\widetilde{\pi})} : K] = [\widetilde{L}^S : K] = \frac{[\widetilde{L} : K]}{\#S} = \frac{[L : K]}{\#V} = \frac{\#N}{\#V} = \dim_K H/I.$$

We thus obtain

$$[L^I : K] \geq [L^{\mathrm{Ker}(\widetilde{\pi})} : K] = \dim_K H/I \geq \dim_K H/\mathrm{Ann}_H(L^I)$$

where the first inequality comes from $I \subseteq \mathrm{Ker}(\widetilde{\pi})$ and the last one from $I \subseteq \mathrm{Ann}_H(L^I)$. Combining this with the surjective morphism $L \otimes H/\mathrm{Ann}_H(L^I) \twoheadrightarrow \mathrm{Hom}_K(L^I, L)$ from Lemma 2.15, we can deduce that this morphism is an isomorphism. By Lemma 2.18, this proves that L^I is an H-subextension. We can also deduce from the isomorphism that

$$[L^I : K] = [L^{\mathrm{Ker}(\widetilde{\pi})} : K] = \dim_K H/I = \dim_K H/\mathrm{Ann}_H(L^I).$$

So, $\mathrm{Ann}_H(L^I) = I$. □

We end this subsection by showing that the space of invariants with respect to a left ideal two-sided coideal coincides with the space of invariants with respect to the associated Hopf ideal.

Lemma 2.29. *Let L/K be a finite H-Galois extension and let $I \subseteq H$ be a left ideal two-sided coideal. Consider the Hopf subalgebra $H_0 = \varphi(I) \subseteq H$ as defined in Definition 1.56. By dualizing, we find that $(H/I)^*$ is a right coideal subalgebra of H^* and $\pi : H^* \twoheadrightarrow H_0^*$ is a Hopf algebra morphism. Then the following subsets of L coincide:*

$$L^I = \rho^{-1}\big(L \otimes (H/I)^*\big) = L^{co\,H_0^*} = L^{H_0}$$

where $\rho : L \to L \otimes H^*$ is the coaction as defined in (1.2).

Proof. $\underline{L^I \subseteq \rho^{-1}(L \otimes (H/I)^*)}$. Take any $x \in L^I$ and take a finite dual base $\{(e_i, f_i)\}$ of H, whose first m elements are in I and the next $n-m$ elements generate a linear complement of I in H. Then $f_{m+1}, \ldots, f_n$ provide exactly a base of $(H/I)^*$ and we find

$$\rho(x) = \sum_{i=1}^{n} (e_i \cdot x) \otimes f_i = \sum_{i=m+1}^{n} (e_i \cdot x) \otimes f_i \in L \otimes (H/I)^*.$$

$\underline{\rho^{-1}(L \otimes (H/I)^*) \subseteq L^{\mathrm{co}\,H_0^*}}$. Recall from Definition 1.56 and Theorem 1.57 that $I = HH_0^+$. Since for any $x \in H_0$, we have that $x - \epsilon(x)1_H \in H_0^+ \subseteq I$, we find that the composition $H_0 \subseteq H \twoheadrightarrow H/I$ is given by the map $x \mapsto \epsilon(x)1$. Dualizing this gives $(H/I)^* \subseteq H^* \twoheadrightarrow H_0^*$, we thus find that $\pi(a) = \epsilon_{H^*}(a)1_{H_0^*}$ for any $a \in (H/I)^*$ where ϵ_{H^*} and $1_{H_0^*}$ are the dual of the multiplication and the dual of the counit respectively (see Propositions 1.45 and 1.43). Now let $x \in L$ such that $\rho(x) \in L \otimes (H/I)^*$, then $x_{[0]} \otimes \pi(x_{[1]}) = x_{[0]} \otimes \epsilon(x_{[1]})1_{H_0^*} = x \otimes 1_{H_0^*}$.
$\underline{L^{\mathrm{co}\,H_0^*} \subseteq L^{H_0}}$. Let $x \in L^{\mathrm{co}\,H_0^*}$, then $x_{[0]} \otimes \pi(x_{[1]}) = x \otimes 1_{H_0^*}$. So $\forall b \in H_0$, $bx =$

$x\left\langle 1_{H_0^*}, b\right\rangle = \epsilon(b)x$ and therefore $x \in L^{H_0}$.
$L^{H_0} \subseteq L^I$. it is easy to see that $L^{H_0} \subseteq L^{H_0^+} = L^{HH_0^+}$. To finish the proof, just recall by Definition 1.56 and Theorem 1.57 that $HH_0^+ = I$. □

Let us end this section by the observation that the notion invariants is stable under base change. Recall that if L is an H-module algebra, and $L \subseteq \widetilde{L}$ is any field extension, then $\widetilde{L} \otimes L$ is a $\widetilde{L} \otimes H$-module algebra.

Lemma 2.30. *Let L be an H-module K-algebra and $F \subseteq H$ a K-linear subspace. Then for any base extension $\widetilde{L}/L$, we have that*

$$(\widetilde{L} \otimes L)^{\widetilde{L}\otimes F} = \widetilde{L} \otimes L^F.$$

Proof. This follows from the fact that the space of invariants is a limit in Vect_K and the extension-of-scalars functor preserves limits. An explicit argument is as follows.

Take $\tilde{x} \otimes x \in \widetilde{L} \otimes L^F$. Then for any $\tilde{y} \otimes h \in \widetilde{L} \otimes F$, we find that

$$(\tilde{y} \otimes h) \cdot (\tilde{x} \otimes x) = \tilde{y}\tilde{x} \otimes h \cdot x = \tilde{y}\tilde{x} \otimes \epsilon(h)x = \epsilon(\tilde{y} \otimes h)\tilde{x} \otimes x.$$

So $\widetilde{L} \otimes L^F \subseteq (\widetilde{L} \otimes L)^{\widetilde{L}\otimes F}$. On the other hand, take any $\sum_i \tilde{x}_i \otimes x_i \in (\widetilde{L} \otimes L)^{\widetilde{L}\otimes F}$, where we suppose without loss of generality that the elements $\tilde{x}_i$ are linearly independent. Then for any $h \in F$, we find using the definition of the action under extension of scalars that

$$(1 \otimes h) \cdot (\sum_i \tilde{x}_i \otimes x_i) = \sum_i \tilde{x}_i \otimes h \cdot x_i$$

and on the other hand, since $\sum_i \tilde{x}_i \otimes x_i$ is $\widetilde{L} \otimes F$-invariant, we find

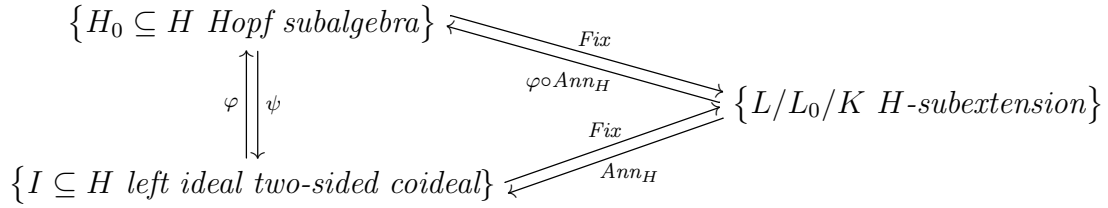
$$(1 \otimes h) \cdot (\sum_i \tilde{x}_i \otimes x_i) = \sum_i \tilde{x}_i \otimes \epsilon(h)x_i$$

Since the elements $\tilde{x}_i$ are linearly independent we can conclude that $x_i \in L^F$ for all indices i, and hence $\sum_i \tilde{x}_i \otimes h \cdot x_i \in \widetilde{L} \otimes L^F$. □

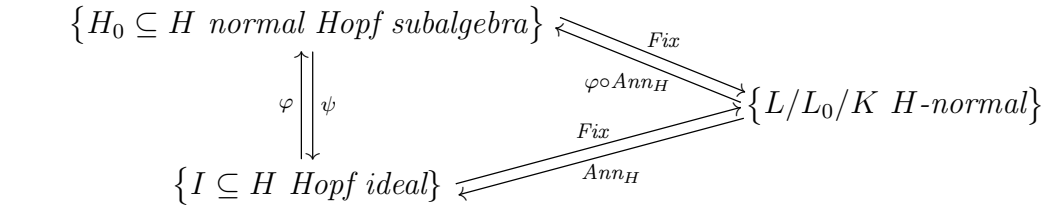
2.5 Correspondence theorem for Hopf-Galois extensions

Theorem 2.31. *Let L/K be a finite separable H-Galois extension. Let Fix, Ann_H and φ be defined as in Proposition 2.2, Definition 2.14 and Definition 1.56 respectively.*

Then the maps



are inverse bijections. Moreover, the above correspondence restricts to the following inverse bijections:

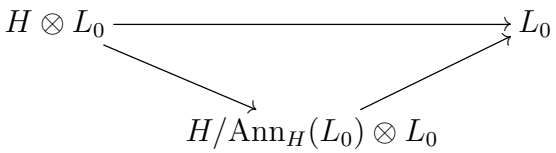


Proof. The vertical arrows come from Theorem 1.58. We know that all the maps Fix and Ann_H are well-defined. By Lemma 2.29, we also know that $\mathrm{Fix}(H_0) = \mathrm{Fix}\big(\psi(H_0)\big)$ and $\mathrm{Fix}(I) = \mathrm{Fix}\big(\varphi(I)\big)$ for any Hopf subalgebra $H_0 \subseteq H$ and any left ideal two-sided coideal $I \subseteq H$. Furthermore, Proposition 2.25 tells that $\mathrm{Ann}_H(L^I) = I$, which provides half of the correspondence.
For the other half, let L_0 be an H-subextension. We clearly have the inclusion $L_0 \subseteq L^{\mathrm{Ann}_H(L_0)}$. Again by Proposition 2.25, we have $[L^{\mathrm{Ann}_H(L_0)} : K] = \dim_K H/\mathrm{Ann}_H(L_0)$. Moreover, by Lemma 2.18, the map $\underline{\mathrm{can}}_0 : L \otimes H/\mathrm{Ann}_H(L_0) \to \mathrm{Hom}_K(L_0, L)$ is an isomorphism, proving that $[L_0 : K] = \dim_K H/\mathrm{Ann}_H(L_0)$. Therefore, $[L^{\mathrm{Ann}_H(L_0)} : K] = [L_0 : K]$ and the inclusion $L_0 \subseteq L^{\mathrm{Ann}_H(L_0)}$ is an equality. □

If L_0 is H-normal, we already know by Proposition 2.23 that L_0/K is $H/\mathrm{Ann}_H(L_0)$-Galois. The next proposition shows that even if L_0 is only an H-subextension, L/L_0 is also Hopf-Galois.

Lemma 2.32. *Suppose L_0 is an H-subextension. Define the left ideal two-sided coideal $I = Ann_H(L_0)$ and the Hopf subalgebra $H_0 = {}^{co\,H/I}H$ of H. Let $h \in H_0$ and $x \in L_0$, then $h \cdot x = \epsilon(h)x$.*

Proof. By definition of $Ann_H(L_0)$, the map $H \otimes L_0 \longrightarrow L : h \otimes x \longmapsto h \cdot x$ factors through $H/\mathrm{Ann}_H(L_0) \otimes L_0$:



Let $H \twoheadrightarrow H/\mathrm{Ann}_H(L_0) : h \mapsto \overline{h}$ be the natural projection, $h \in H_0$ and $x \in L_0$. As $H_0 = {}^{\mathrm{co}\,H/I}H$, we can use that $\overline{h_{(1)}} \otimes h_{(2)} = \overline{1_H} \otimes h$ to get

$$\begin{aligned} h \cdot x &= h \cdot (x1) = (h_{(1)} \cdot x)(h_{(2)} \cdot 1) = (\overline{h_{(1)}} \cdot x)(h_{(2)} \cdot 1) \\ &= (\overline{1_H} \cdot x)(h \cdot 1) = x\epsilon(h). \end{aligned}$$

□

Proposition 2.33. *Let L/K be a finite H-Galois extension and let L_0 be an intermediate field. Suppose L_0 is an H-subextension. Consider the Hopf subalgebra $H_0 = (\varphi \circ Ann_H)(L_0)$ as constructed in Theorem 2.31. Then the following statements hold.*

(a) $L \otimes H_0 = \{\sum_i x_i \otimes h_i \in L \otimes H \mid \underline{can}(\sum_i x_i \otimes h_i) \in End_{L_0}(L)\}$.

(b) L/L_0 *is* $L_0 \otimes H_0$*-Galois, i.e. the map* $\underline{can}_{L/L_0} : L \otimes H_0 \to End_{L_0}(L)$ *is bijective.*

Proof. (a). If $x \otimes h \in L \otimes H_0$, then for all $y \in L_0$ and for all $z \in L$ we have

$$\underline{\mathrm{can}}(x \otimes h)(yz) = x(h_{(1)} \cdot y)(h_{(2)} \cdot z) = x\epsilon(h_{(1)})y(h_{(2)} \cdot z) = xy(h \cdot z) = y\,\underline{\mathrm{can}}(x \otimes h)(z).$$

Therefore, $\underline{\mathrm{can}}(x \otimes h) \in \mathrm{End}_{L_0}(L)$. Conversely, take $\sum_i x_i \otimes h_i \in L \otimes_K H$ such that the elements x_i are linearly independent over K and $\underline{\mathrm{can}}(\sum_i x_i \otimes h_i)$ is left L_0-linear. This means that for all $x_0 \in L_0$ and all $x \in L$, the following equality holds

$$\sum_i x_i x_0 (h_i \cdot x) = \sum_i x_i h_i \cdot (x_0 x) = \sum_i x_i (h_{i(1)} \cdot x_0)(h_{i(2)} \cdot x)$$

Using the bijectivity of $\underline{\mathrm{can}} : L \otimes H \to \mathrm{End}_K(L)$, this equality can be translated into

$$\sum_i x_i x_0 \otimes h_i = \sum_i x_i (h_{i(1)} \cdot x_0) \otimes h_{i(2)}$$

which holds for all $x_0 \in L_0$. Since L_0 is an H-subextension, we have that $\underline{\mathrm{can}}_0 : L \otimes H/\mathrm{Ann}_H(L_0) \to \mathrm{Hom}_K(L_0, L)$ is injective. Hence the previous equality is furthermore equivalent to

$$\sum_i x_i \otimes \pi(1) \otimes h_i = \sum_i x_i \otimes \pi(h_{i(1)}) \otimes h_{i(2)} \in L \otimes H/\mathrm{Ann}_H(L_0) \otimes H$$

where we denote $\pi : H \to H/\mathrm{Ann}_H(L_0)$ for the canonical surjection. Since we assumed that the elements x_i are linearly independent, we find that $\pi(1) \otimes h_i = \pi(h_{i(1)}) \otimes h_{i(2)}$ for all i. Hence h_i belongs in the set of left $H/\mathrm{Ann}_H(L_0)$-coinvariants and thus, by

Theorem 1.57, $h_i \in H_0$.
(b). Consider the following commutative diagram

$$\begin{array}{ccccc} L \otimes H & & \xrightarrow[\sim]{\underline{\text{can}}} & & \text{End}_K(L) \\ \uparrow & & & & \uparrow \\ L \otimes H_0 & \xrightarrow{\cong} & L \otimes_{L_0} (L_0 \otimes H_0) & \xrightarrow{\underline{\text{can}}_{L/L_0}} & \text{End}_{L_0}(L) \end{array}$$

Since $\underline{\text{can}}$ is bijective, $\underline{\text{can}}_{L/L_0}$ is also injective. It is surjective by part (a). Hence L/L_0 is $L_0 \otimes H_0$-Galois. □

We finish this section with a converse result on H-subextensions and H-normal extensions.

Corollary 2.34. *Let L/K be a finite separable H-Galois extension and let L_0 be an intermediate field.*

(a) Let H_0 be a Hopf subalgebra of H and suppose that L/L_0 is $L_0 \otimes H_0$-Galois, then L_0 is an H-subextension.

(b) Suppose L_0 is H-stable. Let I be a Hopf ideal of H such that the action of H on L_0 factors through H/I:

$$\begin{array}{ccc} H \otimes L_0 & \longrightarrow & L_0 \\ & \searrow \quad \nearrow & \\ & H/I \otimes L_0 & \end{array}$$

If L_0/K is H/I-Galois, then L_0 is H-normal.

Proof. (a) Using Proposition 1.65, we get that $L_0 = L^{L_0 \otimes H_0} = L^{H_0}$. By Theorem 2.31, this proves that L_0 is an H-subextension.

(b) We already know by Theorem 2.31 that L^I is H-normal and by Proposition 2.23(d) that L^I/K is H/I-Galois. For all $h \in I$ and $x \in L_0$, we have $h \cdot x = 0$, so $L_0 \subseteq L^I$. Moreover, since both L_0/K and L^I/K are H/I-Galois, then $[L_0 : K] = [L^I : K]$. Therefore, $L_0 = L^I$.

□

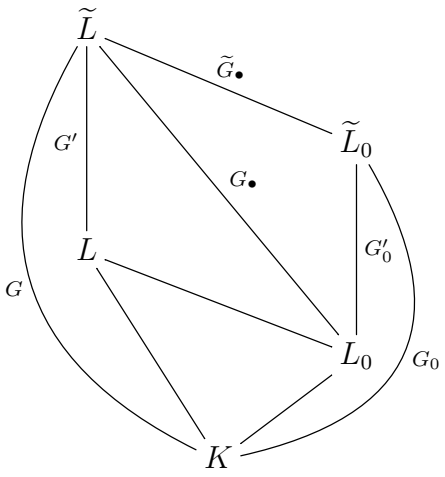
2.6 Relation with the Greither-Pareigis group

In this section, we will look at the properties of the Greither-Pareigis group $N \subseteq \mathrm{Perm}(X)$ to determine whether an intermediate field L_0 is H-stable (Lemma 2.38) or is an H-subextension (Lemma 2.43). We will also translate Theorem 2.31 in terms of groups (Theorem 2.45).

Throughout this section, we will use the following notations (see also §2.2):

1. L/K is a finite separable Hopf-Galois extension with Hopf algebra H;
2. $\widetilde{L}/K$ is a finite Galois extension containing L;
3. $G = \mathrm{Gal}(\widetilde{L}/K)$, $G' = \mathrm{Gal}(\widetilde{L}/L)$ and $X = G/G'$;
4. $N \subseteq \mathrm{Perm}(X)$ is the Greither-Pareigis group associated with the H-Galois extension L/K (Theorem 2.6);
5. L_0 is an intermediate field of L/K;
6. $\widetilde{L}_0/K$ is a finite Galois extension containing L_0 and contained in $\widetilde{L}$;
7. $G_0 = \mathrm{Gal}(\widetilde{L}_0/K)$, $G'_0 = \mathrm{Gal}(\widetilde{L}_0/L_0)$ and $X_0 = G_0/G'_0$;
8. $G_\bullet = \mathrm{Gal}(\widetilde{L}/L_0)$ and $\widetilde{G}_\bullet = \mathrm{Gal}(\widetilde{L}/\widetilde{L}_0)$.

These notations are summarized in the diagram



Note that $\widetilde{G}_\bullet$ is a normal subgroup of both G and $G_\bullet$, we thus have the morphisms of groups

$$G \longrightarrow\!\!\!\!\!\rightarrow G/\widetilde{G}_\bullet \cong G_0 \text{ and } G_\bullet \longrightarrow\!\!\!\!\!\rightarrow G_\bullet/\widetilde{G}_\bullet \cong G'_0. \tag{2.16}$$

We will refer to these maps by $\sigma \mapsto \overline{\sigma}$. Also note that $G' \subseteq G_\bullet \subseteq G$, we can then define the natural projection

$$\pi : X = G/G' \longrightarrow\!\!\!\!\!\rightarrow G/G_\bullet : \sigma G' \longmapsto \sigma G_\bullet \tag{2.17}$$

from the set of G'-cosets to the set of $G_\bullet$-cosets. Note that π is a morphism of left G-modules. Together with the isomorphism of G-modules $G/G_\bullet \cong (G/\widetilde{G}_\bullet)/(G_\bullet/\widetilde{G}_\bullet) \cong G_0/G'_0 = X_0$, we can define the morphism of left G-modules $p : X \twoheadrightarrow X_0$ by the commutative diagram

$$\begin{array}{ccc} X & \xrightarrow{\quad p \quad} & X_0 \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\cong} \\ G/G_\bullet & \xrightarrow{\cong} & (G/\widetilde{G}_\bullet)/(G_\bullet/\widetilde{G}_\bullet) \end{array} \quad : \quad \begin{array}{ccc} \sigma G' & \longmapsto & \overline{\sigma} G'_0 \\ \downarrow & & \uparrow \\ \sigma G_\bullet & \longmapsto & \overline{\sigma G_\bullet} \end{array} \tag{2.18}$$

Suppose that L_0 is H-normal. By Proposition 2.23(d), L_0/K is $H/\mathrm{Ann}_H(L_0)$-normal, so this extension has an associated Greither-Pareigis group $N_0 \subseteq \mathrm{Perm}(X_0)$. Using Lemma 2.7 for the H-Galois extension L/K and the $H/\mathrm{Ann}_H(L_0)$ extension L_0/K, we get the morphisms of Hopf algebras

$$\beta_L : \widetilde{L} \otimes H \xrightarrow{\cong} \widetilde{L}[N] \text{ and } \beta_{L_0} : \widetilde{L}_0 \otimes H/\mathrm{Ann}_H(L_0) \xrightarrow{\cong} \widetilde{L}_0[N_0]\,.$$

Together with the natural projection $H \twoheadrightarrow H/\mathrm{Ann}_H(L_0)$, we obtain the morphisms of Hopf algebras

$$\widetilde{L}[N] \cong \widetilde{L} \otimes H \twoheadrightarrow \widetilde{L} \otimes H/\mathrm{Ann}_H(L_0) \cong \widetilde{L}[N_0],$$

which restricts to a morphism of groups $N \twoheadrightarrow N_0$. As $N \subseteq \mathrm{Perm}(X)$ and $N_0 \subseteq \mathrm{Perm}(X_0)$, we would hope this map to be the restriction on N of a map from $\mathrm{Perm}(X)$ to $\mathrm{Perm}(X_0)$. The next example shows that, in general, there is no canonical map from $\mathrm{Perm}(X)$ to $\mathrm{Perm}(X_0)$.

Example 2.35. Let $S_3 = \langle \sigma, \tau \,|\, \sigma^3 = \tau^2 = (\sigma\tau)^2 = \mathrm{id} \rangle$. Let $G = G_0 = S_3$, $G' = \{\mathrm{id}\}$, $G'_0 = \langle \tau \rangle$, $X = S_3$ and $X_0 = S_3/\langle \tau \rangle$. Let

$$\rho : G \longrightarrow \mathrm{Perm}(X) : g \longmapsto \left(g' \mapsto g'g^{-1}\right)$$

be the right translation map and consider the permutation $\rho(\sigma) \in \mathrm{Perm}(X)$, then $\rho(\sigma)(\mathrm{id}) = \sigma^{-1} \in \sigma^{-1}G'_0$ and $\rho(\sigma)(\tau) = \tau\sigma^{-1} \in \sigma G'_0$. Therefore $\rho(\sigma)$ does not map to an element of $\mathrm{Perm}(X_0)$.

To overcome this problem, we will define the subset of elements of $\mathrm{Perm}(X)$ that are well-defined in $\mathrm{Perm}(X_0)$.

Definition 2.36. Let $\pi : X \twoheadrightarrow G/G_\bullet$ be the map defined in (2.17). We define the subset of *π-compatible permutations*

$$\mathrm{Perm}_\pi(X) = \big\{ f \in \mathrm{Perm}(X) \,|\, \pi(\sigma G') = \pi(\tau G') \Longrightarrow (\pi \circ f)(\sigma G') = (\pi \circ f)(\tau G') \big\}.$$

Lemma 2.37. *The subset $Perm_\pi(X)$ is a subgroup of $Perm(X)$.*

Proof. Let $f, g \in \mathrm{Perm}_\pi(X)$ and let $\sigma G', \tau G' \in X$ such that $\pi(\sigma G') = \pi(\tau G')$. Then

$$\pi(\sigma G') = \pi(\tau G') \Rightarrow \pi\big(g(\sigma G')\big) = \pi\big(g(\tau G')\big) \Rightarrow \pi\big(fg(\sigma G')\big) = \pi\big(fg(\tau G')\big).$$

So, $fg \in \mathrm{Perm}_\pi(X)$. □

The subgroup $\mathrm{Perm}_\pi(X)$ can alternatively be understood as the set of $f \in \mathrm{Perm}(X)$ for which there exists $f_\pi \in \mathrm{Perm}(G/G_\bullet)$ making the diagram

$$\begin{array}{ccc} X & \xrightarrow{\ f\ } & X \\ {\scriptstyle\pi}\big\downarrow & & \big\downarrow{\scriptstyle\pi} \\ G/G_\bullet & \xrightarrow{\ f_\pi\ } & G/G_\bullet \end{array}$$

commmute. Therefore, $\mathrm{Perm}_\pi(X)$ is the largest subgroup of $\mathrm{Perm}(X)$ for which the $G_\bullet$-cosets are blocks. This allows us to define the surjective morphism of groups

$$\mathrm{Perm}_\pi(X) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Perm}(G/G_\bullet) : f \longmapsto \big(\sigma G_\bullet \mapsto (\pi \circ f)(\sigma G')\big)$$

where $\sigma G' \in X$ is any G'-coset such that $\pi(\sigma G') = \sigma G_\bullet$.

The following proposition shows the link between the subgroup $\mathrm{Perm}_\pi(X)$ and the notion of H-stable fields.

Proposition 2.38. *With the notation above, the intermediate field L_0 is H-stable if and only if $N \subseteq Perm_\pi(X)$.*

Proof. Recall from Lemma 2.7 that the action $\alpha : H \otimes L \to L$ extends to the action $\widetilde{\alpha} : \widetilde{L}[N] \underset{\widetilde{L}}{\otimes} X\widetilde{L} \to X\widetilde{L}$. If L_0 is H-stable, then we can define similarly the action $\widetilde{\alpha}_0 : \widetilde{L}[N] \underset{\widetilde{L}}{\otimes} (G/G_\bullet)\widetilde{L} \to (G/G_\bullet)\widetilde{L}$ by the diagram

$$\begin{array}{ccccc}
\widetilde{L}[N] \underset{\widetilde{L}}{\otimes} (G/G_\bullet)\widetilde{L} & & \xrightarrow{\qquad\qquad\widetilde{\alpha}_0\qquad\qquad} & & (G/G_\bullet)\widetilde{L} \\
{\scriptstyle \beta_H \underset{\widetilde{L}}{\otimes} \beta_{L_0}}\uparrow{\scriptstyle \cong} & & & & {\scriptstyle \cong}\uparrow{\scriptstyle \beta_{L_0}} \\
(\widetilde{L} \otimes H) \underset{\widetilde{L}}{\otimes} (\widetilde{L} \otimes L_0) & \xrightarrow{\cong} & \widetilde{L} \otimes (H \otimes L_0) & \xrightarrow{\mathrm{id}\otimes\alpha} & \widetilde{L} \otimes L_0
\end{array}$$

where $(G/G_\bullet)\widetilde{L}$ denotes the set of maps from the set of $G_\bullet$-cosets $G/G_\bullet$ to the field $\widetilde{L}$. The natural projection $\pi : X \twoheadrightarrow G/G_\bullet$ induces the injective map

$$i : (G/G_\bullet)\widetilde{L} \hookrightarrow X\widetilde{L} : f \longmapsto f \circ \pi. \tag{2.19}$$

Putting $\widetilde{\alpha}$, $\widetilde{\alpha}_0$ and i together, we obtain the commutative diagram

$$\begin{array}{ccc}
\widetilde{L}[N] \underset{\widetilde{L}}{\otimes} (G/G_\bullet)\widetilde{L} & \xrightarrow{\widetilde{\alpha}_0} & (G/G_\bullet)\widetilde{L} \\
{\scriptstyle \mathrm{id}\otimes i}\downarrow & & \downarrow{\scriptstyle i} \\
\widetilde{L}[N] \underset{\widetilde{L}}{\otimes} X\widetilde{L} & \xrightarrow{\widetilde{\alpha}} & X\widetilde{L}
\end{array} \tag{2.20}$$

For every $\sigma G' \in X$, let $u_{\sigma G'} \in X\widetilde{L}$ be the map as defined in (2.1) and, for $\sigma G_\bullet \in G/G_\bullet$, define $u_{\sigma G_\bullet} \in (G/G_\bullet)\widetilde{L}$ in a similar way. Then the map i can be written

$$i(u_{\sigma G_\bullet}) = \sum_{\tau G' \in \pi^{-1}(\sigma G_\bullet)} u_{\tau G'}.$$

Let $n \in N$ and let $\sigma G_\bullet \in G/G_\bullet$, then the action of n on $u_{\sigma G_\bullet}$ viewed as an element of $X\widetilde{L}$ is

$$n\big(i(u_{\sigma G_\bullet})\big) = n\Big(\sum_{\tau G' \in \pi^{-1}(\sigma G_\bullet)} u_{\tau G'}\Big) = \sum_{\tau G' \in \pi^{-1}(\sigma G_\bullet)} u_{n(\tau G')} = \sum_{\tau G' \in n\left(\pi^{-1}(\sigma G_\bullet)\right)} u_{\tau G'}.$$

By (2.20), we also know that $n\big(i(u_{\sigma G_\bullet})\big)$ is equal to some element in the image of $i : (G/G_\bullet)\widetilde{L} \to X\widetilde{L}$:

$$\sum_{\tau G' \in n\left(\pi^{-1}(\sigma G_\bullet)\right)} u_{\tau G'} = i\Big(\sum_{\tau G_\bullet \in G/G_\bullet} x_{\tau G_\bullet} u_{\tau G_\bullet}\Big) = \sum_{\tau G_\bullet \in G/G_\bullet} x_{\tau G_\bullet} \sum_{\mu G' \in \pi^{-1}(\tau G_\bullet)} u_{\mu G'} \quad \text{with } x_{\tau G_\bullet} \in \widetilde{L}.$$

Therefore, one coefficient $x_{\tau G_\bullet}$ must be 1 and the others must be 0. We thus have

$$n\big(\pi^{-1}(\sigma G_\bullet)\big) = \pi^{-1}(\tau G_\bullet) \implies (\pi \circ n)\big(\pi^{-1}(\sigma G_\bullet)\big) = \tau G_\bullet \quad \text{for some } \tau G_\bullet \in G/G_\bullet.$$

Let $\sigma_1 G', \sigma_2 G' \in X$ such that $\pi(\sigma_1 G') = \sigma G_\bullet = \pi(\sigma_2 G')$, then $\sigma_1 G', \sigma_2 G' \in \pi^{-1}(\sigma G_\bullet)$ and hence $(\pi \circ n)(\sigma_1 G') = \tau G_\bullet = (\pi \circ n)(\sigma_2 G')$. This proves that $n \in \mathrm{Perm}_\pi(X)$. Conversely, if L_0 is not H-stable, then $\widetilde{\alpha}_0$ does not map into $(G/G_\bullet)\widetilde{L}$. Therefore, there exists $n \in N$ and $\sigma G_\bullet \in G/G_\bullet$ such that $n\big(\pi^{-1}(\sigma G_\bullet)\big)$ is not of the form $\pi^{-1}(\tau G_\bullet)$ for any $\tau G_\bullet \in G/G_\bullet$, i.e. $n \notin \mathrm{Perm}_\pi(X)$. □

Next, we will characterize H-subextensions with a property on the Greither-Pareigis group $N \subseteq \mathrm{Perm}(X)$.

Definition 2.39. We define the subset

$$\mathcal{N}(L_0) = \big\{n \in N \,|\, n(G_\bullet/G') \subseteq G_\bullet/G'\big\}$$

where $G_\bullet/G'$ is the set of G'-cosets $\sigma G'$ with $\sigma \in G_\bullet$. For ease of notation, we will write $\mathcal{N}$ if there is no ambiguity. Because $\mathcal{N} \subseteq \mathrm{Perm}(X)$, we can easily see that, for every $n \in \mathcal{N}$, we have the equality $n(G_\bullet/G') = G_\bullet/G'$. We can thus see $\mathcal{N}$ as a subset of $\mathrm{Perm}(G_\bullet/G')$.

Lemma 2.40. *The subset $\mathcal{N}$ is a subgroup of N.*

Proof. Let $n_1, n_2 \in \mathcal{N}$, then

$$n_1\big(n_2(G_\bullet/G')\big) = n_1(G_\bullet/G') = G_\bullet/G'.$$

So, $n_1 n_2 \in \mathcal{N}$. If $n \in \mathcal{N}$, we also have

$$n^{-1}(G_\bullet/G') = n^{-1}\big(n(G_\bullet/G')\big) = G_\bullet/G'.$$

So, $n^{-1} \in \mathcal{N}$. □

Remark 2.41. As $N \subseteq \mathrm{Perm}(X)$ is regular, we have $\#\mathcal{N} \leq \#(G_\bullet/G') = [L : L_0]$ with equality if and only if $\mathcal{N} \subseteq \mathrm{Perm}(G_\bullet/G')$ is regular.

Lemma 2.42. *If $N \subseteq Perm_\pi(X)$, then $\mathcal{N} \subseteq Perm(G_\bullet/G')$ is regular.*

Proof. Let $n \in N$ be such that $n(1_G G') \in G_\bullet/G'$ and let $\sigma G' \in G_\bullet/G'$. Then $\pi(\sigma G') = \pi(1_G G')$ and, because $N \subseteq \mathrm{Perm}_\pi(X)$, $(\pi \circ n)(\sigma G') = (\pi \circ n)(1_G G') = 1_G G_\bullet$. Therefore, $n(\sigma G') \in G_\bullet/G'$. We thus have

$$\mathcal{N} = \big\{n \in N \,|\, n(1_G G') \in G_\bullet/G'\big\}.$$

Because $N \subseteq \mathrm{Perm}(X)$ is regular, we can conclude that $\#\mathcal{N} = \#(G_\bullet/G') = [L : L_0]$. By Remark 2.41, $\mathcal{N} \subseteq \mathrm{Perm}(G_\bullet/G')$ is regular. □

The following proposition shows the link between the subgroup $\mathcal{N} \subseteq \mathrm{Perm}(G_\bullet/G')$ and the notion of H-subextensions.

Proposition 2.43. *The intermediate field L_0 is an H-subextension if and only if $\mathcal{N} \subseteq Perm(G_\bullet/G')$ is regular and normalized by $\lambda(G)$.*

To prove this proposition, we will need the following lemma.

Lemma 2.44. *Suppose L_0 is an H-subextension. Define the left ideal two-sided coideal $I = Ann_H(L_0)$ and the Hopf subalgebra $H_0 = {}^{co\,H/I}H$ of H.*

(a) Let $V \subseteq N$ be the subgroup defined in (2.14). For every $f \in V$ and for every $\sigma G' \in X$, $\pi(\sigma G') = (\pi \circ f)(\sigma G')$.

(b) $\mathcal{N} = V$.

Proof. (a) By Lemma 2.32, H_0 acts on L_0. The action $H_0 \otimes L_0 \to L_0$ becomes, after base change,

$$(\widetilde{L} \otimes H_0) \underset{\widetilde{L}}{\otimes} (\widetilde{L} \otimes L_0) \longrightarrow \widetilde{L} \otimes L_0. \tag{2.21}$$

Using the isomorphisms $\widetilde{L} \otimes H_0 = \widetilde{L} \otimes {}^{\mathrm{co}\,H/I}H = {}^{\mathrm{co}\,\widetilde{L}\otimes H/I}(\widetilde{L} \otimes H) \cong \widetilde{L}[V]$ and $\widetilde{L} \otimes L_0 \cong (G/G_\bullet)\widetilde{L}$, (2.21) becomes

$$\widetilde{L}[V] \underset{\widetilde{L}}{\otimes} (G/G_\bullet)\widetilde{L} \longrightarrow (G/G_\bullet)\widetilde{L} : f \otimes u_{\sigma G_\bullet} \longmapsto u_{f(\sigma G_\bullet)} \quad \forall f \in V, \forall \sigma G_\bullet \in G/G_\bullet.$$

By Lemma 2.32, the action of H_0 on L_0 factors through the counit $\epsilon : H_0 \to K$. Therefore, the action of $\widetilde{L}[V]$ on $(G/G_\bullet)\widetilde{L}$ also factors through the counit. In particular, for every $f \in V$ and $\sigma G_\bullet \in G/G_\bullet$, since $\epsilon(f) = 1$ (because $V \subseteq N$ and N is the group of grouplike element of $\widetilde{L}[N]$), we get $f(u_{\sigma G_\bullet}) = u_{\sigma G_\bullet}$. Using the inclusion $i : (G/G_\bullet)\widetilde{L} \subseteq X\widetilde{L}$ defined in (2.19), we obtain

$$\sum_{\tau G' \in \pi^{-1}(\sigma G_\bullet)} u_{f(\tau G')} = \sum_{\tau G' \in \pi^{-1}(\sigma G_\bullet)} u_{\tau G'}.$$

Therefore, $\pi\big(f(\tau G')\big) = \pi(\tau G')$ for every $\tau G' \in G/G'$.

(b) By (a), we know that $f(G_\bullet/G') = G_\bullet/G'$ for all $f \in V$. So $V \subseteq \mathcal{N}$. We also know by Remark 2.41 that $\#\mathcal{N} \leq [L : L_0]$. Using the isomorphism $\widetilde{L} \otimes H/I \cong \widetilde{L}[N/V]$ from Lemma 2.26, we get that $\dim_K H/I = \#(N/V)$. Combining it with the equality $\dim_K I = [L : K] - [L_0 : K]$ from Remark 2.19, we finally get $\#V = [L : L_0]$. Therefore $V = \mathcal{N}$.

□

Proof of Proposition 2.43. Suppose L_0 is an H-subextension. We know by Lemma 2.44 that $\mathcal{N} = V$. Therefore, by Lemma 2.28, $\mathcal{N}$ is normalized by $\lambda(G)$.
Conversely, suppose $\mathcal{N} \subseteq \mathrm{Perm}(G_\bullet/G')$ is regular and normalized by $\lambda(G)$. Then both $\widetilde{L}[N]$ and $\widetilde{L}[\mathcal{N}]$ are $\widetilde{L}\#K[G]$-modules with G-action as in (2.5). By Corollary 1.73, we have the isomorphisms of $\widetilde{L}$-vector spaces

$$\widetilde{L}[N] \cong \widetilde{L} \otimes \widetilde{L}[N]^G \text{ and } \widetilde{L}[\mathcal{N}] \cong \widetilde{L} \otimes \widetilde{L}[\mathcal{N}]^G. \tag{2.22}$$

Moreover, the inclusion $\mathcal{N} \subseteq N$ implies that $\widetilde{L}[\mathcal{N}]^G \subseteq \widetilde{L}[N]^G \cong H$. We can therefore see $\widetilde{L}[\mathcal{N}]^G$ as a Hopf subalgebra of H: $\widetilde{L}[\mathcal{N}]^G \cong H_0 \subseteq H$. As $G_\bullet \subseteq G$, the regular subgroup $\mathcal{N} \subseteq \mathrm{Perm}(G_\bullet/G')$ is also normalized by $\lambda(G_\bullet)$. Theorem 2.6 thus implies that L/L_0 is Hopf-Galois with L_0-Hopf algebra $\widetilde{L}[\mathcal{N}]^{G_\bullet}$ (the base field is L_0 because $\mathrm{Gal}(\widetilde{L}/L_0) = G_\bullet$). By taking the $G_\bullet$-invariants in the second isomorphism of (2.22), we obtain

$$\widetilde{L}[\mathcal{N}]^{G_\bullet} \cong (\widetilde{L} \otimes H_0)^{G_\bullet} = \widetilde{L}^{G_\bullet} \otimes H_0 = L_0 \otimes H_0.$$

Thus, the extension L/L_0 is $L_0 \otimes H_0$-Galois. By Corollary 2.34(a), L_0 is an H-subextension. □

We will now prove that, from a subgroup $M \subseteq N$ normalized by $\lambda(G)$, we can construct an H-subextension. Recall that the action of G on $\widetilde{L}[N]$ is given by

$$G \times \widetilde{L}[N] \longrightarrow \widetilde{L}[N] : (\sigma, x.\nu) \longmapsto \sigma(x.\nu) = \sigma(x).\big(\lambda(\sigma)\nu\lambda(\sigma^{-1})\big).$$

Since G acts on N via conjugation by $\lambda(G)$ and since M is also normalized by $\lambda(G)$, G also acts on $\widetilde{L}[M]$. As $\widetilde{L}[N]$ is an $\widetilde{L}\#K[G]$-module, the inclusion of $\widetilde{L}$-Hopf algebras $\widetilde{L}[M] \subseteq \widetilde{L}[N]$ is also an injective morphism of $\widetilde{L}\#K[G]$-modules. Therefore, we can use Corollary 1.73 to restrict it to an inclusion of K-Hopf algebras $\big(\widetilde{L}[M]\big)^G \subseteq \big(\widetilde{L}[N]\big)^G \cong H$. We can thus define the map

$$\mathcal{H} : \big\{M \subseteq N \text{ subgroup normalized by } \lambda(G)\big\} \longrightarrow \big\{H_0 \subseteq H \text{ Hopf subalgebra}\big\} :$$

$$M \longmapsto \beta_H^{-1}\big(\big(\widetilde{L}[M]\big)^G\big)$$

where $\beta_H : \widetilde{L} \otimes H \xrightarrow{\cong} \widetilde{L}[N]$ is the isomorphism from (2.4).

We can now formulate the following correspondence theorem, which is the translation of the Hopf-Galois correspondence (Theorem 2.31) to the language of Greither-Pareigis groups.

Theorem 2.45. *Let L/K be a finite separable H-Galois extension. Then the maps*

$$\big\{\mathcal{N} \subseteq N \text{ subgroup normalized by } \lambda(G)\big\} \underset{\mathcal{N}}{\overset{Fix \circ \mathcal{H}}{\rightleftarrows}} \big\{L/L_0/K \ H\text{-subextension}\big\}$$

are inverse bijections. Moreover, the above correspondence restricts to the following inverse bijections:

$$\big\{\mathcal{N} \subseteq N \text{ normal subgroup normalized by } \lambda(G)\big\} \underset{\mathcal{N}}{\overset{Fix \circ \mathcal{H}}{\rightleftarrows}} \big\{L/L_0/K \ H\text{-normal}\big\}$$

Proof. We already know that these maps are well-defined. Let $M \subseteq N$ be a subgroup normalized by $\lambda(G)$, then the set of G-invariants $\big(\widetilde{L}[M]\big)^G$ is a Hopf subalgebra of $\big(\widetilde{L}[N]\big)^G$. Let $H_0 = \beta_H^{-1}\big(\big(\widetilde{L}[M]\big)^G\big)$ be the associated Hopf subalgebra of $H = \beta_H^{-1}\big(\big(\widetilde{L}[N]\big)^G\big)$. Let $I = \psi(H_0)$ be its associated left ideal two-sided coideal of H as in Definition 1.56. We know by Proposition 2.25 that $L_0 = L^I$ is an H-subextension. Define V as in (2.14), then

$$\widetilde{L}[V] = {}^{\mathrm{co}\,\widetilde{L}\otimes H/I}(\widetilde{L}[N]) = \beta_H\big({}^{\mathrm{co}\,\widetilde{L}\otimes H/I}(\widetilde{L}\otimes H)\big) = \beta_H\big(\widetilde{L}\otimes {}^{\mathrm{co}\,H/I}H\big) = \beta_H\big(\widetilde{L}\otimes H_0\big).$$

Using that $H_0 = \beta_H^{-1}\big(\big(\widetilde{L}[M]\big)^G\big)$ we get

$$\beta_H\big(\widetilde{L}\otimes H_0\big) = \widetilde{L}[M].$$

Therefore, $V = M$. To prove the other half, suppose L_0 is an H-subextension. Let $I = \mathrm{Ann}_H(L_0)$ be the associated left ideal two-sided coideal of H and let V be defined as in (2.14). Consider the Hopf subalgebra $\big(\widetilde{L}[V]\big)^G$ of H, we want to prove that $L^{(\widetilde{L}[V])^G} = L_0$. Computing $\mathrm{HKer}\big(\widetilde{\pi} : \widetilde{L}[N] \twoheadrightarrow \widetilde{L}\otimes H/I\big)$ as in (2.13), we obtain

$$\widetilde{L}[V] = \mathrm{HKer}(\widetilde{\pi}) = {}^{\mathrm{co}\,\widetilde{L}\otimes H/I}\widetilde{L}[N] \cong {}^{\mathrm{co}\,\widetilde{L}\otimes H/I}(\widetilde{L}\otimes H) = \widetilde{L}\otimes {}^{\mathrm{co}\,H/I}H,$$

which is an isomorphism of $\widetilde{L}$-algebra and G-modules. Taking the G-invariants yields

$$\big(\widetilde{L}[V]\big)^G \cong \widetilde{L}^G \otimes {}^{\mathrm{co}\,H/I}H = {}^{\mathrm{co}\,H/I}H.$$

So, $L^{(\widetilde{L}[V])^G} = L^{{}^{\mathrm{co}\,H/I}H} = L_0$.
By Remark 2.27, L_0 is H-normal if and only if $V = M$ is a normal subgroup of N. □

2.7 Opposite Hopf-Galois structures

The main result of this section is to show that for every finite separable H-Galois extension L/K, there exists a Hopf algebra $H^\dagger$ such that

1. L/K is $H^\dagger$-Galois;
2. L_0 is H-stable if and only if L_0 is an $H^\dagger$-subextension;
3. L_0 is an H-subextension if and only if L_0 is $H^\dagger$-stable;
4. $H^{\dagger\dagger} \cong H$ and the actions of H and $H^{\dagger\dagger}$ on L coincide.

Definition 2.46. Let G be any group. We define the *centralizer* of a subset $N \subseteq G$ as

$$\mathrm{Cent}_G(N) = \big\{ g \in G \,|\, g\nu = \nu g \quad \forall \nu \in N \big\}.$$

It is easy to check that $\mathrm{Cent}_G(N)$ is a subgroup of G. If the inclusion $N \subseteq G$ is clear, we will simply write $\mathrm{Cent}(N)$.

Let $N \subseteq \mathrm{Perm}(X)$ be the Greither-Pareigis group associated with the H-Galois extension L/K (as in Theorem 2.6). The following lemmas, due to Greither and Pareigis [GP87], show that $\mathrm{Cent}(N) \subseteq \mathrm{Perm}(X)$ is regular and normalized by $\lambda(G)$. This subgroup thus defines another Hopf-Galois structure on L/K.

Let $n \in \mathbb{N}_0$, S_n be the permutation group of $\{1, 2, ..., n\}$ and $N \subseteq S_n$ be a regular subgroup. Note that the regularity of N means that for every $i \in \{1, ..., n\}$, there is a unique permutation $\nu_i \in N$ such that $\nu_i(1) = i$. We can thus write $N = \big\{ \nu_i \,|\, i \in \{1, ..., n\} \big\}$. Also note that, since N is a subgroup, it contains the identity map id which maps 1 to 1. Therefore, $\nu_1 = \mathrm{id}$.

Lemma 2.47. *[GP87, Lem. 2.4.2] With the above notation, for every $f \in S_n$ we define the map*

$$\varphi_f : \{1, ..., n\} \longrightarrow \{1, ..., n\} : i \longmapsto \nu_i\big(f(1)\big).$$

Then $\varphi_f \in S_n$ and $\mathrm{Cent}(N) = \big\{ \varphi_\nu \,|\, \nu \in N \big\}$. Moreover, $\mathrm{Cent}(N) \subseteq S_n$ is a regular subgroup and $\mathrm{Cent}(N) \cong N^{opp}$ (where N^{opp} is the opposite group whose underlying set is N and with new operation $*$ defined by $\nu * \nu' = \nu'\nu$).

Proof. Let $f \in S_n$, we will first prove that $\varphi_f \in S_n$. Suppose $\varphi_f(i) = \varphi_f(j)$ for $i, j \in \{1, ..., n\}$, then $\nu_i\big(f(1)\big) = \nu_j\big(f(1)\big)$ so ν_i and ν_j send $f(1)$ to the same element. Because $N \subseteq S_n$ is regular, we must have $\nu_i = \nu_j$ and thus $i = j$. This proves that φ_f is a permutation of $\{1, ..., n\}$: $\varphi_f \in S_n$.
Let $\varphi \in \mathrm{Cent}(N)$. For every $i \in \{1, ..., n\}$ we have

$$\varphi(i) = \varphi\nu_i(1) = \nu_i\varphi(1) = \nu_i\nu_{\varphi(1)}(1) = \varphi_{\nu_{\varphi(1)}}(i).$$

So, $\varphi = \varphi_{\nu_{\varphi(1)}}$ and $\mathrm{Cent}(N) \subseteq \{\varphi_\nu \,|\, \nu \in N\}$.
Conversely, let $\nu \in N$ and $\varphi_\nu \in S_n$, we will prove that $\nu_i\varphi_\nu = \varphi_\nu\nu_i$ for every $\nu_i \in N$. By definition of ν_i, we have $\nu_i\nu_j(1) = \nu_{\nu_i(j)}(1)$ for every $j \in \{1, ..., n\}$, and since N is regular, we find that $\nu_i\nu_j = \nu_{\nu_i(j)}$. We thus get

$$\nu_i\varphi_\nu(j) = \nu_i\nu_j\nu(1) = \nu_{\nu_i(j)}\nu(1) = \varphi_\nu\nu_i(j).$$

As this equality holds for every $j \in \{1, ..., n\}$, we obtain $\nu_i\varphi_\nu = \varphi_\nu\nu_i$. We thus have $\{\varphi_\nu \,|\, \nu \in N\} \subseteq \mathrm{Cent}(N)$.
To prove that $\mathrm{Cent}(N) \subseteq S_n$ is a regular subgroup, we will first prove that the subgroup is transitive. Indeed, if $i, j \in \{1, ..., n\}$ then define $k = \nu_i^{-1}(j)$. We thus have $\varphi_{\nu_k}(i) = \nu_i\nu_k(1) = \nu_i(k) = j$. We also have $\#\mathrm{Cent}(N) \leq \#N = n$, so $\mathrm{Cent}(N) \subseteq S_n$ is regular. Finally, let $\nu_i, \nu_j \in N$, we will prove that $\varphi_{\nu_i}\varphi_{\nu_j} = \varphi_{\nu_j\nu_i}$. Because $\nu_1 = \mathrm{id}$, $\varphi_f(1) = \nu_1 f(1) = f(1)$. We thus obtain

$$\varphi_{\nu_i}\varphi_{\nu_j}(1) = \varphi_{\nu_i}\nu_j(1) = \varphi_{\nu_i}(j) = \nu_j\nu_i(1) = \varphi_{\nu_j\nu_i}(1).$$

As both $\varphi_{\nu_i}\varphi_{\nu_j}$ and $\varphi_{\nu_j\nu_i}$ belong to the regular subgroup $N \subseteq S_n$, we have $\varphi_{\nu_i}\varphi_{\nu_j} = \varphi_{\nu_j\nu_i}$. □

Lemma 2.48. *[GP87, Thm. 2.5(b)] Let $N \subseteq S_n$ be a regular subgroup and let $G \subseteq S_n$ be a subgroup such that N is normalized by G. Then Cent(N) is also normalized by G.*

Proof. Let $\varphi_\nu \in \mathrm{Cent}(N)$ and let $g \in G$. As $\mathrm{Cent}(N)$ is regular, we can define φ to be the unique element in $\mathrm{Cent}(N)$ such that $g\varphi(1) = 1$. We claim that $\varphi_{g\nu g^{-1}} = g\varphi\varphi_\nu\varphi^{-1}g^{-1}$. We thus obtain $g^{-1}\varphi_{g\nu g^{-1}}g = \varphi\varphi_\nu\varphi^{-1} \in \mathrm{Cent}(N)$. Because N is normalized by G, $g\nu g^{-1} \in N$. Moreover, if we fix $g \in G$ and if we let ν run through all elements of N, then $g\nu g^{-1}$ runs through all elements of N. Therefore, $g^{-1}\varphi_\nu g \in \mathrm{Cent}(N)$ for every $g \in G$ and every $\nu \in N$.
To prove the claim, let $i \in \{1, ..., n\}$, then we get

$$g\varphi\varphi_\nu\varphi^{-1}g^{-1}(i) = g\varphi\nu_{\varphi^{-1}g^{-1}(i)}\nu(1)$$

and

$$\varphi_{g\nu g^{-1}}(i) = \nu_i g\nu g^{-1}(1) = \nu_i g\varphi\nu\varphi^{-1}g^{-1}(1) = \nu_i g\varphi\nu(1)$$

where the second equality comes from $\nu = \varphi\nu\varphi^{-1}$ (because $\varphi \in \mathrm{Cent}(N)$ commutes with $\nu \in N$) and the third equality comes from $g\varphi(1) = 1 = \varphi^{-1}g^{-1}(1)$. We will now show that $g\varphi\nu_{\varphi^{-1}g^{-1}(i)} = \nu_i g\varphi$, which is equivalent to $\nu_{\varphi^{-1}g^{-1}(i)} = \varphi^{-1}g^{-1}\nu_i g\varphi$. Both

terms belong to N (for the right one, $g^{-1}\nu_i g \in N$ because N is normalized by G and $\varphi^{-1}g^{-1}\nu_i g\varphi \in N$ because $\varphi \in \mathrm{Cent}(N)$ centralizes N), so it is enough to prove that they coincide at 1:

$$\varphi^{-1}g^{-1}\nu_i g\varphi(1) = \varphi^{-1}g^{-1}\nu_i(1) = \varphi^{-1}g^{-1}(i) = \nu_{\varphi^{-1}g^{-1}(i)}(1).$$

This finishes the proof □

Definition 2.49. Let L/K be a finite separable H-Galois extension with Greither-Pareigis group $N \subseteq \mathrm{Perm}(X)$. Then $\mathrm{Cent}(N) \subseteq \mathrm{Perm}(X)$ is regular by Lemma 2.47 and normalized by $\lambda(G)$ by Lemma 2.48. By Theorem 2.6, we can construct a Hopf algebra such that L/K is Hopf-Galois with Greither-Pareigis group $\mathrm{Cent}(N)$. We call this the *opposite Hopf-Galois structure* and we will denote its associated Hopf algebra $H^\dagger := \left(\widetilde{L}[\mathrm{Cent}(N)]\right)^G$ (see Lemma 2.9(c)).

Corollary 2.50. *Let L/K be a finite separable H-Galois extension, then $(H^\dagger)^\dagger \cong H$ and the action of H and $H^{\dagger\dagger}$ on L coincide.*

Proof. We will prove that $\mathrm{Cent}(\mathrm{Cent}(N)) = N$. By definition, we have the inclusion $N \subseteq \mathrm{Cent}(\mathrm{Cent}(N))$. Furthermore, this inclusion is an equality because $\#\mathrm{Cent}(\mathrm{Cent}(N)) = \#\mathrm{Cent}(N) = \#N$. □

We will now prove the main result of this section.

Theorem 2.51. *Let L/K be a finite separable H-Galois extension and let $H^\dagger$ be the Hopf algebra associated with the opposite Hopf-Galois structure. Let L_0 be an intermediate field, then*

(a) L_0 is H-stable if and only if L_0 is an $H^\dagger$-subextension;

(b) L_0 is an H-subextension if and only if L_0 is $H^\dagger$-stable.

Proof. Similarly to what has been done in Lemmas 2.47 and 2.48, for $\sigma G' \in X$ we define $\nu_{\sigma G'} \in N$ to be the unique element in N such that $\nu_{\sigma G'}(1_G G') = \sigma G'$ and for $f \in \mathrm{Perm}(X)$ we define $\varphi_f \in \mathrm{Perm}(X)$ by $\varphi_f(\sigma G') = \nu_{\sigma G'} f(1_G G')$ for all $\sigma G' \in X$. We have $N = \left\{\nu_{\sigma G'} \,|\, \sigma G' \in X\right\}$ and $\nu_{1_G G'} = \mathrm{id}$. Recall from Proposition 2.38 that L_0 is H-stable if and only if

$$N \subseteq \mathrm{Perm}_\pi(X) = \left\{f \in \mathrm{Perm}(X) \,|\, \pi(\sigma G') = \pi(\tau G') \Rightarrow (\pi \circ f)(\sigma G') = (\pi \circ f)(\tau G')\right\}$$

where $\pi : X \longrightarrow G/G_\bullet : \sigma G' \longmapsto \sigma G_\bullet$ is the natural projection. Also recall from Proposition 2.43 that L_0 is an H-subextension if and only if the subgroup

$$\mathcal{N} = \big\{\nu \in N \,|\, \nu(G_\bullet/G') \subseteq G_\bullet/G'\big\} \subseteq \mathrm{Perm}(G_\bullet/G')$$

is regular and normalized by $\lambda(G)$.

We will first suppose that L_0 is H-stable and prove that L_0 is an $H^\dagger$-subextension. We want to prove that the subgroup

$$\mathrm{Cent}(N)_0 = \big\{\varphi_\nu \in \mathrm{Cent}(N) \,|\, \varphi_\nu(G_\bullet/G') \subseteq G_\bullet/G'\big\} \subseteq \mathrm{Perm}(G_\bullet/G')$$

is regular and normalized by $\lambda(G)$. We will first prove the following statement:

$$\forall \sigma G' \in G_\bullet/G', \forall \tau G' \in X: \quad \tau G' \in G_\bullet/G' \Longleftrightarrow \nu_{\sigma G'}(\tau G') \in G_\bullet/G'. \tag{2.23}$$

If $\sigma G', \tau G' \in G_\bullet/G'$, then $\pi(\tau G') = 1_G G_\bullet = \pi(1_G G')$. Because $N \subseteq \mathrm{Perm}_\pi(X)$ we get $\pi\big(\nu(\tau G')\big) = \pi\big(\nu(1_G G')\big)$ for all $\nu \in N$. In particular, for $\nu = \nu_{\sigma G'}$ we obtain $\pi\big(\nu_{\sigma G'}(\tau G')\big) = \pi(\sigma G') = 1_G G_\bullet$ and therefore $\nu_{\sigma G'}(\tau G') \in G_\bullet/G'$. Conversely, if $\sigma G', \nu_{\sigma G'}(\tau G') \in G_\bullet/G'$, then $\pi\big(\nu_{\sigma G'}(\tau G')\big) = 1_G G_\bullet = \pi(\sigma G') = \pi\big(\nu_{\sigma G'}(1_G G')\big)$. Again, because $N \subseteq \mathrm{Perm}_\pi(X)$, we get $\pi\big(\nu\nu_{\sigma G'}(\tau G')\big) = \pi\big(\nu\nu_{\sigma G'}(1_G G')\big)$ for all $\nu \in N$. In particular, for $\nu = \nu_{\sigma G'}^{-1}$ we obtain $\pi(\tau G') = \pi(1_G G') = 1_G G_\bullet$ and therefore $\tau G' \in G_\bullet/G'$. This proves (2.23).
Next, we will prove that

$$\mathrm{Cent}(N)_0 = \big\{\varphi_\nu \in \mathrm{Cent}(N) \,|\, \nu \in \mathcal{N}\big\} \subseteq \mathrm{Perm}(G_\bullet/G'). \tag{2.24}$$

Let $\nu \in N$ and suppose that $\varphi_\nu(G_\bullet/G') \subseteq G_\bullet/G'$. Then for all $\sigma G' \in G_\bullet/G'$ we have $\varphi_\nu(\sigma G') = \nu_{\sigma G'}\nu(1_G G') \in G_\bullet/G'$. By (2.23) we have $\nu(1_G G') \in G_\bullet/G'$. As $\nu \in N \subseteq \mathrm{Perm}_\pi(X)$ and $\pi(\sigma G') = 1_G G_\bullet = \pi(1_G G')$, we obtain that $\pi\big(\nu(\sigma G')\big) = \pi\big(\nu(1_G G')\big) = 1_G G_\bullet$. Thus, $\nu(\sigma G') \in G_\bullet/G'$ for all $\sigma G' \in G_\bullet/G'$, i.e. $\nu(G_\bullet/G') \subseteq G_\bullet/G'$, so $\nu \in \mathcal{N}$. Conversely, let $\nu \in N$ and suppose that $\nu(G_\bullet/G') \subseteq G_\bullet/G'$. Then for all $\sigma G' \in G_\bullet/G'$ we have $\nu(\sigma G') \subseteq G_\bullet/G'$. As $\nu \in N \subseteq \mathrm{Perm}_\pi(X)$ and $\pi(\sigma G') = 1_G G_\bullet = \pi(1_G G')$, we obtain that $1_G G_\bullet = \pi\big(\nu(\sigma G')\big) = \pi\big(\nu(1_G G')\big)$. Thus, $\nu(1_G G') \in G_\bullet/G'$ and by (2.23) we have $\varphi_\nu(\sigma G') = \nu_{\sigma G'}\nu(1_G G') \in G_\bullet/G'$ for all $\sigma G' \in G_\bullet/G'$, i.e. $\varphi_\nu(G_\bullet/G') \subseteq G_\bullet/G'$. This proves (2.24).
We thus have $\#\mathrm{Cent}(N)_0 = \#\mathcal{N} = [L : L_0]$ (the second equality comes from Lemma 2.42 and Remark 2.41) and therefore, by Remark 2.41 again, $\mathrm{Cent}(N)_0 \subseteq \mathrm{Perm}(G_\bullet/G')$ is regular.
To prove that $\mathrm{Cent}(N)_0$ is normalized by $\lambda(G)$, we must show that $\lambda(g^{-1})\varphi_\nu\lambda(g) \in$

$\mathrm{Cent}(N)_0$ for all $g \in G$, $\nu \in \mathcal{N}$. By Lemma 2.48, we already know that $\mathrm{Cent}(N)$ is normalized by $\lambda(G)$. As $\mathrm{Cent}(N)_0 \subseteq \mathrm{Perm}(G_\bullet/G')$ is regular, it is enough to show that $\lambda(g^{-1})\varphi_\nu\lambda(g)(1_G G') \in G_\bullet/G'$. Consider the subset

$$\pi^{-1}(gG_\bullet) = \left\{ g\sigma G' \in X \,|\, \sigma \in G_\bullet \right\} \tag{2.25}$$

whose elements are the G'-cosets which are sent to the $G_\bullet$-coset $gG_\bullet$. We can easily see that $\pi^{-1}(1_G G_\bullet) = G_\bullet/G'$ and more generally that $\pi^{-1}(gG_\bullet) = \lambda(g)\big(\pi^{-1}(1_G G_\bullet)\big)$. Let $\nu \in \mathcal{N}$, $g \in G$ and $\sigma \in G_\bullet$. As $\nu_{g\sigma G} \in N \subseteq \mathrm{Perm}_\pi(X)$ and $\pi\big(\nu(1_G G')\big) = 1_G G_\bullet = \pi(1_G G')$, we obtain $\pi\big(\nu_{g\sigma G'}\nu(1_G G')\big) = \pi\big(\nu_{g\sigma G'}(1_G G')\big) = \pi(g\sigma G') = gG_\bullet$. Taking π^{-1} yields $\varphi_\nu(g\sigma G') = \nu_{g\sigma G'}\nu(1_G G') \in \pi^{-1}(gG_\bullet)$ for all $\nu \in \mathcal{N}, g \in G, \sigma \in G_\bullet$, which can be written

$$\varphi_\nu\big(\pi^{-1}(gG_\bullet)\big) \subseteq \pi^{-1}(gG_\bullet) \quad \forall \nu \in \mathcal{N},\, g \in G.$$

Putting everything together, we get

$$\begin{aligned}
\lambda(g^{-1})\varphi_\nu\lambda(g)(1_G G') &= \lambda(g^{-1})\varphi_\nu(gG') \\
&\in \lambda(g^{-1})\varphi_\nu\big(\pi^{-1}(gG_\bullet)\big) \\
&\subseteq \lambda(g^{-1})\pi^{-1}(gG_\bullet) \\
&= \lambda(g^{-1})\lambda(g)\big(\pi^{-1}(1_G G_\bullet)\big) \\
&= \pi^{-1}(1_G G_\bullet) = G_\bullet/G'.
\end{aligned}$$

We have proved that, if L_0 is H-stable, then the subgroup $\mathrm{Cent}(N)_0 \subseteq \mathrm{Perm}(G_\bullet/G')$ is regular and normalized by $\lambda(G)$. This means that, for the opposite Hopf-Galois structure $H^\dagger$, L_0 is an $H^\dagger$-subextension.

We now suppose that L_0 is an H-subextension and prove that L_0 is $H^\dagger$-stable. We want to prove that $\mathrm{Cent}(N) \subseteq \mathrm{Perm}_\pi(X)$, i.e. for all $\sigma G', \tau G' \in X$:

$$\pi(\sigma G') = \pi(\tau G') \Longrightarrow (\pi \circ \varphi_\nu)(\sigma G') = (\pi \circ \varphi_\nu)(\tau G') \quad \forall \nu \in N.$$

The subgroup $\mathcal{N} \subseteq \mathrm{Perm}(X)$ is normalized by $\lambda(G)$, we have $\lambda(g^{-1})\nu\lambda(g) \in \mathcal{N}$ for all $g \in G$, $\nu \in \mathcal{N}$. Therefore

$$\lambda(g^{-1})\nu\lambda(g)(G_\bullet/G') \subseteq G_\bullet/G' \iff \nu\lambda(g)(G_\bullet/G') \subseteq \lambda(g)(G_\bullet/G').$$

Using (2.25), we can write

$$\nu(gG') \in \nu\big(\pi^{-1}(gG_\bullet)\big) \subseteq \pi^{-1}(gG_\bullet) \tag{2.26}$$

$$\implies \pi\big(\nu(gG')\big) \in \pi\pi^{-1}(gG_\bullet). \tag{2.27}$$

Note that $\pi\pi^{-1}(gG_\bullet)$ is a singleton whose unique element is $gG_\bullet = \pi(gG')$, we therefore obtain

$$\pi\big(\nu(gG')\big) = \pi(gG') \quad \forall \nu \in \mathcal{N},\, \forall g \in G. \tag{2.28}$$

The subgroup $\mathcal{N} \subseteq \mathrm{Perm}(G_\bullet/G')$ is also regular, so $\#\mathcal{N} = \#(G_\bullet/G') = \#\big(\pi^{-1}(gG_\bullet)\big)$ for any $g \in G$. Together with (2.26), this means that for every $hG' \in \pi^{-1}(gG_\bullet)$, there is a unique $\nu \in \mathcal{N}$ such that $\nu(gG') = hG'$. We can slightly change the formulation to obtain the following result:

$$\forall \sigma G', \tau G' \in X : \pi(\sigma G') = \pi(\tau G') \implies \exists! \nu \in \mathcal{N} : \nu(\sigma G') = \tau G'. \tag{2.29}$$

We are now ready to show that $\mathrm{Cent}(N) \subseteq \mathrm{Perm}_\pi(X)$. Let $\sigma G', \tau G' \in X$ such that $\pi(\sigma G') = \pi(\tau G')$. By (2.29), there is a unique $\nu \in \mathcal{N}$ such that $\nu(\sigma G') = \tau G'$. We also have that $\nu\nu_{\sigma G'}(1_G G') = \nu_{\tau G'}(1_G G')$. As both $\nu\nu_{\sigma G'}$ and $\nu_{\tau G'}$ belong to $N \subseteq \mathrm{Perm}(X)$, which is regular, we obtain the equality

$$\nu\nu_{\sigma G'} = \nu_{\tau G'}. \tag{2.30}$$

We can now conclude: for all $\mu \in N$ we get

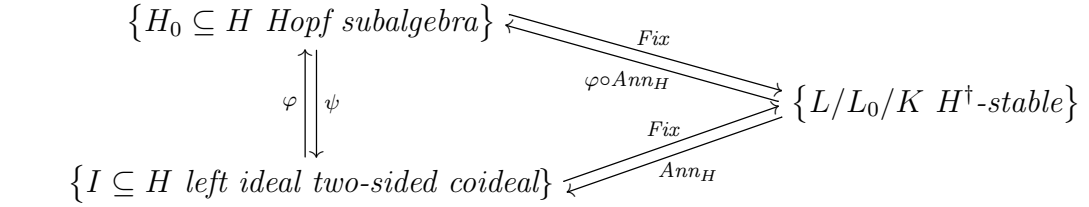
$$\begin{aligned}
\pi\big(\varphi_\mu(\sigma G')\big) &= \pi\big(\nu_{\sigma G'}\mu(1_G G')\big) \\
&= \pi\big(\nu\nu_{\sigma G'}\mu(1_G G')\big) \quad \text{by (2.28)} \\
&= \pi\big(\nu_{\tau G'}\mu(1_G G')\big) \quad \text{by (2.30)} \\
&= \pi\big(\varphi_\mu(\tau G')\big).
\end{aligned}$$

This proves that $\mathrm{Cent}(N) \subseteq \mathrm{Perm}_\pi(X)$. So, for the opposite structure $H^\dagger$, L_0 is $H^\dagger$-stable.

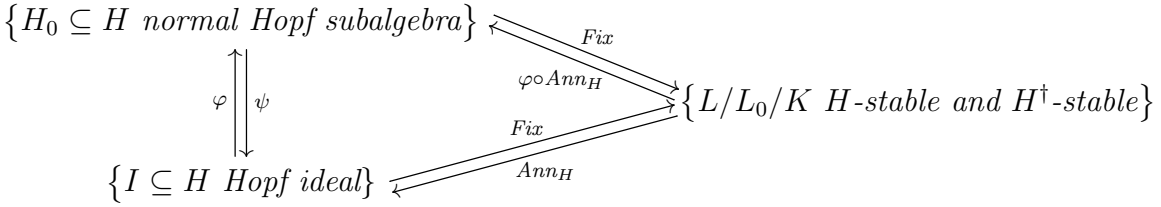
To finish the proof, just recall Corollary 2.50: H and $H^{\dagger\dagger}$ defines the same Hopf-Galois structure. Therefore, if L_0 is an $H^\dagger$-subextension, then L_0 is $H^{\dagger\dagger}$-stable, hence H-stable; if L_0 is $H^\dagger$-stable, then L_0 is an $H^{\dagger\dagger}$-subextension, hence an H-subextension. □

We can now reformulate the correspondence theorem 2.31 in terms of the Hopf-Galois structure given by the Greither-Pareigis group $\mathrm{Cent}(N)$.

Corollary 2.52. *Let L/K be a finite separable H-Galois extension with Greither-Pareigis group $N \subseteq Perm(G/G')$ and let $H^\dagger = \big(\widetilde{L}[N^{opp}]\big)^G$ be the Hopf algebra associated with the group $Cent(N)$. Then the maps*



are inverse bijections. Moreover, the above correspondence restricts to the following inverse bijections:



2.8 Intersection, compositum and compatible Hopf-Galois extensions

In this section, we study the intersection and the compositum of H-subextensions and of H-stable extensions. We also introduce the notion of compatibility between two Hopf-Galois extensions.

Lemma 2.53. *Let L/K be a finite field extension and let L_1 and L_2 be two intermediate fields.*

(a) $End_{L_1L_2}(L) = End_{L_1}(L) \cap End_{L_2}(L)$.

(b) If $End_{L_1}(L) = End_{L_2}(L)$, *then* $L_1 = L_2$.

Proof. (a) Let $f \in \mathrm{End}_K(L)$, then f is L_1L_2-linear if and only if f is both L_1-linear and L_2-linear.

(b) Using (a), we get that $\mathrm{End}_{L_1L_2}(L) = \mathrm{End}_{L_1}(L) = \mathrm{End}_{L_2}(L)$. Furthermore, for any intermediate field E of L/K we have $\dim_K\big(\mathrm{End}_E(L)\big) = [L : K][L : E]$. It thus follows that $[L_1L_2 : K] = [L_1 : K] = [L_2 : K]$. Since $L_1 \subseteq L_1L_2 \supseteq L_2$, it follows that $L_1 = L_1L_2 = L_2$.

□

Let L/K be a finite separable H-Galois extension. We can associate with each H-subextension a left ideal two-sided coideal (Definition 2.14) and a Hopf subalgebra (Definition 1.56). Recall from Lemma 1.35 that the sum of left ideals two-sided coideals of H is again a left ideal two-sided coideal of H and from Lemma 1.36 that the intersection of Hopf subalgebras of H is again a Hopf subalgebra of H. By the previous results, both the sum of left ideals two-sided coideals of H and the intersections of Hopf subalgebras of H are associated with H-subextensions.

Proposition 2.54. *Let L/K be a finite separable H-Galois extension. Let $L_1 = L^{I_1} = L^{H_1}$ and $L_2 = L^{I_1} = L^{H_2}$ be H-subextensions corresponding to left ideals two-sided coideals I_1, I_2 and Hopf subalgebras H_1, H_2 respectively.*

(a) The compositum L_1L_2 is an H-subextension and $L_1L_2 = L^{H_1 \cap H_2}$. If L_1 and L_2 are H-normal, then so is L_1L_2.

(b) The intersection $L_1 \cap L_2$ is an H-subextension and $L_1 \cap L_2 = L^{I_1+I_2}$. If L_1 and L_2 are H-normal, then so is $L_1 \cap L_2$.

Proof. (a) By Proposition 2.33, we have the isomorphisms

$$\underline{\mathrm{can}}_{L/L_i} : L \otimes H_i \longrightarrow \mathrm{End}_{L_i}(L) \quad \text{for } i = 1, 2.$$

Taking intersections on both sides and using Lemma 2.53(a) we obtain a canonical isomorphism

$$L \otimes (H_1 \cap H_2) \longrightarrow \mathrm{End}_{L_1}(L) \cap \mathrm{End}_{L_2}(L) = \mathrm{End}_{L_1L_2}(L).$$

As $H_1 \cap H_2$ is a Hopf subalgebra (Lemma 1.36), it corresponds to a unique H-subextension $L_3 = L^{H_1 \cap H_2}$ with canonical isomorphism $L \otimes (H_1 \cap H_2) \cong \mathrm{End}_{L_3}(L)$. By Lemma 2.53(b), $L_3 = L_1L_2$.
Suppose L_1 and L_2 are H-normal. Then H_1 and H_2 are normal Hopf subalgebra. By Lemma 1.36, $H_1 \cap H_2$ is also a normal Hopf algebra. Therefore, $L_3 = L^{H_1 \cap H_2}$ is H-normal.

(b) By Lemma 1.35, $I_1 + I_2$ is a left ideal two-sided coideal (resp. Hopf ideal) if so are I_1 and I_2. Moreover, it is easy to see that $L^{I_1+I_2} = L^{I_1} \cap L^{I_2} = L_1 \cap L_2$. If L_1 and L_2 are H-subextensions (resp. H-normal), the intermediate field $L_1 \cap L_2$ is therefore an H-subextension (resp. H-normal) with associated left ideal two-sided coideal (resp. Hopf ideal) $I_1 + I_2$.

□

We now introduce the notion of weakly compatible Hopf-Galois extensions which, roughly speaking, are Hopf-Galois extensions with the same action on their intersection.

Definition 2.55. Let L_1/K be a finite separable H_1-Galois extension and L_2/K be a finite separable H_2-Galois extension. Let $E = L_1 \cap L_2$ and let $\pi_i : H_i \longrightarrow\!\!\!\!\!\rightarrow H_i/\mathrm{Ann}_{H_i}(E)$ be the natural projection for $i \in \{1, 2\}$. Then we say that these two Hopf-Galois extensions are *weakly compatible* (with respect to the structures given by H_1 and H_2) if the following two statements hold:

1. E is both H_1-normal and H_2-normal,
2. there exists an isomorphism of Hopf algebras $\psi : H_1/\mathrm{Ann}_{H_1}(E) \xrightarrow{\cong} H_2/\mathrm{Ann}_{H_2}(E)$ such that for all $h_1 \in H_1$, $h_2 \in H_2$ and $x \in E$:

$$h_1 \cdot x = \psi\big(\pi_1(h_1)\big) \cdot x \ \text{ and } \ h_2 \cdot x = \psi^{-1}\big(\pi_2(h_2)\big) \cdot x.$$

Proposition 2.56. *Let L_1/K be a finite separable H_1-Galois extension and L_2/K be a finite separable H_2-Galois extension. Suppose they are weakly compatible. Let $E = L_1 \cap L_2$, then there exists a Hopf algebra H such that $(L_1 \otimes_E L_2)/K$ is H-Galois.*

Proof. Let $L = L_1 \otimes_E L_2$. Consider the pullback in the category of K-Hopf algebras of the diagram

$$\begin{array}{ccccc} H_1 & & & & H_2 \\ & \searrow^{\pi_1} & & \swarrow_{\pi_2} & \\ & & H_1/\mathrm{Ann}_{H_1}(E) \cong H_2/\mathrm{Ann}_{H_2}(E) & & \end{array}$$

We will write $H_1/\mathrm{Ann}_{H_1}(E) \cong \overline{H} \cong H_2/\mathrm{Ann}_{H_2}(E)$ and consider

$$p_i : H_i \longrightarrow\!\!\!\!\!\rightarrow H_i/\mathrm{Ann}_{H_i}(L_i) \xrightarrow{\cong} \!\!\!\!\!\rightarrow \overline{H}.$$

Since the Hopf algebras are cocommutative, the pullback has the following explicit description:

$$H = \big\{h^1 \otimes h^2 \in H_1 \otimes H_2 \,|\, h^1_{(1)} \otimes p_1(h^1_{(2)}) \otimes h^2 = h^1 \otimes p_2(h^2_{(1)}) \otimes h^2_{(2)} \in H_1 \otimes \overline{H} \otimes H_2\big\}.$$

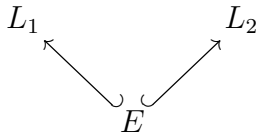
Note that it is also the pullback in the category of K-coalgebras. There is also a natural action of H on L given by

$$(h^1 \otimes h^2) \cdot (x \otimes y) = (h^1 \cdot x) \otimes (h^2 \cdot y) \quad \forall h^1 \otimes h^2 \in H, \forall x \in L_1, \forall y \in L_2$$

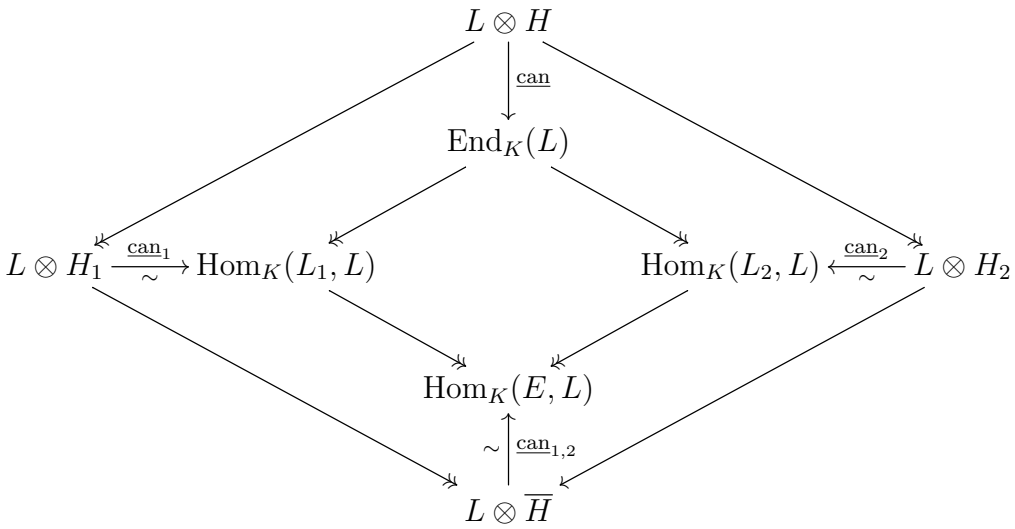
and natural projections

$$H \twoheadrightarrow H_1 : h^1 \otimes h^2 \longmapsto h^1\epsilon_2(h^2) \quad \text{and} \quad H \twoheadrightarrow H_2 : h^1 \otimes h^2 \longmapsto \epsilon_1(h^1)h^2.$$

The pushout in the category of rings of the diagram



is given by the tensor product $L_1 \otimes_E L_2 = L$. Using the contravariant functor $\mathrm{Hom}_K(-, L)$, we obtain a pullback in the category of K-coalgebras. Since $L_1 \otimes H_1 \cong \mathrm{End}_K(L_1)$, $L_2 \otimes H_2 \cong \mathrm{End}_K(L_2)$ and $E \otimes \overline{H} \cong \mathrm{End}_K(E)$ we get after an extension of scalars to L :



Since both inner and outer are pullback diagrams in the category of coalgebras, $L \otimes H$ and $\mathrm{End}_K(L)$ are isomorphic via the canonical map. □

It is a problem that $L_1 \otimes_{L_1 \cap L_2} L_2$ is not the compositum L_1L_2 in general. The following example shows that it is not always possible to endow L_1L_2 with a H-Galois structure such that L_1 and L_2 are H-normal.

Example 2.57. Let $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ where $\omega \neq 1$ is a cubic root of 1. Consider the Galois group $G = G' = \mathrm{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau \,|\, \sigma^3 = \tau^2 = (\sigma\tau)^2 = \mathrm{id} \rangle$ where σ and τ are defined by

$$\begin{cases} \sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega \\ \sigma(\omega) = \omega \end{cases} \quad \text{and} \quad \begin{cases} \tau(\sqrt[3]{2}) = \sqrt[3]{2} \\ \tau(\omega) = \omega^2 \end{cases}$$

Let $L_1 = \mathbb{Q}(\sqrt[3]{2})$ and $\mathrm{Gal}(L/L_1) = \langle\tau\rangle$. Suppose that $L_1/\mathbb{Q}$ is Hopf-Galois with Hopf algebra H_1 given by the Greither-Pareigis group $N_1 = \lambda\big(\langle\sigma\rangle\big) \subseteq \mathrm{Perm}(G/\langle\tau\rangle)$. Let $L_2 = \mathbb{Q}(\sqrt[3]{2}\omega)$ and $\mathrm{Gal}(L/L_2) = \langle\sigma^2\tau\rangle$. Suppose $L_2/\mathbb{Q}$ is Hopf-Galois with Hopf algebra H_2 given by the Greither-Pareigis group $N_2 = \lambda\big(\langle\sigma\rangle\big) \subseteq \mathrm{Perm}(G/\langle\sigma^2\tau\rangle)$. Suppose that $L/\mathbb{Q}$ is H-Galois and that L_1 is H-normal (with induced structure $H/\mathrm{Ann}_H(L_1) \cong H_1$). Let $N \subseteq \mathrm{Perm}(G)$ be its Greither-Pareigis group. By Proposition 2.38, $N \subseteq \mathrm{Perm}_\pi(G)$ where $\pi : G \to G/\langle\tau\rangle$. We also have that the image of N under the projection $\mathrm{Perm}_\pi(G) \twoheadrightarrow \mathrm{Perm}(G/\langle\tau\rangle)$ is N_1. Note that $\#N = 6$ and $\#N_1 = 3$, so we can write $\mathrm{Ker}(N \twoheadrightarrow N_1) = \{\mathrm{id}, f\}$. Because $N \subseteq \mathrm{Perm}(G)$ is regular, f has no fixed element. Moreover, if we write $G/\langle\tau\rangle = \big\{1_G\langle\tau\rangle, \sigma\langle\tau\rangle, \sigma^2\langle\tau\rangle\big\}$ the $\langle\tau\rangle$-cosets of G, then $f(1_G\langle\tau\rangle) = 1_G\langle\tau\rangle$, $f(\sigma\langle\tau\rangle) = \sigma\langle\tau\rangle$ and $f(\sigma^2\langle\tau\rangle) = \sigma^2\langle\tau\rangle$. We can conclude that

$$f(1_G) = \tau, f(\tau) = 1_G, f(\sigma) = \sigma\tau, f(\sigma\tau) = \sigma, f(\sigma^2) = \sigma^2\tau \text{ and } f(\sigma^2\tau) = \sigma^2.$$

If we define the right translation map $\rho : G \to \mathrm{Perm}(G) : g \mapsto (g' \mapsto g'g^{-1})$, then we obtain $f = \rho(\tau)$.
Let $G/\langle\sigma^2\tau\rangle = \big\{1_G\langle\sigma^2\tau\rangle, \sigma\langle\sigma^2\tau\rangle, \sigma^2\langle\sigma^2\tau\rangle\big\}$ be the set of cosets associated with L_2. Applying f on the coset $1_G\langle\sigma^2\tau\rangle$ yields

$$f(1_G) = \tau \in \sigma\langle\sigma^2\tau\rangle \text{ and } f(\sigma^2\tau) = \sigma^2 \in \sigma^2\langle\sigma^2\tau\rangle.$$

Therefore, $N \nsubseteq \mathrm{Perm}_{\langle\sigma^2\tau\rangle}\big(\langle\sigma, \tau\rangle\big)$. We can conclude by Proposition 2.38 that L_2 is not H-stable and hence not H-normal. However, $\mathbb{Q}(\sqrt[3]{2}) \cap \mathbb{Q}(\sqrt[3]{2}\omega) = \mathbb{Q}$ and H_1 and H_2 acts on $\mathbb{Q}$ via their counit map. Thus, $L_1/\mathbb{Q}$ and $L_2/\mathbb{Q}$ are weakly compatible but there is no Hopf-Galois structure on their compositum $\mathbb{Q}(\sqrt[3]{2}, \omega)$ that induces both H_1 and H_2 at the same time.

Definition 2.58. Let L_1/K be a finite separable H_1-Galois extension and L_2/K be a finite separable H_2-Galois extension. We say that these two Hopf-Galois extensions are *compatible* if

1. there exists a Hopf algebra H such that L_1L_2/K is H-Galois,
2. L_1 and L_2 are H-normal subextensions of L/K,
3. for $i \in \{1, 2\}$, there exists an isomorphism of Hopf algebras $\varphi_i : H/\mathrm{Ann}_H(L_i) \cong H_i$ such that
$$h \cdot x = \varphi_i\big(\pi_i(h)\big) \cdot x \quad \forall h \in H, \forall x \in L_i$$
where $\pi_i : H \twoheadrightarrow H/\mathrm{Ann}_H(L_i)$ is the natural projection.

Corollary 2.59. *Let L_1/K be a finite separable H_1-Galois extension and L_2/K be a finite separable H_2-Galois extension. If L_1/K and L_2/K are compatible, then they are weakly compatible. Moreover, if L_1/K and L_2/K are weakly compatible (with $E = L_1 \cap L_2$) and if the morphism of rings $L_1 \otimes_E L_2 \twoheadrightarrow L_1L_2$ is an isomorphism, then L_1/K and L_2/K are compatible.*

Proof. The first part follows from Proposition 2.54(b) and the second part from Proposition 2.56, from the isomorphism $L_1 \otimes_E L_2 \cong L_1L_2$ and from Corollary 2.34(b). □

2.9 Examples

2.9.1 Canonical Galois extensions

Let L/K be a finite Galois extension with Galois group G. Recall from Example 2.10 that there are two Hopf-Galois structures on L/K: the canonical classical Hopf-Galois structure coming from the Greither-Pareigis group $N_\rho = \rho(G) \subseteq \mathrm{Perm}(G)$ and the canonical nonclassical Hopf-Galois structure coming from the Greither-Pareigis group $N_\lambda = \lambda(G) \subseteq \mathrm{Perm}(G)$. If $\rho(\sigma) \in N_\rho$ and $\lambda(\tau) \in N_\lambda$ for $\sigma, \tau \in G$, then we obviously have that $\rho(\sigma)\lambda(\tau) = \lambda(\tau)\rho(\sigma)$. We thus find that $\mathrm{Cent}(N_\rho) \subseteq N_\lambda$ and $\mathrm{Cent}(N_\lambda) \subseteq N_\rho$. By Lemma 2.47, all these groups have the same cardinality. We can thus conclude that $\mathrm{Cent}(N_\rho) = N_\lambda$ and $\mathrm{Cent}(N_\lambda) = N_\rho$. The canonical classical Hopf-Galois structure and the canonical nonclassical Hopf-Galois structure are therefore opposite.

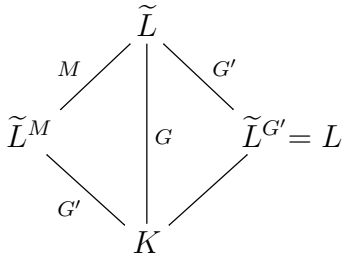
Consider the canonical classical Hopf-Galois structure: L/K is H_ρ-Galois with $H_\rho = K[G]$. By classical Galois theory, every intermediate field L_0 is an H_ρ-subextension. Moreover, L_0 is H_ρ-stable if and only if L_0/K is normal, hence Galois.

For the canonical nonclassical Hopf-Galois structure: L/K is H_λ-Galois with $H_\lambda = L[\lambda(G)]^G$. Because $H_\rho \cong H_\lambda^\dagger$ (and their action on L/K coincide via this isomorphism), we can conclude by Theorem 2.51 that every intermediate field L_0 is H_λ-stable and that L_0 is an H_λ-subextension if and only if L_0/K is Galois.

2.9.2 Almost classical Galois extensions

We will now study a class of Hopf-Galois extensions for which the map Fix defined in Proposition 2.2 is a bijection. This was introduced by [GP87]. Let $\widetilde{L}/K$ be a finite

Galois extension with Galois group $G = M \rtimes G'$ and let $L = \widetilde{L}^{G'}$, then we have the following diagram:



Let H be the Hopf algebra associated with the Greither-Pareigis group $N = \lambda(M) \subseteq \mathrm{Perm}(X)$ with $X = G/G'$.

Let L_0 be any intermediate extension of L/K, $G_\bullet = \mathrm{Gal}(\widetilde{L}/L_0)$ and $\pi : X \longrightarrow\!\!\!\!\!\rightarrow G/G_\bullet$. If $m \in M$ and $\tau_1 G', \tau_2 G' \in X$ such that $\pi(\tau_1 G') = \tau_1 G_\bullet = \tau_2 G_\bullet = \pi(\tau_2 G')$, then

$$\pi\big(\lambda(m)(\tau_1 G')\big) = \pi(m\tau_1 G') = m\tau_1 G_\bullet = m\tau_2 G_\bullet = \pi(m\tau_2 G') = \pi\big(\lambda(m)(\tau_2 G')\big).$$

By Definition 2.36, $\lambda(M) \subseteq \mathrm{Perm}_\pi(X)$ so, by Proposition 2.38, every intermediate extension L_0 is H-stable.

We will now characterize H-subextensions of L/K. If L_0 is any intermediate field of L/K, then $G_\bullet = \mathrm{Gal}(\widetilde{L}/L_0)$ is a subgroup of G containing G'. We thus have $G_\bullet = M' \rtimes G'$ for some subgroup $M' \subseteq M$. Define $\mathcal{N}$ as in Definition 2.39:

$$\mathcal{N} = \big\{\lambda(m) \in \lambda(M) \,|\, \lambda(m)(G_\bullet/G') \subseteq G_\bullet/G'\big\}.$$

For $m \in M$, it is obvious that $m \in M'$ if and only if $\lambda(m)(M' \rtimes G')/G' \subseteq (M' \rtimes G')/G'$. So $\mathcal{N} = \lambda(M')$. As $\#\mathcal{N} = \#M' = \#\big((M' \rtimes G')/G'\big) = \#(G_\bullet/G')$, by Remark 2.41 $\mathcal{N} \subseteq \mathrm{Perm}(G_\bullet/G')$ is regular. Moreover, $\lambda(M')$ is normalized by $\lambda(G)$ if and only if M' is a normal subgroup of G. In this case, we have $L_0 = \widetilde{L}^{M' \rtimes G'} = \widetilde{L}^{M'} \cap \widetilde{L}^{G'}$ where $\widetilde{L}^{M'}/K$ is Galois and contains $\widetilde{L}^M$. By Proposition 2.43, we can conclude that L_0 is an H-subextension if and only if $L_0 = L \cap E$ where E/K is a Galois extension containing $\widetilde{L}^M/K$ (and contained in $\widetilde{L}$).

For the opposite Hopf-Galois structure $H^\dagger$ given by $\mathrm{Cent}\big(\lambda(M)\big)$, any intermediate extension is an $H^\dagger$-subextension (because any intermediate extension if H-stable). This means that the map Fix defined in Proposition 2.2 is bijective. This Hopf-Galois structure is called *almost classical Galois*.

3

Infinite Hopf-Galois theory

3.1 Finite topologies

Let K be a field. Let $(I, \leq)$ be a directed poset and let $(X_i, \xi_{ij} : X_j \to X_i)$ be an inverse system of finite dimensional vector spaces over K. This means that the X_i is a finite dimensional vector space for each $i \in I$ and ξ_{ij} is a surjective linear map for each couple $i, j \in I$ such that $i \leq j$, such that $\xi_{ii} = id_{X_i}$ and for all $i \leq j \leq k$ in I we have that $\xi_{ik} = \xi_{ij} \circ \xi_{jk}$.

A *cone* on $(X_i, \xi_{ij} : X_j \to X_i)$ is a (possibly infinite) vector space X, together with linear maps $\xi_i : X \to X_i$ for all $i \in I$, such that $x_i = \xi_{ij} \circ \xi_j$ for all $i \leq j$. Given such a cone, one can endow X with the coarsest topology such that all maps ξ_i are continuous, where the finite dimensional vector spaces X_i are considered with the discrete topology. This topology is then generated by the following neighbourhoods of open sets around each element $x \in X$:

$$\mathcal{O}_{x,i} = \{y \in X \mid \xi_i(y) = \xi_i(x)\},$$

i.e. the inverse images of singletons under the maps ξ_i. We call this topology the *finite topology* on the cone X.

Among all cones, there exists a (up to isomorphism unique) cone (X, ξ_i) satisfying the universal property that for any other cone (X', ξ'_i), there exists a unique map $u : X' \to X$ such that $\xi'_i = \xi_i \circ u$. This universal cone is exactly the *inverse limit* of the inverse system:

$$X = \varprojlim_{i \in I} X_i$$

Remark that since we supposed that the maps ξ_{ij} are surjective, the maps ξ_i are surjective as well. It is clear that the unique map $u : X' \to X$ is continuous with

respect to the finite topologies. In fact, if X' is any topological vector space and $f : X' \to X$ is any continuous map, then it is clear that $(X', \xi_i \circ f)$ is a cone and f is exactly the unique map induced from the universal property applied to this cone. As a consequence of this observation, one can interpret the inverse limit as a "completion". More precisely, we have the following result.

Lemma 3.1. *Consider an inverse system $(X_i, \xi_{ij} : X_j \to X_i)$ of finite dimensional vector spaces and let $X = \varprojlim_{i \in I} X_i$ be the inverse limit. Then the image of a morphism $f : X' \to X$ of vector spaces is dense with respect to the finite topology on X if and only if the maps $\xi_i \circ f : X' \to X_i$ are surjective for all $i \in I$.*

Proof. Take any element $x_i = \xi_i(x) \in X_i$ for some $i \in I$ and $x \in X$. Then we know that the image of f has a non-empty intersection with the open set $\mathcal{O}_{x,i}$. Consequently, there exists an element $f(x') \in \mathrm{Im} f$ such that $\xi_i \circ f(x') = \xi_i(x) = x_i$. Hence $\xi_i \circ f$ is surjective for all $i \in I$. The converse is proven in the same way. □

3.2 Definition of infinite Hopf-Galois extensions

Let L/K be an infinite algebraic field extension which is Galois in the classical sense. If L_0/K is a finite Galois subextension, then the canonical map

$$L \otimes K[\mathrm{Gal}(L_0/K)] \longrightarrow \mathrm{Hom}_K(L_0, L) : x \otimes \sigma_0 \longmapsto \big(y \mapsto x\sigma_0(y)\big) \tag{3.1}$$

is bijective. Let $\mathcal{L}$ be the set of all finite Galois subextensions L_0/K of L/K. Since any element $x \in L$ is contained in a finite Galois subextension, L is exactly the union of all elements in $\mathcal{L}$. More precisely, L can be reconstructed from $\mathcal{L}$ as the direct limit

$$L = \varinjlim_{L_0 \in \mathcal{L}} L_0,$$

in the category of K-vector spaces. Applying the contravariant functor $\mathrm{Hom}_K(-, L) : \mathsf{Vect}_K \to \mathsf{Vect}_K$, we obtain henceforth an isomorphism

$$\mathrm{End}_K(L) \cong \varprojlim_{L_0 \in \mathcal{L}} \mathrm{Hom}_K(L_0, L).$$

Consequently, taking an inverse limit of the isomorphisms (3.1), we obtain a canonical isomorphism

$$\varprojlim_{L_0 \in \mathcal{L}} (L \otimes K[\mathrm{Gal}(L_0/K)]) \longrightarrow \mathrm{End}_K(L). \tag{3.2}$$

On the other hand, let us consider the infinite Galois group $\mathrm{Gal}(L/K)$, which is known to be an inverse limit itself:

$$\mathrm{Gal}(L/K) \cong \varprojlim_{L_0 \in \mathcal{L}} \mathrm{Gal}(L_0/K)$$

We can consider the associated group algebra $H = K[\mathrm{Gal}(L/K)]$, which is of course a Hopf algebra, and L becomes naturally an H-module algebra by means of the action of the Galois group. Hence, we can consider the canonical map

$$can : \ L \otimes K[\mathrm{Gal}(L/K)] \longrightarrow \mathrm{End}_K(L), \tag{3.3}$$

which is injective but not surjective.

In order to understand the connection between the two canonical maps (3.2) and (3.3), let us endow for each $L_0 \in \mathcal{L}$, the vector spaces $L \otimes K[\mathrm{Gal}(L_0/K)]$ and $\mathrm{Hom}_K(L_0, L)$ with the discrete topology. Then the inverse limits $\varprojlim_{L_0 \in \mathcal{L}} K[\mathrm{Gal}(L_0/K)]$ and $\mathrm{End}_K(L)$ are naturally endowed with the finite topology, as explained in the previous section.

With this topology, the canonical map (3.3) is continuous and the subset

$$L \otimes K[\mathrm{Gal}(L/K)] \subseteq \varprojlim_{L_0 \in \mathcal{L}} L \otimes K[\mathrm{Gal}(L_0/K)]$$

is dense because for every $L_0 \in \mathcal{L}$ the map

$$L \otimes K[\mathrm{Gal}(L/K)] \longrightarrow L \otimes K[\mathrm{Gal}(L_0/K)]$$

is surjective (see Lemma 3.1). So the image of the canonical map (3.3) is also dense, and the domain of (3.2) could be interpreted as the completion of the domain of (3.3). This motivates us to introduce the following definition.

Definition 3.2. Let L/K be a (possibly) infinite separable field extension and H a K-Hopf algebra such that L is a left H-module algebra, then L/K is *H-Galois* if the canonical map

$$can : L \otimes H \longrightarrow \mathrm{End}_K(L) \ , \ \underline{\mathrm{can}}(x \otimes h)(y) = x(h \cdot y)$$

is injective with dense image (where the topology on $\mathrm{End}_K(L)$ is the finite topology, induced by considering the discrete topology on each restriction $\mathrm{End}_K(L_0, L)$ for all finite dimensional intermediate fields L_0 of L/K).

Example 3.3. Let L/K be an infinite field extension and A a K-Hopf algebra which is residually finite dimensional, which means that the Sweedler dual A° is dense in the linear dual A^*, with respect to the finite topology. Let L be an A-comodule algebra and such that the (dual) canonical map

$$L \otimes L \xrightarrow{\sim} L \otimes A\ ,\ x \otimes y \mapsto xy_{[0]} \otimes y_{[1]}$$

is bijective (this means that L is A-Galois in the sense of [DT89]). Then taking L-linear duals, we find a bijection

$$\mathrm{Hom}_K(A, L) \simeq \mathrm{Hom}_L(L \otimes A, L) \xrightarrow{\sim} \mathrm{Hom}_L(L \otimes L, L) \simeq \mathrm{End}_K(L)\ .$$

Furthermore, we have that the subsets

$$L \otimes A^\circ \subseteq L \otimes A^* \subseteq \mathrm{Hom}_K(A, L),$$

are obviously dense with respect to the finite topology on $\mathrm{Hom}_K(A, L)$. Therefore, L/K is an A°-Galois extension in the sense of Definition 3.2.

In the same way as for finite H-Galois extensions, we will define H-normal subextensions of an infinite H-Galois extension L/K. These subextensions will allow us to establish a first correspondence theorem for infinite H-Galois extensions.

Definition 3.4. Let L/K be an infinite H-Galois extension and let L_0/K be a subextension of L/K. We say that L_0 is *H-normal* if L_0 is H-stable and if

$$L \otimes H/\mathrm{Ann}_H(L_0) \longrightarrow \mathrm{Hom}_K(L_0, L)\ ,\ x \otimes \overline{h} \mapsto (y \mapsto x(h \cdot y))$$

is injective, where $\mathrm{Ann}_H(L_0) = \left\{h \in H \,|\, h(x) = 0 \quad \forall x \in L_0\right\}$ and $\overline{h} \in H/\mathrm{Ann}_H(L_0)$ denotes the element represented by $h \in H$.

Proposition 3.5. *Let L_0 be a finite H-normal subextension, then $Ann_H(L_0)$ is a cofinite Hopf ideal and L_0/K is $H/Ann_H(L_0)$-Galois.*

Proof. Following the proof of Proposition 2.23, we can conclude that $\mathrm{Ann}_H(L_0)$ is a biideal.

We will now prove that the canonical map

$$L_0 \otimes H/\mathrm{Ann}_H(L_0) \longrightarrow \mathrm{End}_K(L_0), x \otimes \overline{h} \mapsto (y \mapsto x(h \cdot y)) \tag{3.4}$$

is bijective. Tensoring this map with the identity morphism, we obtain a map

$$L \otimes H/\mathrm{Ann}_H(L_0) \cong L \underset{L_0}{\otimes} \big(L_0 \otimes H/\mathrm{Ann}_H(L_0))\big) \longrightarrow L \underset{L_0}{\otimes} \mathrm{End}_K(L_0)$$

which is exactly the canonical map from Definition 3.4, and therefore injective. Since field extensions are faithfully flat, the map (3.4) is injective as well.

Moreover, by definition of an infinite H-Galois extension, the canonical map

$$\underline{\text{can}} : L \otimes H \longrightarrow \text{End}_K(L)$$

has dense image. Thus by Lemma 3.1 and the definition of the finite topology on $\text{End}_K(L)$, the induced map

$$L \otimes H \longrightarrow \text{Hom}_K(L_0, L)$$

is surjective and hence also the canonical map

$$L_0 \otimes H/\text{Ann}_H(L_0) \longrightarrow \text{End}_K(L_0) \ .$$

is surjective, showing that L_0/K is $H/\text{Ann}_H(L_0)$-Galois. □

Unlike the finite case, not all cofinite Hopf ideals are obtained in this way. To overcome this problem, we will need to introduce a topology on the Hopf algebra H itself. But before that, we will first need to prove some properties on the finite H-normal extensions.

3.3 Properties of finite H-normal extensions

Proposition 3.6. *(Transitivity of compatibility) Let L_0 be a finite H-normal subextension of L/K and let E be an $H/Ann_H(L_0)$-normal subextension of L_0/K, then E is also a finite H-normal subextension of L/K.*

Proof. Let $\text{Ann}_H(E) = \big\{h \in H \,|\, hx = 0 \quad \forall x \in E\big\}$, then we obviously have $\text{Ann}_H(L_0) \subseteq \text{Ann}_H(E)$. The isomorphism

$$L_0 \otimes \big(H/\text{Ann}_H(L_0)\big)/\big(\text{Ann}_H(E)/\text{Ann}_H(L_0)\big)\big) \xrightarrow{\sim} \text{Hom}_K(E, L_0)$$

lifts, by base change to L and with the isomorphism

$$\big(H/\text{Ann}_H(L_0)\big)/\big((\text{Ann}_H(E)/\text{Ann}_H(L_0)\big) \simeq H/\text{Ann}_H(E),$$

to the isomorphism

$$L \otimes H/\text{Ann}_H(E) \xrightarrow{\sim} \text{Hom}_K(E, L) \ .$$

□

Before we prove a result on the compositum of H-normal subextensions, we make some general observations.

Lemma 3.7. *Let H be a cocommutative Hopf algebra, and J_1, J_2 two Hopf ideals. Then*

$$J_1 \wedge J_2 := \{h \in H \mid \Delta(h) \in J_1 \otimes H + H \otimes J_2\}$$

is a Hopf ideal of H, and Δ induces an injective morphism of Hopf algebras

$$H/(J_1 \wedge J_2) \to H/J_1 \otimes H/J_2.$$

Proof. Consider the surjective Hopf algebra morphisms

$$p_1 : H \to H/J_1 \quad \text{and} \quad p_2 : H \to H/J_2,$$
$$q_1 : H/J_1 \to H/(J_1 + J_2) \quad \text{and} \quad q_2 : H/J_2 \to H/(J_1 + J_2).$$

From Section 1.1.4, we know that the pullback of q_1 and q_2 is given by the Hopf algebra

$$P = \big\{ \sum h^1 \otimes h^2 \in H/J_1 \otimes H/J_2 \mid h^1_{(1)} \otimes q_1(h^1_{(2)}) \otimes h^2 = h^1 \otimes q_2(h^2_{(1)}) \otimes h^2_{(2)} \big\}.$$

Since obviously, $q_1 \circ p_1 = q_2 \circ p_2$, the universal property of the pullback induces a Hopf algebra map $u : H \to P$ which is given by $u(h) = p_1(h_{(1)}) \otimes p_2(h_{(2)})$. Then the kernel of u is given exactly by $J_1 \wedge J_2$ (to see this, one can apply [DNR01, Lemma 1.4.8]). Hence $J_1 \wedge J_2$ is indeed a Hopf ideal, and Hopf algebra morphism from the statement of the theorem is exactly the canonical inclusion $\mathrm{Im}(u) \subseteq P \subseteq H/J_1 \otimes H/J_2$. □

Remark 3.8. Note that $H/(J_1 \wedge J_2)$ is not the pullback of q_1 and q_2 in the full category of cocommutative Hopf algebras but it is in the category of "objects under H", that is the lattice of quotient Hopf algebras of H. Translating this in the language of normal Hopf subalgebras of H via the map φ (see Definition 1.56), we see that the normal Hopf subalgebra of H associated to $H/(J_1 \wedge J_2)$ is exactly the biggest normal Hopf subalgebra of H that is both contained in $H_1 := \varphi(H/J_1)$ and $H_2 := \varphi(H/J_2)$. In other words, $\varphi\big(H/(J_1 \wedge J_2)\big) = H_1 \cap H_2$.

Proposition 3.9. *(Compositum) Let L/K be an infinite H-Galois extension and let L_1 and L_2 be H-normal subextensions. Then L_1L_2 is an H-normal subextension as well and $Ann_H(L_1L_2) = Ann_H(L_1) \wedge Ann_H(L_2)$. If L_1 and L_2 are finite, then L_1L_2 is finite as well.*

Proof. We first prove that $\mathrm{Ann}_H(L_1L_2) = \mathrm{Ann}_H(L_1) \wedge \mathrm{Ann}_H(L_2)$. Take any $h \in \mathrm{Ann}_H(L_1) \wedge \mathrm{Ann}_H(L_2)$, then for any $x \in L_1$ and $y \in L_2$ we find that

$$h \cdot (xy) = (h_{(1)} \cdot x)(h_{(2)} \cdot y).$$

Since $h_{(1)} \otimes h_{(2)} \in \mathrm{Ann}_H(L_1) \otimes H + H \otimes \mathrm{Ann}_H(L_2)$, every term in the above expression is 0, so $h \in \mathrm{Ann}_H(L_1L_2)$. Conversely, suppose that $h \in \mathrm{Ann}_H(L_1L_2)$, then we know that for any $x \in L_1$ and $y \in L_2$,

$$h \cdot (xy) = (h_{(1)} \cdot x)(h_{(2)} \cdot y) = 0$$

Since L_2 is H-normal, we know that the canonical map $L_1L_2 \otimes H/\mathrm{Ann}_H(L_2) \to \mathrm{Hom}_K(L_2, L_1L_2)$ is injective, and hence we find that

$$h_{(1)} \cdot x \otimes p_2(h_{(2)}) = 0$$

for all $x \in L_1$, where we denote $p_2 : H \to H/\mathrm{Ann}(L_2)$ the canonical surjection. Since L_1 is also H-normal, we know that the canonical map $L_1 \otimes H/\mathrm{Ann}_H(L_1) \to \mathrm{End}_K(L_1)$ is also injective. Moreover, since K is a field, tensoring this injective map with the identity map on $H/\mathrm{Ann}_H(L_2)$ still yields an injective map. Therefore we obtain that

$$p_1(h_{(1)}) \otimes p_2(h_{(2)}) = 0,$$

where $p_1 : H \to H/\mathrm{Ann}(L_1)$ is again the canonical surjection. Therefore, $\Delta(h) = h_{(1)} \otimes h_{(2)} \in \mathrm{Ann}_H(L_1) \otimes H + H \otimes \mathrm{Ann}_H(L_2)$, which means exactly that $h \in \mathrm{Ann}_H(L_1) \wedge \mathrm{Ann}_H(L_2)$.

Let us now prove that L_1L_2 is H-normal. Clearly, L_1L_2 is H-stable, since both L_1 and L_2 are H-stable. Hence, and by the first part of the proof, we only have to show that the canonical map

$$L \otimes H/\big(\mathrm{Ann}_H(L_1) \wedge \mathrm{Ann}_H(L_2)\big) \to Hom_K(L_1L_2, L)$$

is injective. So take any $\sum_i z^i \otimes \overline{h}^i \in L \otimes H/(\mathrm{Ann}_H(L_1) \wedge \mathrm{Ann}_H(L_2))$ whose image under the above canonical map is 0, where $\overline{h}^i$ are elements in $H/\big(\mathrm{Ann}_H(L_1) \wedge \mathrm{Ann}_H(L_2)\big)$ represented by $h^i \in H$. This means that for any $x \in L_1$ and $y \in L_2$ we have that

$$\sum_i z^i(h^i \cdot (xy)) = \sum_i z^i(h^i_{(1)} \cdot x)(h^i_{(2)} \cdot y) = 0$$

Using again successively the H-normality of L_1 and L_2, we find that this means that

$$\sum_i z^i \otimes p_1(h^i_{(1)}) \otimes p_2(h^i_{(2)}) = 0$$

as an element in $L \otimes H/\mathrm{Ann}(L_1) \otimes H/\mathrm{Ann}(L_2)$. Then applying the injectivity of the morphism $H/\big(\mathrm{Ann}_H(L_1) \wedge \mathrm{Ann}_H(L_2)\big) \to H/\mathrm{Ann}(L_1) \otimes H/\mathrm{Ann}(L_2)$ induced by Δ (see Lemma 3.7), we conclude that

$$\sum_i z^i \otimes \overline{h}^i = 0$$

in $L \otimes H/\big(\mathrm{Ann}_H(L_1) \wedge \mathrm{Ann}_H(L_2)\big)$, and hence L_1L_2 is H-normal. □

Proposition 3.10. *(Intersection) Let L/K be an infinite H-Galois extension and let L_1 and L_2 be two finite H-normal subextensions. Then $L_1 \cap L_2$ is $H/Ann_H(L_1)$-normal and $H/Ann_H(L_2)$-normal.*

Proof. By Proposition 3.9, we know that L_1L_2 is a finite H-normal subextension. Hence, L_1L_2 is a finite $H/\mathrm{Ann}_H(L_1L_2)$-Galois extension by Proposition 3.5, and L_1 and L_2 are $H/\mathrm{Ann}_H(L_1L_2)$-normal subextensions. Hence, by the intersection theorem for finite dimensional Hopf-Galois extensions (Proposition 2.54 (b)), we know that $L_1 \cap L_2$ is an $H/\mathrm{Ann}_H(L_1L_2)$-normal subextension of L_1L_2/K as well, and by Proposition 3.6 $L_1 \cap L_2$ is also a finite H-normal subextension of L/K □

3.4 Topology on H

Let L/K be an (infinite) H-Galois extension. Let $\mathcal{L}$ be the set of all finite H-normal subextensions of L/K. Then for each $L_i \in \mathcal{L}$, we have a finite dimensional Hopf algebra $H/\mathrm{Ann}_H(L_i)$, and for any other $L_j \in \mathcal{L}$ such that $L_i \subseteq L_j$, we have a surjective Hopf algebra morphism $p_{ij} : H/\mathrm{Ann}_H(L_j) \to H/\mathrm{Ann}_H(L_i)$. Hence we obtain an inverse system (L_i, p_{ij}). Using the canonical projections $p_i : H \to H/\mathrm{Ann}_H(L_i)$, we find that H is a cone on this inverse system, and hence can be induced with the associated finite topology. Let us describe a base of open sets for this topology.

Lemma 3.11. *Consider the set*

$$\mathcal{B} = \Big\{ h + Ann_H(L_0) \Big\}_{h \in H, L_0 \in \mathcal{L}}.$$

Then $\mathcal{B}$ is a base for a topology on H, i.e. there is a topology on H whose open subsets are exactly the unions of subsets of $\mathcal{B}$.

Proof. First, we need to prove that $\mathcal{B}$ covers H. This is obvious because $\mathcal{L}$ is non-empty (as it contains at least the finite H-normal extension K/K). Next, we need to prove that for each $h_1 + \mathrm{Ann}_H(L_1)$ and $h_2 + \mathrm{Ann}_H(L_2) \in \mathcal{B}$ and for each h in their intersection, there exists $h_3 + \mathrm{Ann}_H(L_3) \in \mathcal{B}$ such that

$$h \in h_3 + \mathrm{Ann}_H(L_3) \subseteq \big(h_1 + \mathrm{Ann}_H(L_1)\big) \cap \big(h_2 + \mathrm{Ann}_H(L_2)\big).$$

Because the intersection contains an element h, we can assume that $h = h_1 = h_2 = h_3$ so we just need to prove that there exists $L_3 \in \mathcal{L}$ such that

$$\mathrm{Ann}_H(L_3) \subseteq \mathrm{Ann}_H(L_1) \cap \mathrm{Ann}_H(L_2).$$

Now just take the compositum $L_3 = L_1L_2$, then by Proposition 3.9:

$$\mathrm{Ann}_H(L_3) = \mathrm{Ann}_H(L_1) \wedge \mathrm{Ann}_H(L_2) \subseteq \mathrm{Ann}_H(L_1) \cap \mathrm{Ann}_H(L_2).$$

This completes the proof. □

Next, we will prove that the open Hopf ideals of H with respect to the topology given by Lemma 3.11 are exactly the sets $Ann_H(L_0)$ for $L_0 \in \mathcal{L}$.

Proposition 3.12. *Let $U \subseteq H$ be an open subset. If U is a Hopf ideal of H, then $U = Ann_H(L_U)$ for some $L_U \in \mathcal{L}$.*

Proof. Let $U \subseteq H$ be open, then U can be written as a union of subsets in $\mathcal{B}$. If U is also a Hopf ideal, then one of these subsets must be of the form $\mathrm{Ann}_H(L_0)$:

$$\mathrm{Ann}_H(L_0) \subseteq U \text{ for } L_0 \in \mathcal{L} \implies H/\mathrm{Ann}_H(L_0) \twoheadrightarrow H/U.$$

Let $I \subseteq H/\mathrm{Ann}_H(L_0)$ be the kernel of the surjective morphism of (finite dimensional) Hopf algebras $H/\mathrm{Ann}_H(L_0) \twoheadrightarrow H/U$ and consider the intermediate field of I-invariants L_0^I. By Theorem 2.31, L_0^I is an $H/\mathrm{Ann}_H(L_0)$-normal subextension of L_0/K and $\mathrm{Ann}_{H/\mathrm{Ann}_H(L_0)}(L_0^I) = I$. Let $p : H \twoheadrightarrow H/\mathrm{Ann}_H(L_0)$ be the natural projection, then

$$\begin{aligned} \mathrm{Ann}_H(L_0^I) &= p^{-1}\big(\mathrm{Ann}_{H/\mathrm{Ann}_H(L_0)}(L_0^I)\big) = p^{-1}(I) \\ &= \mathrm{Ker}\big(H \twoheadrightarrow H/\mathrm{Ann}_H(L_0) \twoheadrightarrow H/U\big) = U. \end{aligned}$$

Thus, we have that $U = \mathrm{Ann}_H(L_0^I)$ with $L_0^I \in \mathcal{L}$ (Proposition 3.6). □

3.5 Correspondence theorem between open Hopf ideals and finite H-normal intermediate extensions

Proposition 3.13. *Let $I \subseteq H$ be an open Hopf ideal of H, then L^I is H-normal and L^I/K is H/I-Galois and $Ann_H(L^I) = I$.*

Proof. Let $I \subseteq H$ be an open Hopf ideal of H, then by Proposition 3.12, $I = \mathrm{Ann}_H(L_0)$ for some $L_0 \in \mathcal{L}$ so $L^I \supseteq L_0$. We will now prove that $\mathrm{Ann}_H(L^I) = I$.
We obviously have $I \subseteq \mathrm{Ann}_H(L^I)$. For the other inclusion, let $h \in \mathrm{Ann}_H(L^I)$ then

$\forall x \in L_0 \subseteq L^I$, we have that $h \cdot x = 0$. Hence $h \in I$.
So, the canonical isomorphism $L \otimes H/I \cong \mathrm{Hom}_K(L_0, L)$ factors through $\mathrm{Hom}_K(L^I, L)$:

$$L \otimes H/I \twoheadrightarrow \mathrm{Hom}_K(L^I, L) \twoheadrightarrow \mathrm{Hom}_K(L_0, L).$$

Since this composition of surjective maps is an isomorphism, it is a composition of isomorphisms and therefore we obtain that $L_0 = L^I$. □

We can now immediately derive our correspondence theorem for infinite Hopf-Galois extensions.

Theorem 3.14. *Let L/K be an infinite H-Galois extension. The maps*

$$\begin{aligned} \big\{L/L_0/K \,|\, L_0 \textit{ is finite } H\textit{-normal}\big\} &\rightleftarrows \big\{I \subseteq H \,|\, I \textit{ is an open Hopf ideal}\big\} \\ L_0 &\longmapsto J(L_0) = \big\{h \in H \,|\, hx = 0 \quad \forall x \in L_0\big\} \\ L^I := \big\{x \in L \,|\, hx = 0 \quad \forall h \in I\big\} &\longmapsfrom I \end{aligned}$$

are mutually inverse bijections.

Proof. This follows immediately from Proposition 3.13 with Proposition 3.5. □

3.6 Example

Let $p, q_1, q_2, ... \in \mathbb{N}$ be pairwise distinct prime numbers. We define $L = \mathbb{Q}(\sqrt{p}, \sqrt{q_1}, \sqrt{q_2}, ...)$, $L_0 = \mathbb{Q}(\sqrt{q_1}, \sqrt{q_2}, ...)$ and

$$G = \Big\{\sigma \in \mathrm{Gal}\big(L_0/\mathbb{Q}\big) \,|\, \sigma(\sqrt{q_i}) = -\sqrt{q_i} \text{ for finitely many } i \in \mathbb{N}_0\Big\}.$$

Note that $L_0/\mathbb{Q}$ is an infinite $\mathbb{Q}[G]$-Galois extension in the sense of Definition 3.2 even though G is not the Galois group of $L_0/\mathbb{Q}$. This can be explained by the fact that, for every finite Galois intermediate extension $E/\mathbb{Q}$ of $L_0/\mathbb{Q}$, the group morphism $G \to \mathrm{Gal}(E/\mathbb{Q})$ is surjective.

For each $\sigma \in G$, we define $q_\sigma = \prod_{i \in \mathbb{N}_0 \,|\, \sigma(\sqrt{q_i}) = -\sqrt{q_i}} q_i$. Then $L/\mathbb{Q}$ can be endowed with an infinite Hopf-Galois structure. The $\mathbb{Q}$-linear action of G on L_0 is extended to L in the following way:

$$\sigma\big(\sqrt{p}\sqrt{q_{a_1}...q_{a_n}}\big) = 0$$

where $\sigma \in G$ and $q_{a_1}, ..., q_{a_n} \in \{q_1, q_2, ...\}$ are pairwise distinct. For each $\sigma \in G$, we also define the $\mathbb{Q}$-linear map $\sigma_0 : L \to L$ by

$$\sigma_0\big(\sqrt{q_{a_1}...q_{a_n}}\big) = 0 \text{ and } \sigma_0\big(\sqrt{p}\sqrt{q_{a_1}...q_{a_n}}\big) = \sqrt{p}\sqrt{q_\sigma}\sigma\big(\sqrt{q_{a_1}...q_{a_n}}\big).$$

Let H be the $\mathbb{Q}$-vector space generated by all the σ and σ_0. We define on H the following maps:

- unit map: $\iota(1) = \mathrm{id} + \mathrm{id}_0$ where $\mathrm{id} \in G$ is the identity map from L_0 to itself;
- multiplication map: for all $\sigma, \tau \in G$ we define

$$\sigma.\tau = \sigma\tau,\ \sigma.\tau_0 = \sigma_0.\tau = 0,\ \sigma_0.\tau_0 = \frac{gcd(q_\sigma, q_\tau)}{(\mu \circ gcd)(q_\sigma, q_\tau)}(\sigma\tau)_0$$

  where $gcd(q_\sigma, q_\tau)$ is the greatest common divisor of q_σ and q_τ and where $\mu : \mathbb{N}_0 \to \{-1, 0, 1\}$ is the Möbius function;
- counit map: $\epsilon(\sigma) = 1$ and $\epsilon(\sigma_0) = 0$;
- comultiplication map: $\Delta(\sigma) = \sigma \otimes \sigma + \dfrac{\sigma_0 \otimes \sigma_0}{q_\sigma}$ and $\Delta(\sigma_0) = \sigma \otimes \sigma_0 + \sigma_0 \otimes \sigma$;
- antipode: $S(\sigma) = \sigma$ and $S(\sigma_0) = \mu(q_\sigma)\sigma_0$.

With these maps, H is a Hopf algebra and $L/\mathbb{Q}$ is an infinite H-Galois extension. We can see that for any $\sqrt{p}\sqrt{q_{a_1}...q_{a_n}}$ with pairwise distinct $q_{a_1}, ..., q_{a_n} \in \{q_1, q_2, ...\}$, there exists a $\sigma \in G$ such that

$$\sigma_0(\sqrt{p}) = \sqrt{p}\sqrt{q_{a_1}...q_{a_n}}.$$

Therefore, $\sqrt{p}$ does not belong to a finite H-stable intermediate field of $L/\mathbb{Q}$ (the same result goes for any $\sqrt{p}\sqrt{q_{a_1}...q_{a_n}}$). However, by definition of the action of σ and σ_0 on L, every finite subfield contained in L_0 is H-stable. Moreover, the annihilator $\mathrm{Ann}_H(L_0)$ is generated by all the σ_0 and, therefore, the quotient $H/\mathrm{Ann}_H(L_0)$ is naturally isomorphic to $\mathbb{Q}[G]$. We can thus conclude that the morphism

$$L \otimes H/\mathrm{Ann}_H(L_0) \longrightarrow \mathrm{Hom}_K(L_0, L)$$

is injective, i.e. L_0 is an infinite H-subextension and hence an infinite H-normal subextension of $L/\mathbb{Q}$. As pointed earlier, the set $\mathcal{L}$ of all finite H-normal subextensions of $L/\mathbb{Q}$ coincide with the set of all finite H-normal subextensions of $L_0/\mathbb{Q}$. Since G is abelian, $\mathcal{L}$ is simply the set of all finite subextensions of $L_0/\mathbb{Q}$. If E is such an

extension, then the Hopf-Galois structure on $E/\mathbb{Q}$ is the classical Galois one.

This example shows that, unlike in the classical Galois case, the finite H-normal subextensions are not enough to understand an infinite Hopf-Galois extension. Indeed, for $L/\mathbb{Q}$, $\bigcup_{E\in\mathcal{L}} E = L_0 \subsetneq L$. For $L_0/\mathbb{Q}$ it is even worse: L_0 is the union of its finite $\mathbb{Q}[G]$-normal subextensions and all these subextensions inherit the classical Galois structure but G is not the Galois group of $L_0/\mathbb{Q}$.

In view of this, we can conclude that Definition 3.2 permits all kind of strange behaviour. In order to have a situation as close as possible to the classical Galois case, we need to make the definition more restrictive. One way of doing this would be to ask that H is an inverse limit of finite dimensional Hopf algebras.

4

Research perspectives

The results obtained in this thesis will be published in the forthcoming [BVW]. Apart from the main results presented above, we aim for some further results to be included in this paper, which we briefly discuss in this chapter, but which are still to be completed.

4.1 The Van Oystaeyen-Zhang transform

Let us consider a finite dimensional cocommutative Hopf K-algebra H (where K is a field) and L/K be an H-Galois extension (in the sense of Definition 1.60). It was shown in [OZ94], that one can associate to such an extension a second Hopf algebra T, such that L/K is again a T-Galois extension. This construction was generalized in [Sch98], relaxing the cocommutativity condition on H, and leading to Hopf-bi-Galois extensions.

We will review this construction here, adopting the setting from [OZ94] (who worked in the dual setting of comodule algebras) to ours.

Consider the K-algebra $L \otimes L$. Then H acts on $L \otimes L$ via the diagonal action:

$$h \cdot (x \otimes y) = h_{(1)} \cdot x \otimes h_{(2)} \cdot y$$

and in this way $L \otimes L$ is an H-module algebra. Hence we can consider the associated space of invariants

$$T = (L \otimes L)^H = \{x \otimes y \mid h \cdot (x \otimes y) = \epsilon(h)x \otimes y, \forall h \in H\}$$

Following [Gre96], we will call T the *Van Oystaeyen-Zhang transform*, or OZ-transform for short. By the faithfully flat descent (see Proposition 1.70), we find moreover that there is a canonical isomorphism

$$\beta : L \otimes T \xrightarrow{\cong} L \otimes L$$

With this notation, the following theorem collects some results from [OZ94], translated to the language used in this work.

Theorem 4.1. *Let H be a cocommutative Hopf algebra and L/K an H-Galois extension. Then: the following statements hold:*

1. *the OZ-transfrom T is a finite dimensional commutative Hopf algebra, hence T^* is a cocommutative Hopf algebra;*
2. *L is a T^*-module algebra and T^*-Galois;*
3. *the H-subextensions of L/K are in bijective correspondance with the subfields of L that are T^*-stable.*
4. *if H is moreover commutative then $T^* \cong H$.*

As one can observe, the OZ-transform (or its dual) satisfies similar properties as the "opposite Hopf-Galois structure" we have studied in Section 2.7. We aim to clear out whether both constructions are truly the same or whether they differ.

4.2 Infinite Hopf-Galois extensions and profinite Hopf algebras

Now that we have established a correspondence theorem between finite H-normal extensions and open Hopf ideals (see Theorem 3.14), it is natural to study the inverse limit of the quotient Hopf algebras $H/\mathrm{Ann}_H(L_0)$ for $L_0 \in \mathcal{L}$.

Let $(I, \leq)$ be a directed poset and $(H_i)_{i\in I}$ be a family of discrete finite dimensional K-Hopf algebras with homomorphisms $f_{ij} : H_j \to H_i$ for all $i \leq j$ such that $\big((H_i)_{i\in I}, (f_{ij})_{i\leq j}\big)$ is an inverse system. Dually, $\big((H_i^*)_{i\in I}, (f_{ij}^*)_{i\leq j}\big)$ is a direct system of K-Hopf algebras.

Let $\varinjlim_{\mathrm{Hopf}} H_i^*$ (resp. $\varinjlim_{\mathrm{Vect}} H_i^*$) be the direct limit of $\big((H_i^*)_{i\in I}, (f_{ij}^*)_{i\leq j}\big)$ taken in the category of K-Hopf algebras (resp. K-vector spaces). Then these two direct limits coincide (see e.g. [Por11] and [Ago11]) and will refer to them simply with $\varinjlim H_i^*$.

Now, let $\varprojlim_{\mathrm{Hopf}} H_i$ (resp. $\varprojlim_{\mathrm{Vect}} H_i$) be the inverse limit of $\big((H_i)_{i\in I}, (f_{ij})_{i\leq j}\big)$ taken in the category of K-Hopf algebras (resp. K-vector spaces). With this notation, we have the following result.

Proposition 4.2. $\big(\varinjlim H_i^*\big)^\circ \cong \varprojlim_{Hopf} H_i$ *and* $\big(\varinjlim H_i^*\big)^* \cong \varprojlim_{Vect} H_i$.

Proof. Consider the adjoint functors

$$\mathsf{Vect} \underset{G=(-)^*}{\overset{F=(-)^*}{\rightleftarrows}} \mathsf{Vect}^{\mathrm{op}}$$

where F is the left adjoint functor and G is the right adjoint functor. Since left adjoint functors preserve colimits, we get

$$\left(\varinjlim (H_i)^*\right)^* \cong \varprojlim_{\mathrm{Vect}} H_i^{**} \cong \varprojlim_{\mathrm{Vect}} H_i.$$

Similarly, if we consider the adjoint functors

$$\mathsf{Hopf} \underset{G=(-)^\circ}{\overset{F=(-)^\circ}{\rightleftarrows}} \mathsf{Hopf}^{\mathrm{op}}$$

where F is the left adjoint functor and G is the right adjoint functor, then we get

$$\left(\varinjlim (H_i)^*\right)^\circ \cong \varprojlim_{\mathrm{Hopf}} H_i^{*\circ} \cong \varprojlim_{\mathrm{Hopf}} H_i.$$

□

As one can see from the above result, when taking the inverse limit of a family of finite dimensional Hopf algebras, depending whether the limit is taken in the category of vector spaces or in the category of Hopf algebras, we obtain different objects. In fact, we already encountered this phenomenon in section 3.2, where we observed that for a classical infinite Galois extension, we can consider the Hopf algebra $K[\mathrm{Gal}(L/K)]$, but the associated canonical map is no longer surjective. If we should instead consider the bigger object $\varprojlim_{L_0 \in \mathcal{L}} K[\mathrm{Gal}(L_0/K)]$ (which is called the completed group ring) and use a completed tensor product, then the associated canonical map is indeed surjective (and even bijective).

In view of this,we believe it could be useful to develop, in similarity to classical infinite Galois theory, a framework for infinite Hopf-Galois extensions over *profinite Hopf algebras*, of which $\varprojlim_{L_0 \in \mathcal{L}} K[\mathrm{Gal}(L_0/K)]$ (or more generally $\varprojlim_{\mathrm{Vect}} H_i$, as in Proposition 4.2) should be the leading example.

Bibliography

[AG60] M. Auslander and O. Goldman. The Brauer group of a commutative ring. *Trans. Amer. Math. Soc.*, 97:367–409, 1960.

[Ago11] A. L. Agore. Limits of coalgebras, bialgebras and Hopf algebras. *Proc. Amer. Math. Soc.*, 139:855–863, 2011.

[BVW] Hoan-Phung Bui, Joost Vercruysse, and Gabor Wiese. in preparation.

[BW03] Tomasz Brzezinski and Robert Wisbauer. Corings and comodules. *Cambridge University Press*, 2003.

[Byo96] Nigel P. Byott. Uniqueness of hopf galois structure of separable field extensions. *Comm. Algebra*, 24:3217–3228, 3705, 1996.

[Chi89] Lindsay N. Childs. On the Hopf Galois theory for separable field extensions. *Communications in Algebra*, 17(4):809–825, 1989.

[CHR65] S. Chase, D. Harrison, and A. Rosenberg. Galois theory and Galois cohomology of commutative rings. *Mem. Amer. Math. Soc.*, 52:1–19, 1965.

[CRV16] Teresa Crespo, Anna Rio, and Montserrat Vela. On the galois correspondence theorem in separable hopf galois theory. *Journal of Algebra*, 457:312–322, 2016.

[CS69] Stephen U. Chase and Moss E. Sweedler. Hopf algebras and Galois theory. *Lecture Notes in Mathematics*, 97, 1969.

[DI71] F. DeMeyer and E. Ingraham. Separable algebras over commutative rings. *Lecture Notes in Math.*, 181, 1971.

[DNR01] Sorin Dascalescu, Constantin Nastasescu, and Serban Raianu. Hopf algebras: An introduction. *Monographs Textbooks in Pure Appl. Math.*, 235, 2001.

[DT89] Y. Doi and M. Takeuchi. Hopf-Galois extensions of algebras, the Miyashita-Ulbrich action and Azumaya algebras. *J. Algebra*, 121:488–516, 1989.

[GP87] Cornelius Greither and Bodo Pareigis. Hopf Galois theory for separable field extensions. *Journal of Algebra*, 106(1):239 – 258, 1987.

[Gre96] Cornelius Greither. On a transformation of the Hopf algebra in a Hopf Galois extension. *Comm. Algebra*, 24:737–747, 1996.

[Jac85] Nathan Jacobson. Basic algebra i, second edition. *W. H. Freeman and Company*, 1985.

[KKTU19] Alan Koch, Timothy Kohl, Paul J. Truman, and Robert Underwood. Normality and short exact sequences of hopf-galois structures. *Communications in Algebra*, 47(5):2086–2101, 2019.

[Mon93] S. Montgomery. Hopf algebras and their actions on rings. *American Mathematical Society*, 1993.

[New75] Kenneth Newman. A correspondence between bi-ideals and sub-hopf algebras in cocommutative hopf algebras. *Journal of Algebra*, 36(1):1 – 15, 1975.

[OZ94] F. Van Oystaeyen and Y. Zhang. Galois-type correspondences for Hopf Galois extensions. *K-Theory*, 8:257–269, 1994.

[Por08] Hans-E Porst. Fundamental constructions for coalgebras, corings, and comodules. *Appl. Categ. Structures*, 16:223–238, 2008.

[Por11] Hans-E Porst. Limits and colimits of Hopf algebras. *J. Algebra*, 328:254–267, 2011.

[Sch90] Hans-Jürgen Schneider. Principal homogeneous spaces for arbitrary Hopf algebras. *Israel Journal of Mathematics*, 72, 1990.

[Sch97] Peter Schauenburg. A bialgebra that admist a Hopf-Galois extension is a Hopf algebra. *Proc. AMS*, 125:83–85, 1997.

[Sch98] Peter Schauenburg. Galois correspondences for Hopf bigalois extensions. *J. Algebra*, 201:53–70, 1998.

[Swe69] Moss E. Sweedler. Hopf algebras. *W. A. Benjamin Inc.*, 1969.

[Swe75] Moss E. Sweedler. The predual theorem to the Jacobson–Bourbaki theorem. *Trans. Amer. Math. Soc.*, 213:391–406, 1975.