Note di Matematica
Note Mat. **41** (2021) no. 1, 55–67.
ISSN 1123-2536, e-ISSN 1590-0932
doi:10.1285/i15900932v41n1p55

Minimal Hopf-Galois Structures on Separable Field Extensions

Tony Ezome[i]
Université des Sciences et Techniques de Masuku, Faculté des Sciences, Département de mathématiques et informatique, BP 943 Franceville, Gabon
tony.ezome@gmail.com

Cornelius Greither
Institut für Theoretische Informatik, Mathematik und Operations Research, Fakultät für Informatik, Universität der Bundeswehr München, Werner-Heisenberg-Weg 39 85579 Neubiberg
cornelius.greither@unibw.de

Received: 11.11.2020; accepted: 15.4.2021.

Abstract. In Hopf-Galois theory, every H-Hopf-Galois structure on a field extension K/k gives rise to an injective map $\mathcal{F}$ from the set of k-sub-Hopf algebras of H into the intermediate fields of K/k. Recent papers on the failure of the surjectivity of $\mathcal{F}$ reveal that there exist many Hopf-Galois structures for which there are many more subfields than sub-Hopf algebras. In this paper we survey and illustrate group-theoretical methods to determine H-Hopf-Galois structures on finite separable extensions in the extreme situation when H has only two sub-Hopf algebras. This corresponds to the case when the lack of surjectivity is at its extreme.

Keywords: Galois and Hopf-Galois field extensions, Galois correspondence, characteristically simple groups.

MSC 2020 classification: 12F10 (primary); 16T05

1 Introduction

Let k be field. A Hopf algebra H over k is defined to be a k-bialgebra endowed with a k-linear map $S : H \longrightarrow H$ called the antipode so that denoting by ∇ the multiplication, Δ the comultiplication, η the unit and ϵ the counit, we have

$$\nabla \circ (\mathrm{id_H} \otimes S) \circ \Delta = \eta \circ \epsilon = \nabla \circ (S \otimes \mathrm{id_H}) \circ \Delta.$$

Let $\sigma : H \otimes H \longrightarrow H \otimes H$ be the k-linear map defined by $\sigma(x \otimes y) = y \otimes x$ for all $x, y \in H$. Then, H is said to be cocommutative if $\sigma \circ \Delta = \Delta$. Group algebras over k are basic examples of cocommutative k-Hopf algebras. Indeed if G is a group, then the group algebra $k[G]$ is a cocommutative k-Hopf algebra with

[i]This work is partially supported by Simons Foundation via PREMA project, and by the International Centre for Theoretical Physics (ICTP) via their Associate Scheme.
http://siba-ese.unisalento.it/ © 2021 Università del Salento

comultiplication given by $\Delta(g) = g \otimes g$, counit given by $\epsilon(g) = 1$ and antipode given by $S(g) = g^{-1}$, for all $g \in G$. Given a Galois extension of fields K/k, the Fundamental Theorem of Galois Theory (FTGT) states that there is a one-to-one correspondence between the lattice of intermediate fields $k \subseteq F \subseteq K$ and the lattice of subgroups of $G = \mathrm{Gal}(K/k)$. This is the Galois correspondence. It allows us to determine intermediate subfields of K from subgroups of G. So if G is a group with prime order, then the only subfields are K and k. Hopf-Galois theory is a generalization of Galois theory. Indeed if K/k is Galois with Galois group G, then G operates linearly on K as automorphism group, and this action extends to a k-algebra homomorphism $\mu : k[G] \longrightarrow \mathrm{End}_k(K)$. Thus, K/k is Galois with Galois group G if and only if $(1, \mu) : K \otimes_k k[G] \longrightarrow \mathrm{End}_k(K)$ is an isomorphism, where $(1, \mu)$ is given by

$$(1, \mu)(s \otimes h)(t) = s(\mu(h)(t)), \quad \text{for all } s, t \in K, h \in k[G].$$

From this we say that a finite extension of fields K/k is *Hopf-Galois* (we also say that K/k has a *Hopf-Galois structure*) if there exists a finite cocommutative k-Hopf algebra H and a Hopf action $\mu : H \longrightarrow \mathrm{End}_k(K)$ such that

$$(1, \mu) : K \otimes_k H \longrightarrow \mathrm{End}_k(K) \text{ is an isomorphism.}$$

Chase and Sweedler obtained a weak Galois correspondence for Hopf-Galois extensions.

Theorem 4 ([4])**.** Let K/k be a finite Hopf-Galois extension with algebra H and Hopf action $\mu : H \longrightarrow \mathrm{End}_k(K)$. For a k-sub-Hopf algebra H' of H we define

$$K^{H'} = \{x \in K \mid \mu(h)(x) = \epsilon(h) \cdot x \ \text{ for all } h \in H'\},$$

where ϵ is the counit of H. Then, $K^{H'}$ is a subfield of K, containing k, and the map

$$\begin{array}{rccc} \mathcal{F}: & \{H' \subset H \text{ sub-Hopf algebra}\} & \longrightarrow & \{\text{Fields } E \mid k \subseteq E \subseteq K\} \\ & H' & \longmapsto & K^{H'} \end{array}$$

is injective and inclusion reversing.

Recent papers on the failure of the surjectivity of $\mathcal{F}$ reveal that pretty often there are many more subfields than sub-Hopf algebras, see for instance [6], [5], or [9]. We say that *the Galois correspondence holds in its strong form* for a Hopf-Galois structure H on a field extension K/k, if the map $\mathcal{F}$ associated to H in Theorem 4 is a bijection. It is known that the k-sub-Hopf algebras of a finite group algebra $k[G]$ are the group algebras $k[G']$ where G' is a subgroup of G, see for instance [9, Proposition 2.1]. Therefore, FTGT implies that any finite Galois

extension K/k with Galois group G has a natural Hopf-Galois structure (defined by the group algebra $k[G]$) whose Galois correspondence holds in its strong form. In case G has prime order, $k[G]$ has only two k-sub-Hopf algebras. Motivated by this, we define a *minimal Hopf-Galois structure* on a field extension K/k to be a structure given by a k-Hopf algebra H having exactly two k-sub-Hopf algebras; we exclude the trivial case $\dim_k(H) = 1$.

This paper surveys and illustrates group-theoretical methods to determine minimal Hopf-Galois structures on separable field extensions. In section 2 we state a fundamental criterion characterizing these minimal structures. Then we deduce, later in section 4, minimal Hopf-Galois structures on the so-called *almost classically Galois extensions* introduced by Greither and Pareigis in [7]. Sections 3 and 5 are devoted to illustrations. We start with basic examples constructed from simple groups, and counterexamples constructed from groups having a nontrivial proper characteristic subgroup. In particular, we present a family of radical extensions in characteristic zero having no Hopf-Galois structure. By using characteristically simple groups, we prove that for any positive integer $n \leq 11$, except for $n \in \{6, 10\}$, there exists a number field K of degree n having at least one minimal Hopf-Galois structure and whose Galois closure $\tilde{K}$ satisfies $n < [\tilde{K} : \mathbb{Q}] < 672$. All these examples are separable field extensions having either no minimal Hopf-Galois structure, or exactly one minimal structure, or at least two minimal structures. We deduce interesting questions for future work.

2 Fundamental criterion

As previously mentioned, the Galois correspondence associated to an Hopf-Galois structure is not surjective in general. Another difference between Galois theory and Hopf-Galois theory is that one may have several Hopf-Galois structures on the same Galois extension while a Galois extension has only one Galois group. Hopf-Galois theory was first introduced by Chase and Sweedler [4] in 1969 to study purely inseparable extensions. Then Greither and Pareigis [7] developed in 1987 Hopf-Galois theory for separable extensions. Since the publication of [7], many works concerning Hopf-Galois theory have been published. These works deal with interesting problems such as designing methods to determine the number of distinct Hopf-Galois structures on a given Galois extension, finding ways of quantifying Hopf-Galois structures for which Galois correspondence holds in its strong form, or finding ways of quantifying the failure of the surjectivity of the Galois correspondence.

In this section we are interested in identifying minimal Hopf-Galois structures among the structures that can be achieved on a given separable field extension. The starting point is the characterization of Hopf-Galois structures

proposed by Greither and Pareigis.

Theorem 5 ([7], Theorem 2.1)**.** Let K/k be a degree n separable extension and $\tilde{K}$ its normal closure. Set $G = \mathrm{Gal}(\tilde{K}/k)$ and $G' = \mathrm{Gal}(\tilde{K}/K)$. Then K has a k-Hopf-Galois structure if, and only if, there exists a regular subgroup N of $\mathrm{Perm}(G/G')$ normalized by G, where G is identified as a subgroup of $\mathrm{Perm}(G/G')$ via the faithful action

$$\lambda : G \longrightarrow \mathrm{Perm}(G/G')$$

$$g \longmapsto (\lambda_g : xG' \mapsto gxG').$$

Furthermore, the Hopf-Galois structure corresponding to a regular subgroup N of $\mathrm{Perm}(G/G')$ normalized by G is defined by

$$\tilde{K}[N]^G = \{x \in \tilde{K}[N] \mid \sigma(x) = x, \forall \sigma \in G\}$$

where for $x = \sum_{\tau \in N} a_\tau \tau \in \tilde{K}[N]$ and $\sigma \in G$, we have

$$\sigma(x) = \sum_{\tau \in N} \sigma(a_\tau)\lambda(\sigma)\tau\lambda(\sigma)^{-1}.$$

With the notation of Theorem 5, a Hopf-Galois structure on a separable field extension K/k defined by the algebra $\tilde{K}[N]^G$ is said to be of type N. Actually, N and G/G' have necessarily the same order, but there is no natural one-one correspondence between them; in fact G/G' is not even a group in general. We recall that a subgroup N of $\mathrm{Perm}(G/G')$ is said to be regular if the action of N on G/G' is transitive and the stabilizer of any point is trivial. By [7, Theorem 4.1], we know that if such an N is also normalized by G and contained in G then it is a normal complement of G' in G. Theorem 5 says that regular subgroups of $\mathrm{Perm}(G/G')$ normalized by G are in one-to-one correspondence with the Hopf-Galois structures on K/k. The following theorem specifies the minimal Hopf-Galois structures inside this correspondence.

Theorem 6 (Fundamental criterion)**.** Let K/k be a finite separable extension. Let $\tilde{K}$ be the normal closure of K/k. Set $G = \mathrm{Gal}(\tilde{K}/k)$ and $G' = \mathrm{Gal}(\tilde{K}/K)$. Then the minimal Hopf-Galois structures on K/k are defined by the algebras $\tilde{K}[N]^G$ for which N is a regular subgroup of $\mathrm{Perm}(G/G')$ normalized by G such that N has no proper nontrivial subgroup normalized by G. In particular:

1. The number of minimal Hopf-Galois structures on K/k is greater than or equal to the number of normal complements N of G' in G such that N admits no proper nontrivial subgroup U which is a normal subgroup of G.

2. Assume that K/k has a Hopf-Galois structure defined by $\tilde{K}[N]^G$.

    a. If N has a nontrivial proper characteristic subgroup (this is the case when K/k is a Hopf-Galois extension of degree mp where p is a prime number and $p > m > 1$), then this structure is not minimal.

    b. If N has prime order, then the structure is minimal.

3. If K/k is a Galois extension whose Galois group is a simple group, then K/k has only one minimal Hopf-Galois structure.

Proof. Since the Hopf algebras providing a Hopf Galois structure on K/k are of the form $\tilde{K}[N]^G$, the assertion results from [9, Proposition 2.2].

1. This special case is an immediate consequence of [[7], Proposition 4.1].

2. a. Let N be a group of order mp where p is a prime number and $p > m > 1$. Then the unique p-Sylow of N is a nontrivial proper characteristic subgroup. So a Hopf-Galois extension of degree mp with p a prime number such that $p > m > 1$ is a special case of the situation that we are interested in. Assume now that N is a regular subgroup of $\mathrm{Perm}(G/G')$ normalized by G. So $\lambda(x)N\lambda(x)^{-1} \subset N$ for all $x \in G$, where λ is the faithful action described in Theorem 5. Assume also that N possesses at least one nontrivial proper characteristic subgroup U. Since G normalizes N, the maps $n \mapsto \lambda(x)n\lambda(x)^{-1}$ are automorphisms of N. We deduce that G also normalizes U. Hence k, $\tilde{K}[U]^G$ and $\tilde{K}[N]^G$ are distinct k-sub-Hopf algebras of $\tilde{K}[N]^G$ by [9, Proposition 2.2].

    b. In that case, N has no nontrivial proper subgroup. Therefore the only k-sub-Hopf algebras of $\tilde{K}[N]^G$ are k and $\tilde{K}[N]^G$ itself.

3. Assume first that the Galois group G of K/k is an abelian simple group. This means that G is a cyclic group with prime order. From the above item, we deduce that the classical Hopf-Galois structure defined by the group algebra $k[G]$ is a minimal one. This is the only Hopf-Galois structure on K/k by [1, Theorem 1]. On the other hand, assume that K/k is a Galois extension whose Galois group G is a nonabelian simple group. By [2, Theorem 1.1], there are exactly two Hopf-Galois structures on K/k. By [7, Theorem 5.3], we know that one of these structures comes from a Hopf algebra H giving rise to a bijective Galois correspondence between its k-sub-Hopf algebras and intermediate subfields $k \subseteq F \subseteq K$ which are normal over k. However, G is a simple group, therefore the only subfields which are normal over k are k itself and K. Thus, this Hopf-Galois structure is minimal. The other Hopf-Galois structure is the classical one, and it is obviously not minimal, since G

(nonabelian simple) does have nontrivial subgroups. That is, for nonabelian simple G as well, we have only one minimal Hopf-Galois structure.

QED

Remark 1. Concerning item 3 of Theorem 6, we would like to point out that one has precise information about the only two Hopf-Galois structures [2, Theorem 1.1] defined on a Galois extension K/k with nonabelian simple Galois group G. Indeed, one of them, the classical one, is given by the group algebra $H = k[G]$. The other one (the first one to be considered in the last paragraph) arises by taking $N = \lambda(G)$. Hence the action of G on N amounts to the conjugation action of G on itself. The k-Hopf algebra H' which results may be constructed for any G, and as soon as G is not abelian, H' is not isomorphic to H as a k-Hopf algebra.

3 Examples (part 1)

This section illustrates some of the minimal Hopf-Galois structures described in Theorem 6.

3.1 Example 1

Let K/k be a separable extension of degree $n \leq 4$ whose normal closure $\tilde{K}/k$ has Galois group G. Set $G' = \mathrm{Gal}(\tilde{K}/K)$. Assume that G' has a normal complement in G and $\mathrm{Perm}(G/G')$ is isomorphic to G. Then K/k has only one minimal Hopf-Galois structure. Indeed:

1. Assume $n = 2$. Since any separable extension of degree 2 is Galois, our assertion comes from the third item of Theorem 6.

2. Assume $n = 3$. Then G is isomorphic to the symmetric group S_3. The algebra $H = \tilde{K}[C_3]^{S_3}$ defines the only minimal Hopf-Galois structure on K/k.

3. Assume $n = 4$. Then G is isomorphic to S_4. Since:

   a. The Klein four-group $C_2 \times C_2$ is the unique normal subgroup of S_4 of order 4,

   b. C_2 is the unique proper nontrivial subgroup of the Klein four-group,

   c. C_2 is not a normal subgroup of S_4,

   we conclude that $\tilde{K}[C_2 \times C_2]^{S_4}$ defines the only minimal Hopf-Galois structure on K/k.

Remark 2. If K is a number field of degree 5 such that its normal closure $\tilde{K}/\mathbb{Q}$ has Galois group S_5, then $K/\mathbb{Q}$ has no Hopf Galois structure because S_5 admits no normal subgroup of order 5. There is another argument to see this in a more general way, see for instance [7, Proof of Counterexample 2.4].

3.2 Example 2

Hopf-Galois extensions without minimal structure.

1. Given an odd prime number p, it is easily seen that:

   a. No dihedral extension of degree $2p$ can have a minimal Hopf-Galois structure.

   b. No Galois extension whose Galois group is equal to the holomorph of the cyclic group C_p can have a minimal Hopf-Galois structure.

2. a. Let p be an odd prime and n a positive integer. Let k be a field of characteristic zero. Assume $K = k(w)$ with $w^{p^n} = a \in k$ where a is such that $[K : k] = p^n$ and let r denote the largest integer between 0 and n such that $K \cap k(\zeta_{p^r}) = k(\zeta_{p^r})$, where ζ_{p^r} denotes a primitive p^r-th root of unity. It is shown in [10] that if $r < n$ then there are p^r Hopf-Galois structures on K/k of type N, a cyclic group of order p^n. So if $n \geq 2$, then none of these p^r Hopf-Galois structures is a minimal one, since N does have characteristic subgroups.

   b. Assume that K/k is a cyclic extension of degree 2^n for $n \geq 3$. It is shown in [3] that K/k admits $3 \cdot 2^{n-2}$ Hopf Galois structures. Among them 2^{n-2} of cyclic type, 2^{n-2} of dihedral type and 2^{n-2} of generalized quaternion type. In fact, any of these structures is associated to a subgroup N of $\mathrm{Perm}(G/G')$ which has at least one nontrivial proper characteristic subgroup. Indeed:

   - If N is a cyclic group, then any subgroup of N is a characteristic subgroup. In the case when N has order 2^n for $n \geq 3$, there are at least 2 nontrivial proper characteristic subgroups.
   - If $N = D_{2^n}$ is a dihedral group, then its unique normal subgroup of order 2^{n-1} is a nontrivial proper characteristic subgroup.
   - If $N = Q_n$ is a generalized quaternion group, then its unique normal subgroup of order 2 is a nontrivial proper characteristic subgroup.

4 Minimal Hopf-Galois structures on almost classically Galois extensions

As before, we consider a separable field extension K/k of degree n, and we denote by $\tilde{K}$ its normal closure. Set G the Galois group of $\tilde{K}/k$ and G' the Galois group of $\tilde{K}/K$. We previously determined in Theorem 6 a lower bound of the number of minimal Hopf-Galois structures on K/k from normal complements of G' in G. By [7, Definition 4.2], the existence of a normal complement N of G' in G means that K/k is an almost classically Galois extension. This is equivalent to saying that G is equal to the semidirect product $G = N \rtimes_\varphi G'$. Note that any almost classically Galois extension has a Hopf-Galois structure. That is why these extensions are sometimes called almost classically Hopf-Galois extensions. If the normal complement N of G' in G is a cyclic group, one says that K/k is an *almost cyclic extension*, see [3]. Note that any Galois extension K/k is obviously almost classically Galois with $N = \mathrm{Gal}(K/k)$ and $G' = \{1\}$. In this section we are interested in minimal Hopf-Galois structures on almost classically Galois extensions K/k in the case when the Galois group $\mathrm{Gal}(\tilde{K}/k)$ is a subgroup of the holomorph of a characteristically simple group, subject to a certain condition. Recall that for any group N, the group $\mathrm{Inn}(N)$ of all inner automorphisms of N is a normal subgroup of $\mathrm{Aut}(N)$.

Lemma 1. With the above notation, assume that K/k is an almost classically Galois extension such that G is a semidirect product $N \rtimes H$, where N is any group and H is a subgroup of $\mathrm{Aut}(N)$ such that no nontrivial normal subgroup $U \subset N$ is fixed by all elements of H (this assumption is fulfilled in particular if N is characteristically simple and $\mathrm{Aut}(N) = H \cdot \mathrm{Inn}(N)$).

Then $\tilde{K}[N]^G$ defines a minimal Hopf-Galois structure on K/k.

Proof. By [9, Proposition 2.2], the Hopf-Galois structure on K/k defined by $\tilde{K}[N]^G$ is minimal if N has no proper nontrivial subgroup U which is a normal subgroup of $G = N \rtimes_\varphi H$. This means that there is no nontrivial subgroup U of N such that

$$[i_a \circ b](U) = U, \quad \text{for all } a \in N,\ b \in H,$$

where i_a stands for the inner automorphism of N associated to a. Recall that U is fixed by all i_a if and only if it is normal. Therefore the argument is complete, since our hypothesis on H is tailormade to ensure that no nontrivial normal subgroup U of N is fixed by all $b \in H$. QED

Simple groups obviously form a proper subfamily of characteristically simple groups. On the other hand, Galois extensions are almost classically Galois. We thus obtain more minimal Hopf-Galois structures from the study made in this

section than the one made in Section 2. Note that any characteristically simple group is the direct sum of finitely many copies of some simple group (see for instance [2, Lemma 3.2], [11, 3.3.15], or [12, Theorem 8.10]). The Klein four-group is the smallest abelian characteristically simple group which is not simple. Besides, the direct product $A_5 \times A_5$ is the smallest non-abelian characteristically simple group which is not simple. We already described in Example 3.1 minimal Hopf-Galois structures by using the Klein four-group and subgroups of symmetric groups. Lemma 1 allows us to construct even more examples.

5 Examples (part 2)

This section illustrates minimal Hopf-Galois structures stemming from Lemma 1 and Theorem 6.

5.1 Example 3

We are interested in minimal Hopf-Galois structures on some almost classically Galois extensions K/k of degree n such that $n \leq 9$, or $n = 2^r$ and $r \geq 2$.

1. Burnside's theorem in Group Theory states that if G is a finite group of order $p^\alpha q^\beta$ where p and q are prime numbers, α and β are non-negative integers, then G is solvable. On the other hand, Shafarevich showed that that every finite solvable group is realizable over $\mathbb{Q}$. Even if for $n \geq 5$ the symmetric group S_n and the alternating group A_n are not solvable, Hilbert proved that for any positive integer n, the symmetric group S_n and the alternating group A_n are realizable over $\mathbb{Q}$. In addition, Sonn showed in [13] that every finite group of order less than 672 is realizable over $\mathbb{Q}$. Hence for any positive integer $n \leq 11$, except for $n \in \{6, 10\}$, there exists an almost classically Galois extension $K/\mathbb{Q}$ of degree n having at least one minimal Hopf-Galois structure and whose normal closure satisfies $n \leq [\tilde{K} : \mathbb{Q}] < 672$. Indeed:

   a. Assume that n is a prime number ≤ 11. Then the dihedral group D_n is realizable over $\mathbb{Q}$. Let $\tilde{K}/\mathbb{Q}$ be a dihedral extension with Galois group D_n, and K be the fixed field of a chosen subgroup $H \subset D_n$ of order 2. Let $N \subset D_n$ be the unique normal complement of H. Then H and N satisfy the assumption of Lemma 1, and hence K is a number field of degree n which has a minimal Hopf-Galois structure.

   b. In case $n \in \{4, 8, 9\}$, the assertion will follow from subsection 5.2 below.

   c. The exceptional cases when $n \in \{6, 10\}$ are special cases of Theorem 6.

2. It is shown in [3, Corollary 5.7] that any Hopf-Galois structure on an almost cyclic extension of degree 2^r with $r \geq 2$ is of cyclic type. Hence, almost cyclic extensions of degree 2^r with $r \geq 2$ cannot have any minimal Hopf-Galois structures, since such extensions are defined by groups having at least one nontrivial proper characteristic subgroup.

5.2 Example 4

This subsection concerns number fields of degree $4, 8$, or 9.

1. Set $N = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This group N is characteristically simple. The automorphism group of N is $\mathrm{Aut}(N) = \mathrm{GL}_2(\mathbf{F}_2)$, a non-abelian group of order 6. Let H be the subgroup of $\mathrm{Aut}(N)$ generated by $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. The matrix A has exponent 3 and no eigenvalue in $\mathbb{Z}/2\mathbb{Z}$. Therefore no nontrivial subgroup of N is H-invariant. One can also check that the semidirect product $N \rtimes H$ is isomorphic to the alternating group A_4. Denote by $\tilde{K}$ a Galois extension of $\mathbb{Q}$ with Galois group $N \rtimes H$, and let K be the fixed field of H. Hence we may infer from Lemma 1 that $\tilde{K}[N]^{N \rtimes H}$ defines a minimal Hopf-Galois structure on $K/\mathbb{Q}$. By similar arguments, any almost classically Galois extension of degree 4 whose normal closure has Galois group equal to $\mathrm{Hol}(N)$ has a minimal Hopf-Galois structure.

2. Set $N = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which is again characteristically simple, and denote by H the subgroup of $\mathrm{Aut}(N) = \mathrm{GL}_3(\mathbf{F}_2)$ generated by $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$. It is easily checked that H is cyclic of order 7, so the semidirect product $G := N \rtimes H$ has order 56. Moreover A has no eigenvalues in $\mathbb{Z}/2\mathbb{Z}$, and this implies again that N has no nontrivial A-invariant subgroups. Let $\tilde{K}$ be a Galois extension of $\mathbb{Q}$ with Galois group G, and K the fixed field of H. By using Lemma 1 as in the preceding item, we see that $\tilde{K}[N]^G$ defines a minimal Hopf-Galois structure on $K/\mathbb{Q}$. Also, any almost classically Galois extension of degree 8 whose normal closure has Galois group equal to $\mathrm{Hol}(N)$ admits at least one minimal Hopf-Galois structure.

3. Set $N = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and denote by H the subgroup of $\mathrm{Aut}(N) = \mathrm{GL}_2(\mathbf{F}_3)$ generated by the matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, which has exponent 4. Consequently the semidirect product $G := N \rtimes H$ has order 36. Denote by $\tilde{K}$ a Galois extension of $\mathbb{Q}$ with Galois group G, and let K be the fixed field of G'. The same arguments as in the two previous items allow us to conclude that

$\tilde{K}[N]^G$ defines a minimal Hopf-Galois structure on $K/\mathbb{Q}$, and that any almost classically Galois extension of degree 9 whose normal closure has Galois group equal to $\mathrm{Hol}(N)$ has at least one minimal Hopf-Galois structure.

5.3 Example 5

In this last subsection of the body of the paper, we discuss minimal structures that arise from nonabelian characteristically simple groups.

We saw that the Galois group of the normal closure of an almost classically Galois extension is a semidirect product. So the study of minimal almost classically Hop-Galois structures takes us to the study of normal subgroups of semidirect products. In [14] Usenko described subgroups of semidirect products. In particular, he characterized semidirect products $G = N \rtimes_\varphi G'$ all of whose proper normal subgroups are contained in the centralizer of N in G. We describe here minimal Hopf-Galois structures arising from normal subgroups of special semidirect products. Let K/k be an almost classically Galois extension. Assume that the Galois group of its Galois closure $\tilde{K}$ is $G = \mathrm{Hol}(N)$, the holomorph of a nonabelian group N.

Then G has at least two distinct normal subgroups which are isomorphic to N. The first of them is the obvious one: $\Gamma_1 := \{(g; 1) \mid g \in N\}$. We will exhibit a nonobvious second such group. Recall that $\mathrm{Inn}(N)$ is the group of inner automorphisms of N; denote conjugation by $g \in N$ by i_g. We set

$$\Gamma_2 := \{(g^{-1}; i_g) \mid g \in N\}$$

and claim it has the required properties. From the definition of Γ_2, it is obvious that the map $f : N \to \Gamma_2$ that sends g to $(g^{-1}; i_g)$ is bijective. Moreover, a direct calculation shows that

$$(g^{-1}; i_g)(h^{-1}; i_h) = (h^{-1}g^{-1}; i_{gh})$$

for all $g, h \in N$, and hence f is an isomorphism of groups. Likewise one can check that Γ_2 is normal in G. Indeed one can show that $(g^{-1}; i_g)$ actually commutes with $(h; 1)$ for all $g, h \in N$, so $N \times 1$ centralizes Γ_2. And if we conjugate $(g^{-1}; i_g)$ by $(1; \theta)$, then we get, by another small calculation, the element $(\theta(g)^{-1}; i_{\theta(g)})$, which is again in Γ_2; so $1 \times \mathrm{Aut(N)}$ normalizes Γ_2. As N was assumed to be nonabelian, Γ_2 is obviously distinct from Γ_1. Therefore, if N is a characteristically simple group, then Γ_1 and Γ_2 define two distinct minimal Hopf-Galois structures on K/k by Lemma 1 and [7, Theorem 3.1].

6 Conclusion and Perspectives

This work presents Hopf-Galois structures defined by cocommutative Hopf algebras H on separable extensions in the extreme situation when H has only two sub-Hopf algebras. We first characterized these minimal structures in Theorem 6. Then we exhibited in Lemma 1 a special class of cases of almost classically Galois extensions; their normal closures have a Galois group G which is a specific type of subgroup of the holomorph of a characteristically simple group. We provided many illustrations of these two statements, actually giving examples constructed from characteristically simple groups, and also counterexamples constructed from groups having a nontrivial proper characteristic subgroup. The resulting separable field extensions have either no minimal Hopf-Galois structure, or exactly one minimal structure, or at least two minimal structures.

An interesting problem might be to determine an upper bound of the number of minimal Hopf-Galois structures on a degree n extension K/k (separable or not) according to n, in the case when the Galois group of the normal closure $\tilde{K}/k$ is equal to the holomorph of a characteristically simple group N. From classification of characteristically simple groups, one might also start by computing upper bounds of minimal Hopf-Galois structures of families of almost classically Galois extensions. Then one would be able to determine the maximal number of minimal Hopf-Galois structures which can be defined on a given almost classically Galois extension K/k such that $\mathrm{Gal}(\tilde{K}/k) = \mathrm{Hol}(N)$, according to the size of N.

Acknowledgments

The work reported in this paper is supported by the Simons Foundation via the PREMA project, and by the International Centre for Theoretical Physics (ICTP) via their Associate Scheme. The authors would like to thank the anonymous referee for the careful reading and many useful and apposite suggestions.

References

[1] N. P. Byott: *Uniqueness of Hopf-Galois structure for separable field extensions*, Comm. Algebra, **24**, 3217–3228, 1996.

[2] N. P. Byott: *Hopf-Galois structures on field extensions with simple Galois groups*, Bull. London Math. Soc, **36**, 23–29, 2004.

[3] N. P. Byott: *Hopf-Galois structures on almost cyclic field extensions of* 2*-power degree*, J. Algebra, **318**, 351–371, 2007.

[4] S. U. Chase, M. E. Sweedler: Hopf Algebras and Galois Theory, Lecture Notes in Mathematics, **97**, Springer-Verlag, New York/Berlin, 1969.

[5] Lindsay N. Childs: *On the Galois correspondence for Hopf Galois structures*, New York J. Math., 1–10, 2017.

[6] L. N. Childs, C. Greither: *Bounds on the number of ideals in finite commutative nilpotent* $\mathbf{F}_p$*-algebras*, Publ. Math. Debrecen, **92**, 495–516, 2018.

[7] C. Greither, B. Pareigis: *Hopf Galois theory for separable field extensions*, J. Algebra, **106**, 239–258, 1987.

[8] T. Crespo, A. Rio, M. Vela: *From Galois to Hopf-Galois: theory and practice*, Contemp. Math., **649**, 29–46, 2015.

[9] T. Crespo, A. Rio, M. Vela: *On the* Galois *correspondence theorem in separable* Hopf Galois *theory*, Publ. Mat. (Barcelona), **60**, 221–234, 2016.

[10] T. Kohl: *Classification of the Hopf-Galois structures on prime power radical extensions*, J. Algebra, **207**, 525–546, 1998.

[11] Derek J. S. Robinson: A course in the theory of groups, Grad. Texts in Math., New York, Springer, 1982.

[12] John S. Rose: A Course on Group Theory, Cambridge-New York-Melbourne, Cambridge University Press, 1978.

[13] Jack Sonn: *Groups of small order as Galois groups over* $\mathbb{Q}$, Rocky Mountain Journal of Mathematics, **19**, n. 3, 947–956, 1989.

[14] V. M. Usenko: *Subgroups of semidirect products*, Ukrainian Mathematical Journal, **43**, 982–988, 1991.