Received: 28 July 2022 | Revised: 24 November 2022 | Accepted: 7 December 2022

DOI: 10.1112/blms.12815

RESEARCH ARTICLE

Bulletin of the London Mathematical Society

On the connection between Hopf–Galois structures and skew braces

Lorenzo Stefanello[1] | **Senne Trappeniers**[2]

[1]Department of Mathematics, Università di Pisa, Pisa, Italy

[2]Department of Mathematics and Data Science, Vrije Universiteit Brussel, Brussels, Belgium

Correspondence
Lorenzo Stefanello, Department of Mathematics, Università di Pisa, Largo Bruno Pontecorvo 5, 56127 Pisa, Italy.
Email: lorenzo.stefanello@phd.unipi.it

Funding information
Fonds voor Wetenschappelijk Onderzoek - Vlaanderen, Grant/Award Number: 1160522N

Abstract

We present a different version of the well-known connection between Hopf–Galois structures and skew braces, building on a recent paper of A. Koch and P. J. Truman. We show that the known results that involve this connection easily carry over to this new perspective, and that new ones naturally appear. As an application, we present new insights on the study of the surjectivity of the Hopf–Galois correspondence, explaining in more detail the role of bi-skew braces in Hopf–Galois theory.

MSC 2020
12F10, 16T05, 20N99 (primary)

1 | INTRODUCTION

Let L/K be a finite extension of fields. A Hopf–Galois structure on L/K consists of a K-Hopf algebra H together with an action of H on L that satisfies certain technical conditions. When L/K is Galois with Galois group G, the prototypical example consists of the group algebra $K[G]$ with the usual Galois action on L; indeed, the required properties for a Hopf–Galois structure mimic precisely those of this structure, which is called the classical structure.

Hopf–Galois theory was initially introduced in the context of purely inseparable extensions by Chase and Sweedler [18], but after it was mainly studied for separable extensions, providing a generalisation of classical Galois theory. In the particular case in which the extension is also Galois, Hopf–Galois structures have been shown to be extremely useful in dealing with problems in arithmetic. For example, as discussed by Byott in [6], there are situations in which the Galois module structure of an extension of p-adic fields can be better described in a Hopf–Galois structure different from the classical one; see [11, 12] for a detailed analysis on the role of Hopf–Galois theory in local Galois module theory.

A main role in the development of this theory was played by a groundbreaking result of Greither and Pareigis [23]. We assume that L/K is Galois with Galois group G, which is the case of interest in the paper, underlining that the result can be stated also for separable non-normal extensions. Then there exists a bijective correspondence between Hopf–Galois structures on L/K and regular subgroups of the permutation group $\mathrm{Perm}(G)$ of G normalised by $\lambda(G)$, the image of G under the left regular representation. For example, $\rho(G)$, the image of G under the right regular representation, corresponds to the classical structure, while $\lambda(G)$ corresponds to the so-called canonical nonclassical structure, different from the classical one when G is not abelian. We define the type of a Hopf–Galois structure to be the isomorphism class of the corresponding regular subgroup of $\mathrm{Perm}(G)$.

This result was followed by new approaches to the theory, and problems of existence and classification have been studied by several authors; given a group N, does there exist a Hopf–Galois structure of type N on L/K? Can we classify and count the Hopf–Galois structures on L/K? A precise survey of the main results developed in the last years can be found in [11].

A deep problem that can be approached with Greither–Pareigis theory regards the surjectivity of the Hopf–Galois correspondence. Given a Hopf–Galois structure on L/K with K-Hopf algebra H, we can attach to each K-sub Hopf algebra of H an intermediate field of L/K in a natural way. The correspondence we get is called the Hopf–Galois correspondence, which can be shown to be injective [18] but not necessarily surjective. For example, if we consider the classical structure, then we recover the usual Galois correspondence, which is surjective. But it was proved in [23] that if we consider the canonical nonclassical structure, then the image of the Hopf–Galois correspondence consists precisely of the normal intermediate fields of L/K; this shows that if G is Hamiltonian (that is, nonabelian with all the subgroups normal), then the Hopf–Galois correspondence is surjective, but as soon as the group is not abelian nor Hamiltonian, we find a Hopf–Galois structure for which the Hopf–Galois correspondence is not surjective.

More generally, given a Hopf–Galois structure on L/K with Hopf algebra H corresponding to a regular subgroup N of $\mathrm{Perm}(G)$ normalised by $\lambda(G)$, we know that there exists a bijective correspondence between K-sub Hopf algebras of H and subgroups of N normalised by $\lambda(G)$; the first explicit proof of this fact can be found in [17, Proposition 2.2]. As there always exists a bijective correspondence between intermediate fields of L/K and subgroups of the Galois group G, we can translate the Hopf–Galois correspondence to find a correspondence between subgroups of N normalised by $\lambda(G)$ and subgroups of G. This means that for groups of small order the problem can be approached from a quantitative point of view; in [26], the authors used GAP [22] to deal with groups of order 42 and found some nonclassical Hopf–Galois structures for which the number of subgroups of the Galois group G equals the number of subgroups of N normalised by $\lambda(G)$, meaning that the Hopf–Galois correspondence for these structures is surjective.

A look in the literature seems to suggest that these cases are not really common. Beside these examples and the aforementioned classical structure and canonical nonclassical structure when G is Hamiltonian, there exists only one other known class of Hopf–Galois structures for which the Hopf–Galois correspondence is surjective; this was obtained from the study of the connection between Hopf–Galois structures and skew braces, objects introduced by Guarnieri and Vendramin [24], building on the pioneering work of Rump [35]. Skew braces are related with several other topics, such as radical rings, solutions of the Yang–Baxter equation, and the holomorph of a group. In particular, they are connected with regular subgroups of permutation groups, and in this way, also with Hopf–Galois structures. This connection, which is not

bijective, was initially suggested in [3] and then made precise in the appendix of Byott and Vendramin in [39].

Thanks to this connection, the problem of the surjectivity of the Hopf–Galois correspondence was translated into a different language by Childs [13, 14], who showed that given a Hopf–Galois structure on L/K with Hopf algebra H, there exists a bijective correspondence between K-sub Hopf algebras of H and certain substructures of the associated skew brace. In this way, Childs proved that for all the Hopf–Galois structures on a Galois extension with Galois group cyclic of odd prime power order, the Hopf–Galois correspondence is surjective.

Despite this promising start, to the best knowledge of the authors, no further examples of this behaviour have been found. A new approach, introduced in [16], seems to suggest how difficult it is to find them. Namely, instead of looking for Hopf–Galois structures for which the Hopf–Galois correspondence is surjective, one can study the failure of the surjectivity. Given a Hopf–Galois structure on L/K with Hopf algebra H, how far is the Hopf–Galois correspondence from being surjective? The idea is to compute (or estimate) the ratio between the number of K-sub Hopf algebras of H and the number of intermediate fields of L/K, which was translated by Childs in a problem regarding just the associated skew brace.

A possible explanation for the lack of new examples could be given by the fact that the substructures of skew braces studied by Childs, which seem to arise naturally from Hopf–Galois theory, are not the usual substructures considered in the theory of the skew braces, namely, left ideals, strong left ideals, and ideals. This issue was initially addressed by Koch and Truman [32], who considered the notion of opposite skew brace and showed that the substructures studied by Childs coincide with left ideals of the opposite skew brace. They moved the problem to a more familiar setting, and combined this observation with the results of [26] to describe some known properties of Hopf–Galois structures in terms of the opposite skew brace.

This intuition is at the very base of this paper, where we present a new version of the known connection between Hopf–Galois structures and skew braces, as per the following points.

(1) Use directly the opposite skew brace.
(2) Make the connection bijective.
(3) Forget about the regular subgroup.

The idea is that using this new point of view one can explicitly see how the knowledge of the structure of a skew brace gives useful and qualitative information for the associated Hopf–Galois structure. In particular, the role of bi-skew braces, certain skew braces introduced by Childs [15] and then further studied by Caranti [9] and the authors [38], seems to appear in a more transparent way from this new perspective, for example, in order to find Hopf–Galois structures for which the Hopf–Galois correspondence is surjective.

The paper is organised as follows. In Section 2, we introduce the necessary preliminaries on Hopf–Galois structures, skew braces, and their connections. We also recall the tool of Galois descent, useful throughout the rest of the paper. In Section 3, we explicitly describe the new connection we propose. We remark how the known advantages of the usual connection still apply in the new perspective, and we see how some old and new results can be explained and derived. In Section 4, we use the new point of view to deal with the Hopf–Galois correspondence. In particular, we present new qualitative results, examples, and statements to explain why, in some situations, the Hopf–Galois correspondence is surjective, from a more general perspective. A main role here is played by bi-skew braces.

2 | PRELIMINARIES

2.1 | Hopf–Galois structures

Let L/K be a finite extension of fields. A *Hopf–Galois structure* on L/K consists of a K-Hopf algebra H together with an action $\star$ of H on L such that L is an H-module algebra and the K-linear map

$$L \otimes_K H \to \mathrm{End}_K(L), \quad x \otimes h \mapsto (y \mapsto x(h \star y))$$

is bijective. (We remark that two isomorphic K-Hopf algebras whose action on L respect the isomorphism give the same structure.) For more insights on the definition, we refer to [12].

For example, when L/K is Galois with Galois group G, the *classical structure* consists of the group algebra $K[G]$ together with the usual Galois action.

Following [18], given a Hopf–Galois structure on L/K with K-Hopf algebra H, we can attach to each K-sub Hopf algebra H' of H an intermediate field F of L/K, as follows:

$$F = L^{H'} = \{x \in L \mid h' \star x = \varepsilon(h')x \text{ for all } h' \in H'\},$$

where ε denotes the counit of H'. We obtain in this way the *Hopf–Galois correspondence*, which is always injective. We remark that the F-Hopf algebra $F \otimes_K H'$ acts on L naturally and gives a Hopf–Galois structure on L/F, and in particular, $[L : F]$ equals the dimension of H' as K-vector space; see also [11, Section 7] for more details.

A K-sub Hopf algebra H' of H is *normal* if for all $h \in H$ and $h' \in H'$,

$$\sum_{(h)} h_{(1)}h'S(h_{(2)}) \in H', \quad \sum_{(h)} S(h_{(1)})h'h_{(2)} \in H',$$

where, in Sweedler's notation, the image of h under the comultiplication Δ of H is $\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)}$, and S denotes the antipode of H. If H' is a normal K-sub Hopf algebra of H, then by [34, Lemma 3.4.2 and Proposition 3.4.3] there exists a short exact sequence

$$K \to H' \to H \to \overline{H} \to K$$

of K-Hopf algebras, in the sense of [1, Proposition 1.2.3]. Moreover, if $F = L^{H'}$, then the action of H on L yields an action of $\overline{H}$ on F which gives a Hopf–Galois structure on F/K; see [7, Lemma 4.1].

We recall that $h \in H$ is a *grouplike element* if $\Delta(h) = h \otimes h$.

One fundamental tool in this theory is given by Galois descent; we briefly recall it here for the convenience of the reader, summarising [12, Section 2.12]. Suppose that L/K is Galois with Galois group G. Given an L-Hopf algebra M on which G acts semilinearly, we say that M is *G-compatible* if all the maps defining the structure of M as an L-Hopf algebra are G-equivariant. (Here G acts on L via Galois action and on $M \otimes_L M$ diagonally.)

Denote by $\mathcal{K}$ the category of K-Hopf algebras, where morphisms are K-Hopf algebra homomorphisms, and by $\mathcal{L}$ the category of G-compatible L-Hopf algebras, where morphisms are G-equivariant L-Hopf algebra homomorphisms. Then there exists an equivalence of categories between $\mathcal{K}$ and $\mathcal{L}$, as follows.

- If $H \in \mathcal{K}$, then $L \otimes_K H \in \mathcal{L}$, where here G acts on the first factor of the tensor product; given a morphism $\varphi : H_1 \to H_2$ in $\mathcal{K}$, we have that $\mathrm{id} \otimes \varphi : L \otimes_K H_1 \to L \otimes_K H_2$ is a morphism in $\mathcal{L}$.
- If $M \in \mathcal{L}$, then $M^G = \{m \in M \mid G \text{ acts trivially on } m\} \in \mathcal{K}$; given a morphism $\psi : M_1 \to M_2$ in $\mathcal{L}$, the restriction of ψ to M_1^G is a morphism $M_1^G \to M_2^G$.
- If $H \in \mathcal{K}$, then

$$H \to (L \otimes_K H)^G, \quad h \mapsto 1 \otimes h$$

is an isomorphism in $\mathcal{K}$, and if $M \in \mathcal{L}$, then

$$L \otimes_K M^G \to M, \quad l \otimes m \mapsto lm$$

is an isomorphism in $\mathcal{L}$.

We immediately derive some consequences.

- Let $M \in \mathcal{L}$. Then there exists a bijective correspondence between K-sub Hopf algebras of M^G and L-sub Hopf algebras of M which are invariant under the action of G on M. Explicitly, given such an L-sub Hopf algebra M', the corresponding K-sub Hopf algebra is $(M')^G$, and M' is normal in M if and only if $(M')^G$ is normal in M^G.
- Let

$$L \to A \to M \to B \to L$$

be a short exact sequence of L-Hopf algebras. If all the L-Hopf algebras are G-compatible and all the L-Hopf algebra homomorphisms are G-equivariant, then

$$K \to A^G \to M^G \to B^G \to K$$

is a short exact sequence of K-Hopf algebras.
- For all $M_1, M_2 \in \mathcal{L}$, we have that $(M_1 \otimes_L M_2)^G$ and $M_1^G \otimes_K M_2^G$ are isomorphic as K-Hopf algebras.
- Let $M \in \mathcal{L}$, and take $h \in M^G$. Then h is a grouplike element of M^G if and only if h is a grouplike element of M.

Example 2.1. Let N be a finite group on which G acts via automorphisms, and extend this to an action of G on $L[N]$, where G acts on L via Galois action. Then it is straightforward to check that $L[N] \in \mathcal{L}$. Here the L-sub Hopf algebras of $L[N]$ are the group algebras $L[N']$ for subgroups N' of N (see [17, Proposition 2.1]), and almost by definition, $L[N']$ is normal in $L[N]$ if and only if N' is normal in N. We deduce that the K-sub Hopf algebras of $L[N]^G$ are of the form $L[N']^G$ for subgroups N' of N invariant under the action of G, and $L[N']^G$ is normal in $L[N]^G$ if and only if N' is normal in N. Note that moreover, the lattices of K-sub Hopf algebras of $L[N]^G$ and subgroups of N invariant under the action of G, with the usual binary operations, are isomorphic.

If N' is a normal subgroup of N invariant under the action of G, then, by [12, Proposition 4.14],

$$L \to L[N'] \to L[N] \to L[N/N'] \to L$$

is a short exact sequence of L-Hopf algebras which are G-compatible, where all the L-Hopf algebra homomorphisms are G-equivariant, so

$$K \to L[N']^G \to L[N]^G \to L[N/N']^G \to K$$

is a short exact sequence of K-Hopf algebras.

Finally, as the grouplike elements of $L[N]$ are the elements of N, we find that the grouplike elements of $L[N]^G$ are the elements of N on which G acts trivially.

We conclude by mentioning [23, Theorem 2.1], whose proof heavily relies on Galois descent, which gives a description of the K-Hopf algebras arising in this theory. Recall that a subgroup N of $\mathrm{Perm}(G)$ is *regular* if the map

$$N \to G, \quad \eta \mapsto \eta[1]$$

is a bijection. For example, $\lambda(G)$ and $\rho(G)$ are regular subgroups of $\mathrm{Perm}(G)$, where for all $\sigma, \tau \in G$,

$$\lambda(\sigma)[\tau] = \sigma\tau, \quad \rho(\sigma)[\tau] = \tau\sigma^{-1}.$$

Then there exists a bijective correspondence between Hopf–Galois structures on L/K and regular subgroups of $\mathrm{Perm}(G)$ normalised by $\lambda(G)$; explicitly, if N is such a subgroup, then we can consider the L-Hopf algebra $L[N]$, where G acts on L via Galois action and on N via conjugation by $\lambda(G)$, and then via Galois descent take the K-Hopf algebra $L[N]^G$, which gives a Hopf–Galois structure on L/K with the following action on L:

$$\left(\sum_{\eta \in N} a_\eta \eta\right) \star x = \sum_{\eta \in N} a_\eta (\eta^{-1}[1])(x).$$

As already mentioned, $\rho(G)$ corresponds to the classical structure, while $\lambda(G)$ corresponds to the so-called *canonical nonclassical structure*. We say that the *type* of a Hopf–Galois structure is the isomorphism class of the corresponding regular subgroup N of $\mathrm{Perm}(G)$.

2.2 | Skew braces

A *skew (left) brace* is a triple $(G, \cdot, \circ)$, where $(G, \cdot)$ and $(G, \circ)$ are groups and the following property holds: for all $\sigma, \tau, \kappa \in G$,

$$\sigma \circ (\tau \cdot \kappa) = (\sigma \circ \tau) \cdot \sigma^{-1} \cdot (\sigma \circ \kappa),$$

where σ^{-1} denotes the inverse of σ in $(G, \cdot)$. We denote by $\overline{\sigma}$ the inverse of σ with respect to $(G, \circ)$. It is easy to prove that for a skew brace $(G, \cdot, \circ)$, the identities of $(G, \cdot)$ and $(G, \circ)$ coincide. The *order* of a skew brace is the cardinality of the underlying set G.

For example, given a group $(G, \circ)$, we have that $(G, \circ, \circ)$ is a skew brace, which is said to be *trivial*. Similarly, if we define $\sigma \circ_{\mathrm{op}} \tau = \tau \circ \sigma$, then $(G, \circ_{\mathrm{op}}, \circ)$ is a skew brace, which is said to be

almost trivial. More generally, if $(G, \cdot, \circ)$ is a skew brace, then also $(G, \cdot_{\mathrm{op}}, \circ)$ is a skew brace, called the *opposite skew brace* of $(G, \cdot, \circ)$.

Notation 2.2. Given a skew brace $(G, \cdot, \circ)$, if we want to apply a group theoretical construction with respect to one of the group operations, then we write the operation as subscript, to avoid ambiguity. For example, we write $\iota_{\cdot}(\sigma)$ to denote conjugation by σ in $(G, \cdot)$, for $\sigma \in G$.

With each element σ of a skew brace $(G, \cdot, \circ)$ we can associate the bijective map

$$\gamma(\sigma) : G \to G, \quad \tau \mapsto {}^{\gamma(\sigma)}\tau = \sigma^{-1} \cdot (\sigma \circ \tau).$$

This yields a group homomorphism

$$\gamma : (G, \circ) \to \mathrm{Aut}(G, \cdot);$$

see [24, Proposition 1.9]. The map γ, which is called the called the *gamma function* of $(G, \cdot, \circ)$, gives an action of $(G, \circ)$ on $(G, \cdot)$ via automorphisms.

For example, the gamma function of $(G, \cdot, \cdot)$ is given by $\gamma(\sigma) = \mathrm{id}$. Also, if γ is the gamma function of a skew brace $(G, \cdot, \circ)$, then the gamma function of $(G, \cdot_{\mathrm{op}}, \circ)$ is given by $\iota_{\cdot}(\sigma)\gamma(\sigma)$, as an easy computation shows.

Consider two skew braces $(G_1, \cdot, \circ)$ and $(G_2, \cdot, \circ)$. A *skew brace homomorphism* is a map $f : G_1 \to G_2$ such that $f(\sigma \cdot \tau) = f(\sigma) \cdot f(\tau)$ and $f(\sigma \circ \tau) = f(\sigma) \circ f(\tau)$ for all $\sigma, \tau \in G_1$. *Skew brace isomorphisms* and *automorphisms* are defined accordingly, and we denote by $\mathrm{Aut}(G, \cdot, \circ)$ the group of skew brace automorphisms of $(G, \cdot, \circ)$.

Let $(G, \cdot, \circ)$ be a skew brace. A *left ideal* of $(G, \cdot, \circ)$ is a subgroup G' of $(G, \cdot)$ that is invariant under the action of $(G, \circ)$ via the gamma function γ of $(G, \cdot, \circ)$. Note that this immediately implies that G' is also a subgroup of $(G, \circ)$, so $(G', \cdot, \circ)$ is a skew brace, and that actually we can also replace 'subgroup of $(G, \cdot)$' with 'subgroup of $(G, \circ)$' in the definition. If G' is normal in $(G, \cdot)$, then we say that G' is a *strong left ideal*; if G' is also normal in $(G, \circ)$, then we say that G' is an *ideal*. In this last case, the quotient $(G/G', \cdot, \circ)$ is a skew brace in a natural way.

For example,

$$\mathrm{Fix}(G, \cdot, \circ) = \{\tau \in G \mid {}^{\gamma(\sigma)}\tau = \tau \text{ for all } \sigma \in G\}$$

is a left ideal of $(G, \cdot, \circ)$; see [21, Proposition 1.6].

It is clear that the characteristic subgroups of $(G, \cdot)$ are strong left ideals of $(G, \cdot, \circ)$. More generally, the strong left ideals of $(G, \cdot, \circ)$ are precisely the left ideals of $(G, \cdot, \circ)$ which are also left ideals of $(G, \cdot_{\mathrm{op}}, \circ)$, because of the description of the gamma function of $(G, \cdot_{\mathrm{op}}, \circ)$.

A skew brace $(G, \cdot, \circ)$ is *metatrivial* if there exists an ideal G' of $(G, \cdot, \circ)$ such that $(G', \cdot, \circ)$ and $(G/G', \cdot, \circ)$ are trivial skew braces. For example, by [4, Theorem 2.12], all the skew braces that can be obtained with [38, Theorem 6.6] are metatrivial.

Let $(G_1, \cdot, \circ)$ and $(G_2, \cdot, \circ)$ be skew braces. Following [39], given a group homomorphism

$$\alpha : (G_2, \circ) \to \mathrm{Aut}(G_1, \cdot, \circ),$$

we can define a *semidirect product* of $(G_1, \cdot, \circ)$ and $(G_2, \cdot, \circ)$ to be the skew brace $(G, \cdot, \circ)$, where $G = G_1 \times G_2$ as set, with $(G, \cdot) = (G_1, \cdot) \times (G_2, \cdot)$ and $(G, \circ) = (G_1, \circ) \rtimes (G_2, \circ)$, where the

semidirect product is taken with respect to α. When α is the trivial group homomorphism, we find the *direct product* of skew braces,

$$(G_1, \cdot, \circ) \times (G_2, \cdot, \circ).$$

We can generalise the notion of direct product to any finite number of skew braces. Note that the gamma function of the direct product of skew braces $(G_i, \cdot, \circ)$ is given by the gamma functions of the skew braces $(G_i, \cdot, \circ)$ in the obvious way.

If $(G, \cdot, \circ)$ is a skew brace isomorphic to a semidirect product of skew braces, then there exist an ideal G_1 and a strong left ideal G_2 of $(G, \cdot, \circ)$ such that $(G, \circ)$ is the inner semidirect product of $(G_1, \circ)$ and $(G_2, \circ)$, and $(G, \cdot)$ is the inner direct product of $(G_1, \cdot)$ and $(G_2, \cdot)$. When the semidirect product is a direct product, also G_2 is an ideal of $(G, \cdot, \circ)$.

Finally, a *bi-skew brace* is a skew brace $(G, \cdot, \circ)$ such that also $(G, \circ, \cdot)$ is a skew brace. If $(G, \cdot, \circ)$ is a bi-skew brace and γ is the gamma function of $(G, \cdot, \circ)$, then the gamma function γ' of $(G, \circ, \cdot)$ is given by $\gamma'(\sigma) = \gamma(\sigma)^{-1} = \gamma(\overline{\sigma})$; see [9, Section 3]. By [10, table at page 1175], a skew brace is a bi-skew brace if and only if its gamma function has values in $\mathrm{Aut}(G, \circ)$. If $(G, \cdot, \circ)$ is a bi-skew brace, then the left ideals of $(G, \cdot, \circ)$ and $(G, \circ, \cdot)$ coincide; see [38, Lemma 3.1].

2.3 | Hopf–Galois structures and skew braces

We recall the well-known connection between Hopf–Galois structures and skew braces. While it was originally developed in the appendix of Byott and Vendramin in [39], we present here an equivalent version, which does not involve explicitly the holomorph, as described in [41, Proposition 2.1] (see also [11, Section 2.8]). This is based on the following result, which is a slight reformulation of [24, Theorem 4.2].

Theorem 2.3. *Let $(G, \cdot)$ and $(G, \circ)$ be groups with the same identity. Then $(G, \cdot, \circ)$ is a skew brace if and only if $\lambda_\cdot(G)$ is normalised by $\lambda_\circ(G)$ in* $\mathrm{Perm}(G)$.

Let L/K be a finite Galois extension of fields with Galois group $(G, \circ)$.

- Consider a Hopf–Galois structure on L/K, corresponding to a regular subgroup N of $\mathrm{Perm}(G)$ normalised by $\lambda_\circ(G)$. We can use the bijection

$$N \to G, \quad \eta \mapsto \eta[1]$$

  to transport the group structure of N to G. In this way, we find a group structure $(G, \cdot)$ for which it is immediate to show that $\lambda_\cdot(G) = N$. By Theorem 2.3, we conclude that $(G, \cdot, \circ)$ is a skew brace.
- Let $(A, \cdot, \circ)$ be a skew brace with $(A, \circ) \cong (G, \circ)$. Use this bijection to transport the structure of $(A, \cdot)$ to G, to find a skew brace $(G, \cdot, \circ)$ isomorphic to $(A, \cdot, \circ)$. By Theorem 2.3, we have that $N = \lambda_\cdot(G)$ is normalised by $\lambda_\circ(G)$, so we obtain a Hopf–Galois structure on L/K.

Example 2.4. Peculiarly, under this connection, the classical structure yields the almost trivial skew brace. On the other hand, the trivial skew brace is obtained by the canonical nonclassical structure.

We immediately state an important and well-known consequence.

Theorem 2.5. *Let N and G be finite groups. Then the following are equivalent.*

- *There exists a skew brace $(A, \cdot, \circ)$ with $(A, \cdot) \cong N$ and $(A, \circ) \cong G$.*
- *There exists a Hopf–Galois structure of type N on every Galois extension of fields with Galois group isomorphic to G.*

Remark 2.6. A bi-skew brace $(A, \cdot, \circ)$ of finite order yields not only a Hopf–Galois structure of type $(A, \cdot)$ on every Galois extension of fields with Galois group isomorphic $(A, \circ)$, but also a Hopf–Galois structure of type $(A, \circ)$ on every Galois extension of fields with Galois group isomorphic to $(A, \cdot)$.

We underline that the previous connection is not bijective, as distinct Hopf–Galois structures can correspond to isomorphic skew braces. This was precisely quantified in [41, Corollary 2.4]; see also [33, Corollary 3.1] and Section 3. However, there is a way to obtain from this connection a bijective correspondence. Indeed, as a consequence of Theorem 2.3 (see [20, Section 7]), given a group $(G, \circ)$, there exists a bijective correspondence between group operations $\cdot$ such that $(G, \cdot, \circ)$ is a skew brace and regular subgroups of $\mathrm{Perm}(G)$ normalised by $\lambda_\circ(G)$, via

$$\cdot \mapsto \lambda_\cdot(G).$$

In this way, given a finite Galois extension of fields L/K with Galois group $(G, \circ)$, we obtain a bijective correspondence between operations $\cdot$ such that $(G, \cdot, \circ)$ is a skew brace and Hopf–Galois structure on L/K, which is a key observation for our new point of view.

3 | THE NEW CONNECTION

We begin with our main result, in which we propose a new version of the connection between Hopf–Galois structures and skew braces. We underline that some of the consequences, as developed in this section, can also be obtained from the usual theory, for example, from [26], together with the observations on opposite skew braces in [32, Theorem 5.6]. However, we prefer to develop directly the theory from this new perspective, to highlight how old and new statements can be derived in a transparent way, without too much effort.

Theorem 3.1. *Let L/K be a finite Galois extension of fields with Galois group $(G, \circ)$. Then the following data are equivalent:*

- *a Hopf–Galois structure on L/K;*
- *an operation $\cdot$ such that $(G, \cdot, \circ)$ is a skew brace.*

Explicitly, given an operation $\cdot$ such that $(G, \cdot, \circ)$ is a skew brace, we can consider the Hopf–Galois structure on L/K consisting of the K-Hopf algebra $L[G, \cdot]^{(G,\circ)}$, where $(G, \circ)$ acts on L via Galois action and on $(G, \cdot)$ via the gamma function of $(G, \cdot, \circ)$, with action on L given as follows:

$$\left(\sum_{\sigma \in G} \ell_\sigma \sigma\right) \star x = \sum_{\sigma \in G} \ell_\sigma \sigma(x).$$

Proof. Denote by $\mathcal{S}$ the set of group operations $\cdot$ on G such that $(G, \cdot, \circ)$ is a skew brace, and by $\mathcal{R}$ the set of regular subgroups of $\mathrm{Perm}(G)$ normalised by $\lambda_\circ(G)$. Consider the composition

$$\mathcal{S} \to \mathcal{S} \to \mathcal{R},$$

where the first map is the bijection that sends $\cdot$ to $\cdot_{\mathrm{op}}$ and the second map is the bijection that sends $\cdot$ to $\lambda_\cdot(G)$, as described at the end of Section 2. Since $\lambda_{\cdot_{\mathrm{op}}}(G) = \rho_\cdot(G)$, we obtain a bijection

$$\mathcal{S} \to \mathcal{R}, \quad \cdot \mapsto \rho_\cdot(G),$$

which by Greither–Pareigis theory yields the equivalence of data in the statement.

We just need to show that the Hopf–Galois structures on L/K can be described in the claimed way. So take an operation $\cdot$ such that $(G, \cdot, \circ)$ is a skew brace. Clearly $(G, \cdot) \cong \rho_\cdot(G)$, via the map

$$\sigma \mapsto \rho_\cdot(\sigma).$$

This yields an L-Hopf algebra isomorphism $L[G, \cdot] \to L[\rho_\cdot(G)]$. Let $(G, \circ)$ act on $(G, \cdot)$ via the gamma function of $(G, \cdot, \circ)$. We show that this isomorphism is also $(G, \circ)$-equivariant. It is enough to show that for all $\sigma, \tau \in G$,

$$\rho_\cdot({}^{\gamma(\sigma)}\tau) = \lambda_\circ(\sigma)\rho_\cdot(\tau)\lambda_\circ(\sigma)^{-1}.$$

The claim follows because the left-hand side element is the unique element of $\rho_\cdot(G)$ which sends $1 \in G$ to

$$({}^{\gamma(\sigma)}\tau)^{-1} = {}^{\gamma(\sigma)}(\tau^{-1}) = \sigma^{-1} \cdot (\sigma \circ \tau^{-1}),$$

while the right-hand side element is the unique element of $\rho_\cdot(G)$ which sends $1 \in G$ to

$$\sigma \circ (\overline{\sigma} \cdot \tau^{-1}) = (\sigma \circ \overline{\sigma}) \cdot \sigma^{-1} \cdot (\sigma \circ \tau^{-1}) = \sigma^{-1} \cdot (\sigma \circ \tau^{-1}).$$

By Galois descent, we derive that $L[G, \cdot]^{(G,\circ)}$ and $L[\rho_\cdot(G)]^{(G,\circ)}$ are isomorphic as K-Hopf algebras, and the isomorphism is given as follows:

$$\sum_{\sigma \in G} \ell_\sigma \sigma \mapsto \sum_{\sigma \in G} \ell_\sigma \rho_\cdot(\sigma).$$

To conclude, we need to find the action of $L[G, \cdot]^{(G,\circ)}$ on L that respects this isomorphism:

$$\begin{aligned}\left(\sum_{\sigma \in G} \ell_\sigma \sigma\right) \star x = \left(\sum_{\sigma \in G} \ell_\sigma \rho_\cdot(\sigma)\right) \star x &= \sum_{\sigma \in G} \ell_\sigma (\rho_\cdot(\sigma)^{-1}[1])(x) \\ &= \sum_{\sigma \in G} \ell_\sigma \sigma(x).\end{aligned}$$

□

Remark 3.2. We believe that this point of view could simplify computation. Indeed, note the similarities of the Hopf–Galois action described in Theorem 3.1 with the usual Galois action. Also, an

important role is played by the gamma function, which is a well-known and studied feature of a skew brace.

Remark 3.3. Following the proof of Theorem 3.1, it should be clear that we are associating with a Hopf–Galois structure on L/K the skew brace that is opposite to the usual one. Explicitly, given a Hopf–Galois structure in Greither–Pareigis terms, so a regular subgroup N of $\mathrm{Perm}(G)$ normalised by $\lambda_\circ(G)$, then the way to find the operation $\cdot$ associated to this structure is the following:

$$\sigma \cdot \tau = \nu(\nu^{-1}(\tau)\nu^{-1}(\sigma)),$$

where $\nu : N \to G$ is the usual bijection that maps η to $\eta[1]$.

For the rest of the section, we fix a finite Galois extension L/K with Galois group $(G, \circ)$.

Notation 3.4. To lighten the notation, we associate a Hopf–Galois structure on L/K with a skew brace $(G, \cdot, \circ)$, implicitly meaning the operation $\cdot$ such that $(G, \cdot, \circ)$ is a skew brace.

We immediately see that the new version of the connection fixes the peculiar behaviour described in Example 2.4.

Example 3.5.

- Consider the trivial skew brace $(G, \circ, \circ)$. As the gamma function in this case is given by $\gamma(\sigma) = \mathrm{id}$, we find that the Hopf algebra in the Hopf–Galois structure on L/K associated with $(G, \circ, \circ)$ is $K[G, \circ]$, and we recover the classical structure.
- If instead we consider the almost trivial skew brace $(G, \circ_{\mathrm{op}}, \circ)$, we find the Hopf–Galois structure on L/K originally corresponding to $\lambda_\circ(G)$, that is, the canonical nonclassical structure.

Example 3.6. Let A and B be finite groups. Consider a group homomorphism $\alpha : B \to \mathrm{Aut}(A)$, and suppose that $(G, \circ)$ is the semidirect product of A and B with respect to α. Given $(a, b) \in G$ and $x \in L$, write $(a, b)(x)$ for the Galois action. Finally, take $(G, \cdot) = A \times B$. Then by [24, Example 1.4], we have that $(G, \cdot, \circ)$ is a skew brace. We obtain a Hopf–Galois structure on L/K, which we now describe.

First, a straightforward calculation shows that the gamma function of $(G, \cdot, \circ)$ is given as follows:

$$\gamma(c,d)(a, b) = ({}^{\alpha(d)}a, b).$$

In particular, the K-Hopf algebra $L[G, \cdot]^{(G,\circ)}$ we obtain consists of the elements $\sum_{(a,b)\in G} \ell_{(a,b)}(a, b) \in L[G, \cdot]$ that satisfy, for all $(c, d) \in G$,

$$\sum_{(a,b)\in G} \ell_{(a,b)}(a, b) = \sum_{(a,b)\in G} [(c, d)(\ell_{(a,b)})]({}^{\alpha(d)}a, b).$$

Such an element acts on L as follows:

$$\left(\sum_{(a,b)\in G} \ell_{(a,b)}(a,b)\right) \star x = \sum_{(a,b)\in G} \ell_{(a,b)}(a,b)(x).$$

Given a Hopf–Galois structure on L/K with associated skew brace $(G,\cdot,\circ)$, we can define the *type* of the structure to be the isomorphism class of $(G,\cdot)$; note that this coincides with the usual definition. In particular, the known results about existence and classification can also be translated and obtained using the new point of view. Indeed, Theorem 2.5 immediately follows from Theorem 3.1, as well as the result counting the number of Hopf–Galois structures associated with the same isomorphism class of a skew brace. We recall this result and its proof here, which is just a slight modification of the proof of [33, Corollary 3.1].

Proposition 3.7. *Let $(G,\cdot,\circ)$ be a skew brace. Then there are*

$$\frac{|\operatorname{Aut}(G,\circ)|}{|\operatorname{Aut}(G,\cdot,\circ)|}$$

Hopf–Galois structures on L/K such that the associated skew brace is isomorphic to $(G,\cdot,\circ)$.

Proof. Consider the set $\mathcal{S}$ of group operations $\cdot'$ on G such that $(G,\cdot',\circ)$ is a skew brace. We need to count for how many operations $\cdot' \in \mathcal{S}$, the skew brace $(G,\cdot',\circ)$ is isomorphic to $(G,\cdot,\circ)$. There is an action of $\operatorname{Aut}(G,\circ)$ on $\mathcal{S}$, as follows:

$$\phi : \cdot' \to \cdot'_{\phi}, \quad \sigma \cdot'_{\phi} \tau = \phi(\phi^{-1}(\sigma) \cdot' \phi^{-1}(\tau)).$$

Then the orbit of $\cdot \in \mathcal{S}$ consists precisely of the operations $\cdot'$ such that $(G,\cdot',\circ)$ is a skew brace isomorphic to $(G,\cdot,\circ)$. As the stabiliser of $\cdot$ under this action is $\operatorname{Aut}(G,\cdot,\circ)$, we derive the assertion. □

We also remark that Byott's translation [5] for Galois extensions, an extremely useful tool to count Hopf–Galois structures, can be obtained in this fashion. We recall here the statement and a quick proof, along the lines of the one described in [12, Section 7], but without involving regular subgroups. Let $(N,\cdot)$ be a group of the same order as $(G,\circ)$. Denote by $e(G,N)$ the number of Hopf–Galois structures on L/K of type $(N,\cdot)$, which by Theorem 3.1 equals the number of operations $\cdot$ such that $(G,\cdot,\circ)$ is a skew brace with $(G,\cdot) \cong (N,\cdot)$, and denote by $f(G,N)$ the number of operations $\circ$ such that $(N,\cdot,\circ)$ is a skew brace with $(N,\circ) \cong (G,\circ)$.

Theorem 3.8. *The following equality holds:*

$$e(G,N) = \frac{|\operatorname{Aut}(G,\circ)|}{|\operatorname{Aut}(N,\cdot)|} f(G,N).$$

Proof. Consider $\mathcal{N} = \{\text{bijections } \varphi : N \to G\}$ and $\mathcal{G} = \{\text{bijections } \psi : G \to N\}$. Clearly, there exists a bijection

$$\delta : \mathcal{N} \to \mathcal{G}, \quad \varphi \mapsto \varphi^{-1}.$$

For all $\varphi \in \mathcal{N}$, consider $(G, \cdot_\varphi)$, where $\cdot_\varphi$ is the operation obtained by φ via transport of structure. In particular, $\varphi\colon (N,\cdot) \to (G,\cdot_\varphi)$ is an isomorphism. Similarly, for all $\psi \in \mathcal{G}$, one can define $(N, \circ_\psi)$. It is straightforward to check that δ restricts to a bijection

$$\mathcal{N}' = \{\varphi \in \mathcal{N} \mid (G, \cdot_\varphi, \circ) \text{ is a skew brace}\} \to \mathcal{G}' = \{\psi \in \mathcal{G} \mid (N, \cdot, \circ_\psi) \text{ is a skew brace}\}.$$

Note that the right action of $\mathrm{Aut}(N,\cdot)$ on $\mathcal{N}'$ via composition satisfies the following properties.

- The orbits of $\mathcal{N}'$ under the action of $\mathrm{Aut}(N,\cdot)$ correspond bijectively to the operations $\cdot$ such that $(G,\cdot,\circ)$ is a skew brace and $(N,\cdot) \cong (G,\cdot)$.
- The action of $\mathrm{Aut}(N,\cdot)$ on $\mathcal{N}'$ is fixed-point-free.

We deduce that the cardinality of $\mathcal{N}'$ equals $|\mathrm{Aut}(N,\cdot)|e(G,N)$. A similar argument yields that the cardinality of $\mathcal{G}'$ equals $|\mathrm{Aut}(G,\circ)|f(G,N)$, so

$$|\mathrm{Aut}(N,\cdot)|e(G,N) = |\mathrm{Aut}(G,\circ)|f(G,N). \qquad \square$$

We describe now the structure of the Hopf algebras in terms of the associated skew braces. Consider a Hopf–Galois structure on L/K, with associated skew brace $(G,\cdot,\circ)$.

Theorem 3.9. *The K-sub Hopf algebras of $L[G,\cdot]^{(G,\circ)}$ are precisely those of the form $L[G',\cdot]^{(G,\circ)}$ for left ideals G' of $(G,\cdot,\circ)$. Moreover, $L[G',\cdot]^{(G,\circ)}$ is normal in $L[G,\cdot]^{(G,\circ)}$ if and only if G' is a strong left ideal of $(G,\cdot,\circ)$.*

Proof. This follows from Galois descent and the fact that the subgroups of $(G,\cdot)$ invariant under the action of $(G,\circ)$ via the gamma function of $(G,\cdot,\circ)$ are precisely the left ideals of $(G,\cdot,\circ)$. $\square$

Consider a left ideal G' of $(G,\cdot,\circ)$. Then G' corresponds to an intermediate field $L^{H'}$ of L/K via the Hopf–Galois correspondence, where $H' = L[G',\cdot]^{(G,\circ)}$. But as G' is a subgroup of $(G,\circ)$, we have that G' also corresponds to an intermediate field F of L/K via the usual Galois correspondence. We denote both fields by $L^{G'}$, the ambiguity justified by the following pleasant consequence of Theorem 3.1.

Corollary 3.10. *The following equality holds:*

$$L^{H'} = F.$$

Proof. It is clear that if $x \in F$, then $x \in L^{H'}$. Indeed, given $\sum_{\sigma\in G} \ell_\sigma \sigma \in H'$, we have

$$\left(\sum_{\sigma\in G} \ell_\sigma \sigma\right) \star x = \sum_{\sigma\in G} \ell_\sigma \sigma(x) = \sum_{\sigma\in G} \ell_\sigma x = \varepsilon\left(\sum_{\sigma\in G} \ell_\sigma \sigma\right) x.$$

The assertion then follows from $[L : F] = |G'| = [L : L^{H'}]$. $\square$

As the action of $(G,\circ)$ on $(G,\cdot)$ is given by the gamma function of $(G,\cdot,\circ)$, we can easily describe the grouplike elements of $L[G,\cdot]^{(G,\circ)}$.

Corollary 3.11. *The grouplike elements of the K-Hopf algebra $L[G,\cdot]^{(G,\circ)}$ are the elements of* $\mathrm{Fix}(G,\cdot,\circ)$.

We study now how several known notions in skew brace theory have a natural description in Hopf–Galois theory.

Left ideals. As already mentioned, a left ideal G' of $(G,\cdot,\circ)$ corresponds to a K-sub Hopf algebra $L[G',\cdot]^{(G,\circ)}$ of $L[G,\cdot]^{(G,\circ)}$, which then corresponds to an intermediate field $F = L^{G'}$ of L/K. The extension L/F is Galois with Galois group $(G',\circ)$, and there exists a natural Hopf–Galois structure on L/F given by the F-Hopf algebra $F \otimes_K L[G',\cdot]^{(G,\circ)}$. The skew brace associated with this Hopf–Galois structure is precisely $(G',\cdot,\circ)$. Indeed, by Galois descent, the natural map

$$F \otimes_K L[G',\cdot]^{(G,\circ)} \to L[G',\cdot]^{(G',\circ)}$$

is an F-Hopf algebra isomorphism, and as both the actions of these Hopf algebras on L are obtained by that of $L[G,\cdot]^{(G,\circ)}$, the assertion easily follows.

Strong left ideals. Suppose in addition that G' is a strong left ideal of $(G,\cdot,\circ)$, so G' is normal in $(G,\cdot)$. In this case, $L[G',\cdot]^{(G,\circ)}$ is normal in $L[G,\cdot]^{(G,\circ)}$, and we obtain a short exact sequence of K-Hopf algebras

$$K \to L[G',\cdot]^{(G,\circ)} \to L[G,\cdot]^{(G,\circ)} \to L[G/G',\cdot]^{(G,\circ)} \to K.$$

We find a Hopf–Galois structure on F/K with K-Hopf algebra $L[G/G',\cdot]^{(G,\circ)}$.

Ideals. Finally, suppose that G' is an ideal of $(G,\cdot,\circ)$. Then F/K is Galois with Galois group $(G/G',\cdot)$, and the Hopf–Galois structure on F/K given by $L[G/G',\cdot]^{(G,\circ)}$ is associated with the skew brace $(G/G',\cdot,\circ)$, because in this case the equality $L[G/G',\cdot]^{(G,\circ)} = F[G/G',\cdot]^{(G/G',\circ)}$ holds.

Semidirect products. Suppose that $(G,\cdot,\circ)$ is isomorphic to a semidirect product of skew braces. Then there exists an ideal G_1 and a strong left ideal G_2 of $(G,\cdot,\circ)$ such that $(G,\circ)$ is the inner semidirect product of $(G_1,\circ)$ and $(G_2,\circ)$, and $(G,\cdot)$ is the inner direct product of $(G_1,\cdot)$ and $(G_2,\cdot)$. Write $F_1 = L^{G_1}$ and $F_2 = L^{G_2}$. In this case, the towers $K \subseteq F_1 \subseteq L$ and $K \subseteq F_2 \subseteq L$ are described exactly as before. Moreover, $L[G,\cdot]$ is isomorphic to $L[G_1,\cdot] \otimes_L L[G_2,\cdot]$ as $(G,\circ)$-compatible L-Hopf algebras, and by Galois descent,

$$L[G,\cdot]^{(G,\circ)} \cong L[G_1,\cdot]^{(G,\circ)} \otimes_K L[G_2,\cdot]^{(G,\circ)}$$

as K-Hopf algebras.

We note moreover that because G_1 is an ideal of $(G,\cdot,\circ)$, the obvious isomorphism $\varphi\colon (G_2,\circ) \to (G/G_1,\circ)$ between Galois groups is in fact an isomorphism of skew braces $\varphi\colon (G_2,\cdot,\circ) \to (G/G_1,\cdot,\circ)$. This implies that the Hopf–Galois structures on L/F_2 and F_1/K given by the previous description are associated with skew braces isomorphic in a natural way. By this observation and Galois descent, we can also deduce that

$$F_2 \otimes_K F_1[G/G_1,\cdot]^{(G/G_1,\circ)} \cong L[G_2,\cdot]^{(G_2,\circ)}$$

as F_2-Hopf algebras.

Direct products. If the semidirect product is also direct, then the Galois group $(G, \circ)$ is the inner direct product of $(G_1, \circ)$ and $(G_2, \circ)$, and we can repeat the previous analysis also for F_2/K, which is Galois in this case.

Metatriviality. Suppose now that $(G, \cdot, \circ)$ metatrivial. Consider an ideal G' of $(G, \cdot, \circ)$ such that $(G', \cdot, \circ)$ and $(G/G', \cdot, \circ)$ are trivial skew braces, and write $F = L^{G'}$. Then the Hopf–Galois structures on L/F and F/K obtained by the action of $L[G, \cdot]^{(G,\circ)}$ on L are the classical structures.

Remark 3.12. There are notions of solubility and nilpotency of skew braces that generalise metatriviality; see, for example, [21, 31]. For Hopf–Galois structures associated with skew braces $(G, \cdot, \circ)$ with these properties, similar conclusions, involving tower of intermediate fields of L/K, can be derived.

We believe that the study of this kind of properties of the skew brace, together with appropriate ramification on the extension L/K, could bring new results in Hopf–Galois module theory. For example, in [7], a key role for the study of the Hopf–Galois module structure of a Galois extension L/K of p-adic fields of degree p^2, p a prime, was played by an intermediate normal field F of L/K such that, given a Hopf–Galois structure on L/K, F is in the image of the Hopf–Galois correspondence, and the Hopf–Galois structure on L/K yields the classical structures on L/F and F/K.

More generally, all the skew braces obtained with [38, Theorem 6.6], which generalise several constructions developed in recent years, are metatrivial, so similar reasonings could be repeated.

4 | THE HOPF–GALOIS CORRESPONDENCE

In this final section, we study the Hopf–Galois correspondence with respect to the new version of the connection. We fix a finite Galois extension of fields L/K with Galois group $(G, \circ)$. From the discussion of Section 3, we immediately derive the following result.

Corollary 4.1. *Consider a Hopf–Galois structure on L/K, with associated skew brace $(G, \cdot, \circ)$. Then the Hopf–Galois correspondence for this structure is surjective if and only if every subgroup of $(G, \circ)$ is a left ideal of $(G, \cdot, \circ)$.*

Specifically, if G' is a subgroup of $(G, \circ)$, then $L^{G'}$ is in the image of the Hopf–Galois correspondence if and only if G' is a left ideal of $(G, \cdot, \circ)$.

Example 4.2. Consider the classical structure, with associated skew brace $(G, \circ, \circ)$. In this case, every subgroup of $(G, \circ)$ is a left ideal of $(G, \circ, \circ)$, so we find, as expected, that the Hopf–Galois correspondence for this structure is surjective.

We note the following facts, which are direct consequences of Corollary 4.1

Remark 4.3. If $(G, \cdot, \circ)$ is a skew brace and $(G, \cdot)$ has less subgroups than $(G, \circ)$, then for the Hopf–Galois structure on L/K associated with $(G, \cdot, \circ)$, the Hopf–Galois correspondence is not surjective.

Remark 4.4. Suppose that $(G, \cdot, \circ)$ is a skew brace isomorphic to the direct product of skew braces $(G_i, \cdot, \circ)$ of pairwise coprime orders. If all the subgroups of $(G_i, \circ)$ are left ideals of $(G_i, \cdot, \circ)$, then

all the subgroups of $(G, \circ)$ are left ideals of $(G, \cdot, \circ)$, so for the Hopf–Galois structure on L/K associated with $(G, \cdot, \circ)$, the Hopf–Galois correspondence is surjective.

We focus now our attention on Hopf–Galois structures associated with bi-skew braces. In this case, the gamma functions take values in the automorphisms of the Galois group $(G, \circ)$, so we easily derive the following fact.

Lemma 4.5. *Consider a Hopf–Galois structure on L/K such that the associated skew brace $(G, \cdot, \circ)$ is a bi-skew brace. Let G' be a characteristic subgroup of $(G, \circ)$. Then $L^{G'}$ is in the image of the Hopf–Galois correspondence for this structure.*

Corollary 4.6. *Suppose that $(G, \circ)$ is a cyclic group, and consider a Hopf–Galois structure on L/K such that the associated skew brace $(G, \cdot, \circ)$ is a bi-skew brace. Then the Hopf–Galois correspondence for this structure is surjective.*

Example 4.7. Suppose that $(G, \circ)$ is cyclic of order 8. As shown in [36], there exists a skew brace $(G, \circ, \cdot)$ with $(G, \cdot) \cong Q_8$, the quaternion group. A straightforward calculation shows that $(G, \circ, \cdot)$ is a bi-skew brace. We conclude by Corollary 4.6 that for the Hopf–Galois structure on L/K associated with the skew brace $(G, \cdot, \circ)$, the Hopf–Galois correspondence is surjective.

We remark that for a Hopf–Galois structure on L/K associated with a bi-skew brace $(G, \cdot, \circ)$, the Hopf–Galois correspondence is surjective if and only if $\gamma(\sigma)$ is a *power automorphism* of $(G, \circ)$ for all $\sigma \in G$, that is, ${}^{\gamma(\sigma)}\tau$ is a power of τ in $(G, \circ)$ for all $\tau \in G$. Indeed, the power automorphisms of $(G, \circ)$ are precisely the automorphisms of $(G, \circ)$ that map every subgroup of $(G, \circ)$ to itself.

Example 4.8. Suppose that $(G, \circ)$ is the direct product of an abelian group A and the cyclic group C_2 of order 2. Denote by α the action of C_2 on A via inversion, and consider the semidirect product $(G, \cdot) = A \rtimes C_2$ with respect to this action. Then $(G, \cdot, \circ)$ is a bi-skew brace; see [24, Examples 1.4 and 1.5]. Here the gamma function of $(G, \cdot, \circ)$ is given as follows:

$$\gamma(c,d)(a, b) = ({}^{\alpha(d^{-1})}(a), b),$$

which is either equal to (a, b) or to $\overline{(a, b)}$. In particular, $\gamma(c, d)$ is a power automorphism of $(G, \circ)$, and we conclude that for the Hopf–Galois structure on L/K associated with $(G, \cdot, \circ)$, the Hopf–Galois correspondence is surjective.

We deal now with bi-skew braces $(G, \cdot, \circ)$ whose gamma functions have values in the inner automorphism group of $(G, \circ)$; these skew braces have been recently studied in [19, 20, 27, 28, 38]. Denote by $Z(G)$ the centre of $(G, \circ)$ and by $N(G)$ the *norm* of $(G, \circ)$, that is, the intersection of the normalisers of the subgroups of $(G, \circ)$. It is clear that $\iota_\circ(\sigma)$ is a power automorphism of $(G, \circ)$ if and only if $\sigma \in N(G)$.

We can apply this fact to obtain Hopf–Galois structures on L/K for which the Hopf–Galois correspondence is surjective, as follows. Given a group homomorphism $\psi : (G, \circ) \to N(G)/Z(G)$, define

$$\sigma \cdot_\psi \tau = \sigma \circ {}^{\iota_\circ(\psi(\sigma))}\tau = \sigma \circ \psi(\sigma) \circ \tau \circ \overline{\psi(\sigma)};$$

here by $\psi(\sigma)$ we denote any element in the coset $\psi(\sigma)$ in $N(G)/Z(G)$, with a little abuse of notation justified by the fact that if $\tau \in Z(G)$, then $\iota_\circ(\tau) = \mathrm{id}$.

Theorem 4.9. *For all group homomorphisms $\psi : (G, \circ) \to N(G)/Z(G)$, we have that $(G, \cdot_\psi, \circ)$ is a bi-skew brace, and for the Hopf–Galois structure on L/K associated with $(G, \cdot_\psi, \circ)$, the Hopf–Galois correspondence is surjective.*

Proof. Let $\psi : (G, \circ) \to N(G)/Z(G)$ be a group homomorphism. By the main theorem of [37], the quotient $N(G)/Z(G)$ is abelian, so we can apply [38, Theorem 6.6] to derive that $(G, \cdot_\psi, \circ)$ is a bi-skew brace and the gamma function of $(G, \cdot_\psi, \circ)$ is given by $\gamma(\sigma) = \iota_\circ(\overline{\psi(\sigma)})$. In particular, the gamma function of $(G, \cdot_\psi, \circ)$ is given by conjugation by elements of $N(G)$ in $(G, \circ)$, so by power automorphisms of $(G, \circ)$, and therefore we obtain our assertion. □

Remark 4.10. Note that distinct group homomorphisms $(G, \circ) \to N(G)/Z(G)$ in Theorem 4.9 yield distinct operations, so distinct Hopf–Galois structures on L/K.

Example 4.11. Suppose that $(G, \circ) = Q_8$, the quaternion group of order 8. There are 22 Hopf–Galois structures on L/K, and six of them are of cyclic type; see [39, table 2]. As $(G, \circ)$ is Hamiltonian, we derive that $N(G) = G$, so $N(G)/Z(G) \cong C_2 \times C_2$. Since there are 16 distinct group homomorphisms

$$Q_8 \to C_2 \times C_2,$$

we obtain 16 distinct Hopf–Galois structures on L/K for which the Hopf–Galois correspondence is surjective. We find indeed all the Hopf–Galois structures on L/K except for the six of cyclic type, for which the Hopf–Galois correspondence is not surjective by Remark 4.3.

Example 4.12. Suppose that $(G, \circ)$ is the nonabelian group of order p^3 and exponent p^2, with p odd prime. An easy reasoning implies that $N(G)$ is the elementary abelian subgroup of $(G, \circ)$ of order p^2, while the centre is cyclic of order p. As there are p^2 distinct group homomorphisms

$$(G, \circ) \to C_p,$$

we obtain p^2 distinct Hopf–Galois structures on L/K for which the Hopf–Galois correspondence is surjective.

The following result, whose proof is immediate, shows that the behaviour of the canonical nonclassical structure can also be assumed by other Hopf–Galois structures.

Proposition 4.13. *Consider a Hopf–Galois structure on L/K such that associated skew brace $(G, \cdot, \circ)$ is a bi-skew brace with gamma function $\gamma : (G, \circ) \to \mathrm{Inn}(G, \circ)$. Then every normal intermediate field K of L/K is in the image of the Hopf–Galois correspondence for this structure.*

Moreover, if $\gamma : (G, \circ) \to \mathrm{Inn}(G, \circ)$ is surjective, then the image of the Hopf–Galois correspondence consists precisely of the normal intermediate fields of L/K.

Example 4.14. Consider the canonical nonclassical structure, with associated skew brace $(G, \circ_{\mathrm{op}}, \circ)$. Here, $\gamma(\sigma) = \iota_\circ(\sigma)$ for all $\sigma \in G$. Applying Proposition 4.13, we recover the well-known property of the canonical nonclassical structure.

Example 4.15. Suppose that $(G, \circ)$ is nilpotent of class two, and define

$$\sigma \cdot \tau = \sigma \circ {}^{\iota_\circ(\sigma)}\tau = \sigma \circ \sigma \circ \tau \circ \overline{\sigma}.$$

Then by [20, Proposition 5.6], we have that $(G, \cdot, \circ)$ is a bi-skew brace and the gamma function of $(G, \cdot, \circ)$ is given by $\gamma(\sigma) = \iota_\circ(\overline{\sigma})$. By Proposition 4.13, we derive that for the associated Hopf–Galois structure on L/K, the image of the Hopf–Galois correspondence consists precisely of the normal intermediate fields of L/K.

It is easy to see that if there exists $\sigma \in G$ such that $\sigma \circ \sigma$ is not in the centre of $(G, \circ)$, then the Hopf–Galois structure we find is different from the canonical nonclassical structure. This holds, for example, for the Heisenberg group of order p^3, with p an odd prime.

We study now a question posed in [16]. Let L_1/K_1 be a finite Galois extension of fields with Galois group $(G, \circ)$, and consider a Hopf–Galois structure on L_1/K_1, with associated skew brace $(G, \cdot, \circ)$. We can rewrite the *Hopf–Galois correspondence ratio*, defined as the ratio of the number intermediate fields of L_1/K_1 in the image of the Hopf–Galois correspondence to the number of intermediate fields of L_1/K_1, as follows:

$$GC(L_1/K_1, L_1[G, \cdot]^{(G,\circ)}) = \frac{|\{\text{left ideals of } (G, \cdot, \circ)\}|}{|\{\text{subgroups of } (G, \circ)\}|}.$$

Suppose in addition that $(G, \cdot, \circ)$ is a bi-skew brace, and let L_2/K_2 be a finite Galois extension of fields with Galois group $(G, \cdot)$. The skew brace $(G, \circ, \cdot)$ is associated with a Hopf–Galois structure on L_2/K_2. Are these two Hopf–Galois structures related in some way?

The next result follows immediately from the facts that the lattices of left ideals of $(G, \cdot, \circ)$ and K_1-sub Hopf algebras of $L_1[G, \cdot]^{(G,\circ)}$ are isomorphic, and the left ideals of $(G, \cdot, \circ)$ and $(G, \circ, \cdot)$ coincide.

Theorem 4.16. *The following facts hold.*

- *The lattices of K_1-sub Hopf algebras of $L_1[G, \cdot]^{(G,\circ)}$ and K_2-sub Hopf algebras of $L_2[G, \circ]^{(G,\cdot)}$ are isomorphic.*
- *There is the same number of intermediate fields in the images of the Hopf–Galois correspondence for the Hopf–Galois structure on L_1/K_1 associated with $(G, \cdot, \circ)$ and the Hopf–Galois structure on L_2/K_2 associated with $(G, \circ, \cdot)$.*
- *The following equality holds:*

$$\frac{GC(L_1/K_1, L_1[G, \cdot]^{(G,\circ)})}{GC(L_2/K_2, L_2[G, \circ]^{(G,\cdot)})} = \frac{|\{\text{subgroups of } (G, \cdot)\}|}{|\{\text{subgroups of } (G, \circ)\}|}.$$

In particular, the ratio between the two Hopf–Galois correspondence ratios is constant and depends only on the isomorphism classes of the Galois groups.

Example 4.17. Suppose that $(G, \cdot, \circ)$ is the skew brace of Example 4.8 with p an odd prime and $A = C_p$. Then $(G, \cdot)$ is dihedral of order $2p$ and $(G, \circ)$ is cyclic of order $2p$. There are $p + 3$ subgroups of $(G, \cdot)$ and four subgroups of $(G, \circ)$, and as every subgroup of $(G, \circ)$ is a left ideal of $(G, \cdot, \circ)$, we have the following equalities:

$$GC(L_1/K_1, L_1[G, \cdot]^{(G,\circ)}) = 1,$$

$$GC(L_2/K_2, L_2[G, \circ]^{(G,\cdot)}) = \frac{4}{p+3},$$

$$\frac{GC(L_1/K_1, L_1[G, \cdot]^{(G,\circ)})}{GC(L_2/K_2, L_2[G, \circ]^{(G,\cdot)})} = \frac{p+3}{4}.$$

We conclude by focusing our attention on Hopf–Galois structures associated with skew braces that are not necessarily bi-skew braces. We begin with the following theorem, which was proved in [30]. We provide a quick proof for convenience.

Theorem 4.18. *Let N be a group. If there exists m such that the number of characteristic subgroups of order m of N is greater than the number of subgroups of order m of $(G, \circ)$, then L/K has no Hopf–Galois structures of type N.*

Proof. If L/K has a Hopf–Galois structure of type N, then there exists a skew brace $(G, \cdot, \circ)$ with $(G, \cdot) \cong N$. As every characteristic subgroup of $(G, \cdot)$ is a left ideal of $(G, \cdot, \circ)$, so also a subgroup of $(G, \circ)$, we immediately derive a contradiction. □

On the contrary, if there exists a skew brace $(G, \cdot, \circ)$ such that the number of characteristic subgroups of $(G, \cdot)$ equals the number of subgroups of $(G, \circ)$, then the Hopf–Galois structure on L/K associated with $(G, \cdot, \circ)$ assumes a nice behaviour.

Proposition 4.19. *Consider a Hopf–Galois structure on L/K, with associated skew brace $(G, \cdot, \circ)$. Suppose that the number of characteristic subgroups of $(G, \cdot)$ equals the number of subgroups of $(G, \circ)$. Then the Hopf–Galois correspondence for this structure is surjective.*

Proof. Every characteristic subgroup of $(G, \cdot)$ is a left ideal of $(G, \cdot, \circ)$, so also a subgroup of $(G, \circ)$. In particular, every subgroup of $(G, \circ)$ is a left ideal. □

Example 4.20. Suppose that $(G, \circ)$ is cyclic of odd prime power order, and consider a Hopf–Galois structure on L/K, with associated skew brace $(G, \cdot, \circ)$. By [29], also $(G, \cdot)$ is cyclic, so by Proposition 4.19, we conclude that the Hopf–Galois correspondence is surjective; we have recovered [13, Proposition 4.3].

Example 4.21. Suppose that $(G, \circ)$ is cyclic of order 2^m, with $m \geqslant 1$, and consider a Hopf–Galois structure on L/K, with associated skew brace $(G, \cdot, \circ)$. We claim that the Hopf–Galois correspondence for this structure is surjective.

If $m = 1, 2$, then by the explicit classification in [2, Proposition 2.4], one can check that $(G, \cdot, \circ)$ is a bi-skew brace, so the result follows from Corollary 4.6.

Suppose now that $m \geqslant 3$. By [8, Theorem 6.1], necessarily $(G, \cdot)$ is cyclic, the dihedral group, or the generalised quaternion group. With the unique exception of $m = 3$ and $(G, \cdot) \cong Q_8$, the numbers of characteristic subgroups of $(G, \cdot)$ and subgroups of $(G, \circ)$ coincide, so we conclude by Proposition 4.19.

Finally, suppose that $m = 3$ and $(G, \cdot) \cong Q_8$. Then the centre Z of $(G, \cdot)$ is a characteristic subgroup of order 2. It follows that Z is an ideal of $(G, \cdot, \circ)$. By the case $m = 2$, we know that $(G/Z, \cdot, \circ)$ has a left ideal G'/Z of order 2, which easily implies that G' is a left ideal of $(G, \cdot, \circ)$ of order 4.

Remark 4.22. With the classification given in [2], it is easy to construct a skew brace $(G, \cdot, \circ)$ with $(G, \circ)$ cyclic of order p^3, where p is a prime, such that $(G, \cdot, \circ)$ is not a bi-skew brace. Thus, Examples 4.20 and 4.21 do not follow from Corollary 4.6.

We shall now conclude by characterising all the Galois extensions that behave like Examples 4.20 and 4.21. First, a useful lemma.

Lemma 4.23. *Suppose that $(G, \circ)$ is isomorphic to a direct product of groups $(A, \circ)$ and $(B, \circ)$, and that there exists a skew brace $(A, \cdot, \circ)$ such that not every subgroup of $(A, \circ)$ is a left ideal of $(A, \cdot, \circ)$. Then there exists a Hopf–Galois structure on L/K for which the Hopf–Galois correspondence is not surjective.*

Proof. We can use the group isomorphism $(G, \circ) \cong (A, \circ) \times (B, \circ)$ to transport the structure of $(A, \cdot) \times (B, \circ)$ to G. We obtain a group operation $\cdot$ such that $(G, \cdot, \circ)$ is a skew brace isomorphic to $(A, \cdot, \circ) \times (B, \circ, \circ)$. By assumption, there exists a subgroup of $(G, \circ)$ which is not a left ideal of $(G, \cdot, \circ)$, so for the Hopf–Galois structure on L/K associated with $(G, \cdot, \circ)$, the Hopf–Galois correspondence is not surjective. □

Theorem 4.24. *The following are equivalent.*

- *For all the Hopf–Galois structures on L/K, the Hopf–Galois correspondence is surjective.*
- *The Galois group $(G, \circ)$ is cyclic, and for all primes p and q dividing the order of $(G, \circ)$, we have that p does not divide $q - 1$.*

Proof. Suppose first that $(G, \circ)$ is cyclic of order n and for all primes p and q dividing n, we have that p does not divide $q - 1$. Consider a Hopf–Galois structure on L/K, with associated skew brace $(G, \cdot, \circ)$. If n is even, then n has no odd prime divisors, so the result follows from Example 4.21.

If instead n is odd, then by [40, Corollary 1.7], we have that $(G, \cdot)$ is isomorphic to a semidirect product of cyclic groups $C_a \rtimes C_b$, where a and b are coprime and $ab = n$. But by the assumption on the divisors of the order of $(G, \circ)$, this semidirect product is necessarily a direct product. In particular, $(G, \cdot)$ is cyclic, and we can apply [21, Corollary 4.3] to deduce that $(G, \cdot, \circ)$ is isomorphic to a direct product of skew braces of coprime odd prime power order. The assertion then follows from Remark 4.4 and Example 4.20.

Conversely, suppose that for all the Hopf–Galois structures on L/K, the Hopf–Galois correspondence is surjective. As this holds for the canonical nonclassical structure, $(G, \circ)$ is either abelian or Hamiltonian. We proceed by exclusion.

Suppose first that $(G, \circ)$ is Hamiltonian. Then there exists an abelian group A such that $(G, \circ)$ is isomorphic to the direct product of Q_8 and A; see [25, Theorem 12.5.4]. As already mentioned, there exists a skew brace $(G', \cdot, \circ)$ where $(G', \circ) \cong Q_8$ and $(G', \cdot)$ is cyclic. By applying Remark 4.3 and Lemma 4.23, we derive a contradiction.

We deduce that $(G, \circ)$ is necessarily abelian. Suppose that $(G, \circ)$ is not cyclic. Then there exists a prime p such that $(G, \circ)$ is isomorphic to a direct product of the form $C_{p^r} \times C_{p^s} \times A$, where $1 \leqslant s \leqslant r$. Write σ for a generator of C_{p^r} and τ for a generator of C_{p^s}. In a slight variation of [38, Example 6.7], there exists a skew brace $(G', \cdot, \circ)$ such that $(G', \circ)$ equals $C_{p^r} \times C_{p^s}$ with the direct product operation and

$$(\sigma^i, \tau^j) \cdot (\sigma^a, \tau^b) = (\sigma^{i+a}, \tau^{j+b+ia}).$$

Note that the subgroup $C_{p^r} \times \{1\}$ of $(G', \circ)$ is not a subgroup of $(G', \cdot)$, so in particular it is not a left ideal of $(G', \cdot, \circ)$. Again by Lemma 4.23, we find a contradiction.

We deduce that $(G, \circ)$ is necessarily cyclic. Suppose that there exist primes p and q dividing the order of $(G, \circ)$ such that p divides $q - 1$. Let $(G', \circ)$ be the direct product of the Sylow q-subgroup Q and the Sylow p-subgroup P of $(G, \circ)$. By assumption on p and q, we can construct a nontrivial semidirect product $(G', \cdot)$ of Q and P. By [24, Example 1.5], we have that $(G', \cdot, \circ)$ is a skew brace. Suppose that $\{1\} \times P$ is a left ideal of $(G', \cdot, \circ)$. Then $\{1\} \times P$ is not a left ideal of $(G', \cdot_{\mathrm{op}}, \circ)$, because otherwise $\{1\} \times P$ would be normal subgroup of $(G', \cdot)$. As $(G, \circ)$ is isomorphic to the direct product of all its Sylow subgroups, we find a contradiction from Lemma 4.23. □

ACKNOWLEDGEMENTS

The first author was a member of GNSAGA (INdAM). The second author was supported by Fonds voor Wetenschappelijk Onderzoek - Vlaanderen, grant 1160522N.

Open Access Funding provided by Universita degli Studi di Pisa within the CRUI-CARE Agreement.

JOURNAL INFORMATION

REFERENCES

1. N. Andruskiewitsch and J. Devoto, *Extensions of Hopf algebras*, Algebra i Analiz. **7** (1995), no. 1, 22–61. MR 1334152.
2. D. Bachiller, *Classification of braces of order p^3*, J. Pure Appl. Algebra **219** (2015), no. 8, 3568–3603. MR 3320237.
3. D. Bachiller, *Counterexample to a conjecture about braces*, J. Algebra **453** (2016), 160–176. MR 3465351.
4. V. G. Bardakov, M. V. Neshchadim, and M. K. Yadav, *On λ-homomorphic skew braces*, J. Pure Appl. Algebra. **226** (2022), no. 6, 37. MR 4346001.
5. N. P. Byott, *Uniqueness of Hopf Galois structure for separable field extensions*, Comm. Algebra. **24** (1996), no. 10, 3217–3228. MR 1402555.
6. N. P. Byott, *Galois structure of ideals in wildly ramified abelian p-extensions of a p-adic field, and some applications*, J. Théor. Nombres Bordeaux. **9** (1997), no. 1, 201–219. MR 1469668.
7. N. P. Byott, *Integral Hopf–Galois structures on degree p^2 extensions of p-adic fields*, J. Algebra **248** (2002), no. 1, 334–365. MR 1879021.
8. N. P. Byott, *Hopf–Galois structures on almost cyclic field extensions of 2-power degree*, J. Algebra **318** (2007), no. 1, 351–371. MR 2363137.
9. A. Caranti, *Bi-skew braces and regular subgroups of the holomorph*, J. Algebra **562** (2020), 647–665. MR 4130907.

10. E. Campedel, A. Caranti, and I. Del Corso, *Hopf-Galois structures on extensions of degree p^2q and skew braces of order p^2q: the cyclic Sylow p-subgroup case*, J. Algebra **556** (2020), 1165–1210. MR 4089566.
11. L. N. Childs, C. Greither, K. P. Keating, A. Koch, T. Kohl, P. J. Truman, and R. G. Underwood, *Hopf algebras and Galois module theory*, Mathematical Surveys and Monographs, vol. 260, American Mathematical Society, Providence, RI, 2021. MR 4390798.
12. L. N. Childs, *Taming wild extensions: Hopf algebras and local Galois module theory*, Mathematical Surveys and Monographs, vol. 80, American Mathematical Society, Providence, RI, 2000. MR 1767499.
13. L. N. Childs, *On the Galois correspondence for Hopf Galois structures*, New York J. Math. **23** (2017), 1–10. MR 3611070.
14. L. N. Childs, *Skew braces and the Galois correspondence for Hopf Galois structures*, J. Algebra **511** (2018), 270–291. MR 3834774.
15. L. N. Childs, *Bi-skew braces and Hopf Galois structures*, New York J. Math. **25** (2019), 574–588. MR 3982254.
16. L. N. Childs, *On the Galois correspondence for Hopf Galois structures arising from finite radical algebras and Zappa–Szép products*, Publ. Mat. **65** (2021), no. 1, 141–163. MR 4185830.
17. T. Crespo, A. Rio, and M. Vela, *On the Galois correspondence theorem in separable Hopf Galois theory*, Publ. Mat. **60** (2016), no. 1, 221–234. MR 3447739.
18. S. U. Chase and M. E. Sweedler, *Hopf algebras and Galois theory*, Lecture Notes in Mathematics, vol. 97, Springer, Berlin, 1969. MR 0260724.
19. A. Caranti and L. Stefanello, *From endomorphisms to bi-skew braces, regular subgroups, the Yang–Baxter equation, and Hopf–Galois structures*, J. Algebra **587** (2021), 462–487. MR 4304796.
20. A. Caranti and L. Stefanello, *Brace blocks from bilinear maps and liftings of endomorphisms*, J. Algebra **610** (2022), 831–851. MR 4473766.
21. F. Cedó, A. Smoktunowicz, and L. Vendramin, *Skew left braces of nilpotent type*, Proc. Lond. Math. Soc. (3) **118** (2019), no. 6, 1367–1392. MR 3957824.
22. The GAP Group, *GAP: Groups, Algorithms, and Programming, Version 4.12.2*, 2022.
23. C. Greither and B. Pareigis, *Hopf Galois theory for separable field extensions*, J. Algebra **106** (1987), no. 1, 239–258. MR 878476.
24. L. Guarnieri and L. Vendramin, *Skew braces and the Yang–Baxter equation*, Math. Comp. **86** (2017), no. 307, 2519–2534. MR 3647970.
25. M. Hall, Jr., *The theory of groups*, The Macmillan Company, New York, NY, 1959. MR 0103215.
26. A. Koch, T. Kohl, P. J. Truman, and R. Underwood, *Normality and short exact sequences of Hopf-Galois structures*, Comm. Algebra. **47** (2019), no. 5, 2086–2101. MR 3977722.
27. A. Koch, *Abelian maps, bi-skew braces, and opposite pairs of Hopf-Galois structures*, Proc. Amer. Math. Soc. Ser. B. **8** (2021), 189–203. MR 4273165.
28. A. Koch, *Abelian maps, brace blocks, and solutions to the Yang–Baxter equation*, J. Pure Appl. Algebra. **226** (2022), no. 9, 107047. MR 4381676.
29. T. Kohl, *Classification of the Hopf Galois structures on prime power radical extensions*, J. Algebra. **207** (1998), no. 2, 525–546. MR 1644203.
30. T. Kohl, *Characteristic subgroup lattices and Hopf–Galois structures*, Internat. J. Algebra Comput. **29** (2019), no. 2, 391–405. MR 3934792.
31. A. Konovalov, A. Smoktunowicz, and L. Vendramin, *On skew braces and their ideals*, Exp. Math. **30** (2021), no. 1, 95–104. MR 4223285.
32. A. Koch and P. J. Truman, *Opposite skew left braces and applications*, J. Algebra. **546** (2020), 218–235. MR 4033084.
33. A. Koch and P. J. Truman, *Skew left braces and isomorphism problems for Hopf–Galois structures on Galois extensions*, J. Algebra Appl. (2022). https://doi.org/10.1142/S0219498823501189
34. S. Montgomery, *Hopf algebras and their actions on rings*, CBMS Regional Conference Series in Mathematics, vol. 82 (published for the Conference Board of the Mathematical Sciences, Washington, DC), American Mathematical Society, Providence, RI, 1993. MR 1243637.
35. W. Rump, *Braces, radical rings, and the quantum Yang–Baxter equation*, J. Algebra **307** (2007), no. 1, 153–170. MR 2278047.
36. W. Rump, *Classification of cyclic braces*, J. Pure Appl. Algebra **209** (2007), no. 3, 671–685. MR 2298848.
37. E. Schenkman, *On the norm of a group*, Illinois J. Math. **4** (1960), 150–152. MR 113928.

38. L. Stefanello and S. Trappeniers, *On bi-skew braces and brace blocks*, J. Pure Appl. Algebra **227** (2023), no. 5, 107295. MR 4521746.
39. A. Smoktunowicz and L. Vendramin, *On skew braces*, J. Comb. Algebra **2** (2018), no. 1, 47–86. (With an appendix by N. Byott and L. Vendramin.) MR 3763907.
40. C. (Sin Yi) Tsang, *Hopf-Galois structures on cyclic extensions and skew braces with cyclic multiplicative group*, Proc. Amer. Math. Soc. Ser. B **9** (2022), 377–392. MR 4500760.
41. K. N. Zenouz, *Skew braces and Hopf–Galois structures of Heisenberg type*, J. Algebra **524** (2019), 187–225. MR 3905210.