Università di Pisa

Department of Mathematics

Dissertation for the Ph.D. Programme in Mathematics

Hopf–Galois Structures, Skew Braces, and Their Connection

Candidate: Lorenzo Stefanello

Supervisors: Prof. Ilaria Del Corso
Dr. Paul J. Truman

Date of defence: 10 April 2024

To Vichinga

Acknowledgement

I am deeply grateful to several people for their invaluable contributions throughout this extraordinary three-year journey that has been my Ph.D.

To Ilaria, for introducing me to beautiful mathematics and always encouraging me to do what was best for me, without ever considering your interests. Already halfway through my master's degree in Padova, I had decided that I wanted to do my doctorate with you. I have since turned down other positions, and there has never been a day when I regretted this choice.

To Paul, for agreeing to guide me into the world of Hopf–Galois structures with extreme generosity and professionalism. I have wonderful memories of our long work calls, which always began with conversations about ordinary life, and of my three trips to Keele, where you welcomed me in the best possible way.

To Andrea, for taking me under your wing and teaching me so much over the years, both professionally and personally. Your courses in Trento were the first to make me fall in love with mathematics and algebra, and it was an honour for me to have the opportunity to work and publish with you.

To Senne, for our collaborations that form the basis of this thesis. Your visit to Pisa and my visit to Brussels were among the highlights of my Ph.D.

To the mathematicians in the communities of Hopf–Galois structures and skew braces, for always welcoming me at the various events you have organised. You have made me feel accepted and part of something bigger than myself.

To PingPong132, for being a daily part of my last two years in Pisa. Sure, there were too many games and distractions, but you helped make this journey something unique.

To Majer Monaco, for giving me football emotions I have not felt in a long time, both in wins and losses.

To Elisa, for your exceptional hospitality and valuable advice about my career. Every day in Pisa you made me feel effortlessly at home.

To Alessandro, Andrea, Federico, Manuel, and all my friends, not only for sharing most of my passions, but also for enriching my life and constantly being there for me, without reservation.

To Stefania, Francesco, Pietro, Paola, and my family, because in spite of my difficult character, you never fail to provide me with your support.

To the most important person of all, Victoria. The fact that this is the third thesis dedicated to you explains the value of our relationship more than words can express.

Contents

Introduction

This dissertation deals with (the connection between) two active areas of algebra: Hopf–Galois theory and skew brace theory.

Overview of the literature

Hopf–Galois structures. The idea behind Hopf–Galois theory lies in the following observation: If L/K is a finite Galois extension of fields with Galois group G, then we can think as its "Galois structure" as consisting of the group algebra $K[G]$, which is a K-Hopf algebra, together with an action of $K[G]$ on L that satisfies well-known and nice properties. With this in mind, given a finite extension of fields L/K, we can define a *Hopf–Galois structure* on L/K to consist of a K-Hopf algebra H together with an action of H on L that mimics the properties of the group ring action in the Galois setting. In particular, when L/K is Galois with Galois group G, then the *classical structure* consists of $K[G]$ with the usual Galois action on L.

As suggested by the definition, Hopf–Galois structures provide a generalisation of classical Galois theory. In fact, Hopf–Galois structures may exist also for extensions of fields that are not necessarily Galois. For example, the main goal of [CS69], where this notion was introduced by Chase and Sweedler, was the study of certain extensions that are not even separable. The idea is that we can reproduce typical results of Galois theory in this more general setting, and to look for similar consequences, even for extensions that are not Galois. One important example is the following: Let L/K be a finite extension of fields, and consider a Hopf–Galois structure on L/K with K-Hopf algebra H. Then we can attach to each K-Hopf subalgebra of H an intermediate field of L/K, mimicking the usual Galois theoretic idea of taking fixed fields. The correspondence we obtain, called the *Hopf–Galois correspondence*, is injective but not necessarily surjective. It is of interest to find examples of Hopf–Galois structure with a bijective Hopf–Galois correspondence; as to be expected, this happens when we consider the classical structures.

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 of arithmetic nature. For example, as discussed by Byott in [Byo97], 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 structure; see [Chi00, CGK$^+$21] for a detailed analysis on the role of Hopf–Galois theory in local Galois module theory.

As a consequence of all these facts, the need of an effective way to describe Hopf–Galois extensions feels natural. A result in this direction was proved by Greither and Pareigis [GP87], who described explicitly Hopf–Galois structures for separable (not necessarily Galois) extensions in a group-theoretic terms. When applied to extensions that are also Galois, this description attaches to a Hopf–Galois structure a suitable regular subgroup of a permutation group, in a bijective way. This remarkable correspondence is transparent; given such a subgroup, corresponding to a Hopf–Galois structure on L/K, both the K-Hopf algebra and its action on L are explicitly described. In particular, the action on L is obtained by "twisting" that of the Galois group G.

The Greither–Pareigis theorem had a huge impact in Hopf–Galois theory. The possibility to describe concretely the Hopf–Galois structures opened several new directions. As a first implication, some of the main results of Hopf–Galois theory can be recast in a familiar way; the Hopf subalgebras of the Hopf algebras appearing in this theory can be detected in group-theoretic terms, and also the Hopf–Galois correspondence may be rewritten in a more manageable language [CRV16b, GP87, KKTU19]. As a consequence, some examples of Hopf–Galois structures on Galois extensions with a bijective Hopf–Galois correspondence were discussed: Greither and Pareigis found on every Galois extension a Hopf–Galois structure, the *canonical nonclassical structure*, with a bijective Hopf–Galois correspondence when the Galois group is Hamiltonian. Other examples were found in [KKTU19] computationally, via the computer software GAP. However, perhaps surprisingly, there are no more examples of this behaviour found with Greither–Pareigis theory; as explained in [KKTU19], the Hopf–Galois correspondence, recast thanks to the Greither–Pareigis theorem, can be explicitly described combinatorially, but remains quite mysterious.

One difficulty with Greither–Pareigis theorem is that to describe Hopf–Galois structure we have to consider $\mathrm{Perm}(G)$, whose size is quite large already for small sizes of G. In particular, the description of the required subgroups of $\mathrm{Perm}(G)$ may be computationally challenging. A solution to this issue was proposed in [Byo96]. Say that the *type* of a Hopf–Galois structure is the isomorphism class of the associated regular subgroup N. Then Byott translated the problem of finding the Hopf–Galois structures of type N on a finite Galois extension with Galois group G, to the problem of finding the regular subgroups isomorphic to G in the holomorph of N. As the holomorph has in general sensibly smaller size than a permutation group, it is clear how this translation motived several results of the following years, regarding classification, counting, and existence problems [Byo04, Byo07, BC12, Byo13, Byo15, BML22, CCDC20, CCDC24, Koh98, NZ19]. Nevertheless, a full classification of Hopf–Galois structures is far from being complete.

Skew braces. Building on previous work of Rump [Rum07a], Guarnieri and Vendramin introduced in [GV17] the notion of a new algebraic structure: a

skew (left) brace is a triple $(A, +, \circ)$, where $(A, +)$ and $(A, \circ)$ are (not necessarily abelian) groups related by a compatibility condition similar to a left distributivity. For example, if $(A, +)$ is a group, then $(A, +, +)$ satisfies this axiom, and skew braces of this form are called *trivial*.

The introduction of skew braces is motivated by the study of set-theoretic solutions of the Yang–Baxter equation [Dri92], an equation that arises from statistical mechanics with deep applications in mathematics and physics, such as for quantum groups, Hopf algebras, knot theory, and integrable systems. In particular, skew braces can be used to construct explicitly certain classes of these solutions, and given such a solution, one can attach to it a skew brace whose structure describes some of its properties [GV17]. Furthermore, in the last few years it has become evident how skew braces are related to many more topics of mathematics, such as radical rings, regular subgroups, and Hopf–Galois structures. As a consequence, a significant body of literature has been developed, and the multitude of techniques employed has become a trademark of this theory [Bac18, CJO14, Ced18, GV17, Rum07a, SV18].

As a consequence of these interactions, a systematic study of the algebraic structure of skew braces has commenced. Many notions typical of group and ring theory have been mimicked in the context of skew braces, such as (left) ideals, nilpotency, and solubility [BBERJSPC23, CSV19, GV17, JKVAV19, JKVAV21, KSV21]; a special role in this development has been played by the *gamma function* of a skew brace $(A, +, \circ)$, a suitable group homomorphism $\gamma\colon (A, \circ) \to \mathrm{Aut}(A, +)$. Various research directions have been followed in the last few years. We mention here some, which motivate some of the problems and questions addressed in this dissertation; given all the interactions of skew braces, it is not surprising that some of the following results or problems were originally formulated in different settings, and that in general it is of particular interest to understand what these statements mean in relation to other topics.

An important area of research consists of defining and studying particular classes of skew braces. Nilpotent (in various senses) skew braces were the main focus of [BJ23, CSV19, JVAV23], while soluble skew braces, whose definition follows the commutator theory for skew braces developed in [BFP23], were considered in [BBERJSPC23]. In [Chi19], Childs introduced the notion of *bi-skew brace*, which is a skew brace $(A, +, \circ)$ such that also $(A, \circ, +)$ is a skew brace. These objects were also the main focus of in [Car20]. A related class of skew braces, which we term *homomorphic* in this dissertation, was introduced by Bardakov, Neshchadim, and Yadav in [BNY22]. Other examples were studied in [CCS19, DC23, Rum14, Smo22].

A second possibility lies in the study of results related to the classification of skew braces of a given cardinality, or skew braces such that one of the underlying group operations is isomorphic to a given group. Problems of this kind were approached, for examples, in [AB20, AB21, Bac15, CCDC20, NZ19, Rum07b, Rum19]

A final direction consists of defining new examples of skew braces, possibly satisfying certain properties. These can be used as a sample for testing new conjectures, for disproving them (as in [Bac16]), or more in general, to under-

stand in a deeper way the connections of the skew braces with other topics. We just mention two constructions. Koch showed in [Koc21] how to start from a finite group $(A,+)$ and a group homomorphism $\psi\colon (A,+)\to(A,+)$ with abelian image to construct explicitly a bi-skew brace $(A,+,\circ)$. Similarly, in [BG22], Bardakov and Gubarev showed how to use Rota–Baxter operators for groups $(A,+)$, defined in [GLS21] in a totally different context, to construct skew braces of the form $(A,+,\circ)$.

Their connection. The idea of a possible connection between Hopf–Galois structures and skew braces was initially suggested by Bachiller [Bac16], and is based on the fact that both skew braces and Hopf–Galois structures have their interpretation by means of regular subgroups of the holomorph of a certain group. This intuition was formalised precisely in the appendix by Byott and Vendramin of [SV18], and also appeared in slightly different but equivalent terms in [NZ19] and [KT20].

So let L/K be a finite Galois extension of fields with Galois group G, and consider a Hopf–Galois structure on L/K. By the Greither–Pareigis theory, this structure corresponds to a certain regular subgroup N of $\mathrm{Perm}(G)$. The fact that N is regular naturally yields by transport of structure a group structure $(N,\circ)$ isomorphic to G and the additional condition that N needs to satisfy translates precisely to the skew brace axiom for $(N,+,\circ)$, where $+$ is the original group structure of N. Every (isomorphism class of) skew brace of the form $(N,+,\circ)$, with $(N,\circ)$ isomorphic to G, can be obtained in this way, but the connection we get is not bijective, as more Hopf–Galois structures may correspond to the same skew brace (up to isomorphism).

This surprising connection motivated even more both the topics, because it showed that quantitative problems, like counting and classifying, are essentially the same in the two settings. Nevertheless, this connection appeared less transparent for explicit results. It was not clear how the qualitative description of a skew brace and the knowledge of its structure yielded concrete information in Hopf–Galois theory, and very few results in the literature explored structural statements. In [Chi17, Chi18], Childs showed that given a Hopf–Galois structure with Hopf algebra H on a finite Galois extension L/K with Galois group G, then the K-Hopf subalgebras of H are in bijective correspondence with certain substructures of the associated skew brace. In this way, he managed to translate the Hopf–Galois correspondence into a skew brace setting, and showed that if G is cyclic of order p^n, for p odd prime, then all the Hopf–Galois structures on L/K have a bijective Hopf–Galois correspondence.

Despite this promising start, no new examples of this behaviour were found. Considering also the examples mentioned above, there were just four classes of examples of Galois extensions in which we may find surjective Hopf–Galois correspondences, as claimed for example in the introduction of [Chi21]. 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, for example the left ideals. This issue was initially

addressed by Koch and Truman [KT20], who introduced the concept of *opposite* skew brace and realised that the substructures studied by Childs coincide with the left ideals of the opposite skew brace. They moved the problem to a more familiar setting, and this intuition seems to suggest a deeper role of opposite skew braces in Hopf–Galois theory.

What is in this dissertation

The main goal of this dissertation is to propose a new version of the connection between Hopf–Galois structures and skew braces [ST23b], with the goal to make the connection bijective, explicit, and more structural. As already hinted at the end of the previous section, the known connection between these topics presents some issues. Specifically, the connection is not particularly transparent; it is not bijective, it requires us to pass through regular subgroups, and usually the classification and existence results of skew braces are not immediate to translate effectively in the setting of Hopf–Galois theory. While there are several quantitative results that are consequence of the connection, there are very few statements that explain how the knowledge of the structure of a skew brace can be translated in Hopf–Galois theory, and this implies that various properties of skew braces have no particular interpretation in relation to Hopf–Galois structures. The attempt of Childs to describe the Hopf subalgebras of the Hopf algebras appearing in Hopf–Galois theory in terms of certain substructures of the connected skew brace has been an important step in this direction, but the unfamiliarity of these structures in the context of skew braces limited the examples of bijective Hopf–Galois correspondence to just one class.

As already mentioned, in [KT20], it was shown how Childs's substructures are precisely the left ideals of the opposite skew brace. This fact motivated the work [ST23b] with Trappeniers. The basic structures of skew braces, left ideals, have a meaning in Hopf–Galois theory as soon as the skew brace considered is opposite to the usual one. So we wondered whether rethinking the connection using opposite skew braces could lead to new insights on both theories, fixing the issues mentioned above. We tried to approach the matter in two ways:

- "Straighten out" the connection, attaching to a Hopf–Galois structure a skew brace that, in the previous connection, would have been the opposite.
- Describe entirely the Hopf–Galois structures in terms of the associated skew braces, thinking of this connection in a bijective way.

With these points in mind, we proved the following theorem, which is Theorem 3.2.3 in this dissertation.

Theorem ($\star$)**.** *Let L/K be a finite Galois extension with Galois group $(G, \circ)$. Then there exists a bijective correspondence between*

- *the operations $+$ such that $(G, +, \circ)$ is a skew brace;*
- *the Hopf–Galois structures on L/K.*

Specifically, an operation $+$ such that $(G,+,\circ)$ is a skew brace corresponds to the Hopf–Galois structure $(H,\cdot)$ described as follows:

- *$H = L[(G,+)]^{(G,\circ)}$, where $(G,\circ)$ acts on L via Galois action and on $(G,+)$ via the gamma function γ of the skew brace $(G,+,\circ)$; in particular,*

$$H = \left\{ \sum_{\tau\in G} \ell_\tau \tau \in L[(G,+)] \mid \sigma(\ell_\tau) = \ell_{(\gamma(\sigma)_\tau)} \text{ for all } \sigma,\tau \in G \right\}.$$

- *Given $\sum_{\tau\in G} \ell_\tau \tau \in H$ and $x \in L$,*

$$\left(\sum_{\tau\in G} \ell_\tau \tau \right) \cdot x = \sum_{\tau\in G} \ell_\tau \tau(x).$$

The dissertation, as the title suggests, consists of three chapters, and it is structured in order to introduce, state, motivate, and discuss Theorem ($\star$). Specifically, the chapters are organised as follows.

An overview of Hopf–Galois structures. In Chapter 1 we introduce preliminary results in Hopf–Galois theory. In section 1.1, we recall some notions and properties of Hopf algebras, which are employed in section 1.2 to give the definition of Hopf–Galois structures. In order to deal with Theorem ($\star$), we need some results concerning Galois descent, which are stated and proved in section 1.3 in a form suitable to our needs, and also the known group-theoretic descriptions of Hopf–Galois structures via regular subgroups developed by Greither–Pareigis and Byott, which we recall in section 1.4.

New results on skew braces. In Chapter 2 we study skew braces. As mentioned, the goal of this dissertation is to discuss Theorem ($\star$), and thus to consider skew braces in relation to Hopf–Galois structures, mimicking in some sense the role of groups in classical Galois theory; however, in this chapter we opt to give a more general picture, by introducing new results we found in the collaborations [CS21, CS22, CS23, ST23a] with Caranti and with Trappeniers, even if they do not find immediate applications in Hopf–Galois theory.

After section 2.1, devoted to preliminaries, we propose in section 2.2 a systematic analysis of homomorphic skew braces and bi-skew braces, underlining various similarities of these classes and presenting results related to various notions of nilpotency and solubility. We also study their role in the study of solutions of the Yang–Baxter equation. Some of these results are applied in section 2.3, where we give a complete resolution of [Ven19, Problem 2.27], by showing in Theorem 2.3.10 that there are exactly three isomorphism classes of the skew braces $(A,+,\circ)$ with $(A,\circ)$ cyclic infinite, and describing them explicitly. These two sections are based on [ST23a].

After, in section 2.4, we study a class of skew braces, that we term *inner* and that have been already considered in literature in some instances. After some

immediate structural results, we introduce a characterisation of such skew braces in cohomological term, following in [CS23], in order to clarify their relation with Rota–Baxter operators; specifically, we show in Theorem 2.4.17 that we can attach the cohomology class of a suitable 2-cocycle to every inner skew brace, and that the inner skew brace can be obtained via a Rota–Baxter operator (as showed in [BG22]) if and only if this class is trivial.

Finally, in section 2.5, we propose new constructions to obtain skew braces, giving a particular focus on inner skew braces, homomorphic skew braces, and bi-skew braces. These constructions were developed in [CS21, CS22, ST23a], and various of these examples appear also in Chapter 3, as they provide examples of Hopf–Galois structures with desirable properties.

A new version of the connection. The final chapter is devoted to the development of the main goal of the dissertation, following the discussion of [ST23b].

In section 3.1, we recall the previous connection between Hopf–Galois structures and skew braces. We also give an overview of the results of Childs [Chi18] and Koch and Truman [KT20] that are strong motivation for what follows.

In section 3.2, we state and prove Theorem ($\star$), which is [ST23b, Theorem 3.1]. We give various examples and immediate applications of this result. As a first consequence, we show that the classical structure corresponds to the trivial skew brace; while this may seem unsurprising, it was not true in the previous description, where the classical structure yielded the opposite of the trivial skew brace.

It is important to remark that the usual quantitative results that were based on the previous connection between skew braces and Hopf–Galois structures can still be derived as a consequence of new perspective; in some specific case, the proofs are sensibly shorter, and the same also holds for some classical results in Hopf–Galois theory. We see this fact explicitly in section 3.3.

In section 3.4, we present some key consequences of Theorem ($\star$): the substructures and properties of the skew braces assume concrete meaning also in the theory of Hopf–Galois structures, as these can be used to describe explicitly the Hopf algebras appearing and their actions, which can be seen to be just slight variations of the usual Galois action. As a concrete example, we show in Theorem 3.4.1 that there exists a bijection the between left ideals of a skew brace and the Hopf subalgebras of a Hopf algebra, when these are connected by Theorem ($\star$).

As a consequence of this alignment, we shed in section 3.5 some light on the problem of the bijectivity of the Hopf–Galois correspondence, which we translate into a natural problem in skew brace theory. First, in Theorem 3.5.1, we present an effective method, given an intermediate field, to check whether it is in the image of the Hopf–Galois correspondence. We derive, in this way, examples of Hopf–Galois structures for which we can ask, a priori, the properties that intermediate fields need to satisfy in order to be in the image of the Hopf–Galois correspondence. Second, we provide an explicit way to obtain, on any given extension, a Hopf–Galois structure with a bijective Hopf–Galois correspondence, applying some properties of the *norm* of a group and some

constructions developed in section 2.5; see Theorem 3.5.10. While in some situations we can obtain just the trivial skew brace, in others we can find various new examples; for a Galois extension with quaternion Galois group, we obtain 16 Hopf–Galois structures with a bijective Hopf–Galois correspondence. Third, we study the role of bi-skew brace in Hopf–Galois theory, clarifying the relation between the two Hopf–Galois structures obtained by the two skew braces that underlie a bi-skew brace in Theorem 3.5.16. This gives an answer to a question of Childs [Chi21]. Finally, in Theorem 3.5.23, we classify entirely all the Galois extensions L/K such that every Hopf–Galois structure on L/K has a bijective Hopf–Galois correspondence, showing that this is the case exactly when the Galois group is cyclic and p does not divide $q-1$ for all primes p and q dividing the order of the Galois group.

We conclude the dissertation by summarising most of the consequence of Theorem $(\star)$ developed so far in a final "take-home" theorem presented in section 3.6.

Chapter 1

Hopf–Galois Structures

The goal of this chapter is to summarise preliminary results in the theory of Hopf–Galois structures. First, we give an overview of some facts about Hopf algebras, in order to present the main definitions and statements in Hopf–Galois theory, on the model of classical Galois theory. After, we review some results related to Galois descent; these play a key role for the study of various Hopf algebras properties in the final chapter of this work. Finally, we recall some descriptions of Hopf–Galois structures via group-theoretic tools.

In general, we state these well known results without proof, loosely following the first two chapters of [Chi00]. The only exception regards some statements for Galois descent, which are usually proved in literature for more specific cases, and which we prove for completeness.

In this chapter we fix a field K, and unadorned tensors denote tensors over K. If A is a K-algebra (always assumed to be associative), then we write

$$\mathbf{m}\colon A \otimes A \to A, \quad a \otimes b \mapsto ab$$

for the multiplication map and

$$\mathbf{i}\colon K \to A, \quad k \mapsto k1_A$$

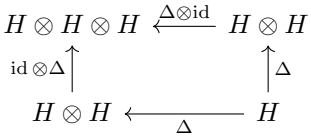
for the unit map, which are both linear maps.

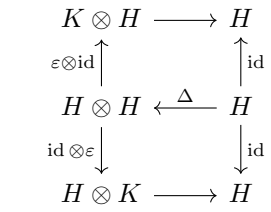
1.1 Hopf algebras

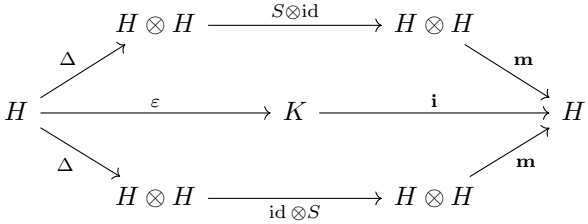
We begin with a quick overview of Hopf algebras, referring to classical books like [Swe69] and [Mon93]. To define Hopf algebras, one needs to talk about coalgebras and bialgebras. However, as these notions are not explicitly needed in the following, we just condense everything in a single definition.

Definition 1.1.1. A *K-Hopf algebra* is a K-algebra H together algebra homomorphisms $\Delta\colon H \to H \otimes H$ and $\varepsilon\colon H \to K$, called respectively *comultiplication*

and *counit*, and a linear map $S\colon H \to H$, called *antipode*, such that the following diagrams are commutative:







Notation 1.1.2. For the comultiplication of a K-Hopf algebra H, we adopt *Sweedler's notation*: if $h \in H$, then we write

$$\Delta(h) = \sum h_1 \otimes h_2 \in H \otimes H.$$

For example, by the definition of Hopf algebra, we obtain

$$\sum \varepsilon(h_1)h_2 = h = \sum h_1 \varepsilon(h_2).$$

Remark 1.1.3. As a K-Hopf algebra is also a K-algebra, we shall freely use terms related to notions typical of K-algebras also for Hopf algebras, tacitly referring to the underlying K-algebra structure. For example, a K-Hopf algebra H is *commutative* if H is so as a K-algebra.

Definition 1.1.4. Let H and J be K-Hopf algebras. An algebra homomorphism $f\colon H \to J$ is a *(K-)Hopf algebra homomorphism* if for all $h \in H$,

$$(f \otimes f)(\Delta(h)) = \Delta(f(h)), \qquad \varepsilon(h) = \varepsilon(f(h)), \qquad f(S(h)) = S(f(h)).$$

If in addition f is bijective, then we say that f is a *(K-)Hopf algebra isomorphism*, and we say that H and J are *isomorphic* (written $H \cong J$) as K-Hopf algebras.

Definition 1.1.5. Let H be a K-Hopf algebra.

- A *Hopf subalgebra* J of H is a subalgebra that satisfies $\Delta(J) \subseteq J \otimes J$ and $S(J) \subseteq J$.
- A *Hopf ideal* I of H is an ideal that satisfies $\Delta(I) \subseteq I \otimes H + H \otimes I$, $\varepsilon(I) = 0$, and $S(I) \subseteq I$.

Example 1.1.6. As to be expected, the Hopf ideals are exactly the kernels of the Hopf algebra homomorphisms:

- If H and J are K-Hopf algebras and $f\colon H \to J$ is a Hopf algebra homomorphism, then
$$\ker f = \{h \in H \mid f(h) = 0\}$$
is a Hopf ideal of H.
- If H is a K-Hopf algebra and I is a Hopf ideal of H, then also H/I is a K-Hopf algebra, with structure induced by that of H, and the map
$$\pi\colon H \to H/I, \quad h \mapsto \overline{h} = h + I$$
is a Hopf algebra homomorphism such that $\ker f = I$.

Definition 1.1.7. Let H be a K-Hopf algebra. A Hopf subalgebra J of H is *normal* if for all $h \in H$ and $j \in J$,
$$\sum h_1 j S(h_2) \in J.$$

For all Hopf subalgebras J of a K-Hopf algebra H, we write
$$J^+ = \{j \in J \mid \varepsilon(j) = 0\},$$
and we denote by HJ^+ and J^+H, respectively, the left ideal and right ideal of H generated by J^+.

Definition 1.1.8. A K-Hopf algebra H is *cocommutative* if for all $h \in H$,
$$\sum h_1 \otimes h_2 = \sum h_2 \otimes h_1.$$

For cocommutative Hopf algebras, normal Hopf subalgebras yield a natural notion of quotients that may be derived also from a categorical point of view [GSV19]. A proof of the following theorem can be found in [Mon93, Theorem 3.4.6].

Theorem 1.1.9. *Let H be a cocommutative K-Hopf algebra. Then there exists a bijective correspondence between*

- *the normal Hopf subalgebras of H;*
- *the Hopf ideals of H.*

Specifically, a normal Hopf subalgebra J corresponds to the Hopf ideal HJ^+.

In particular, if H is a cocommutative K-Hopf algebra and J is a normal Hopf subalgebra, then we can write a quotient K-Hopf algebra H/J, tacitly meaning H/HJ^+. We write

$$H/J = \left\{ \overline{h} \mid h \in H \right\},$$

where $\overline{h} = h + HJ^+$. The following result is immediate by [AD95b, Lemma 1.1.8]

Corollary 1.1.10. *Let H be a cocommutative K-Hopf algebra, and let J be a normal Hopf subalgebra of H. Then*

$$J^+H = HJ^+$$

Example 1.1.13 below motivates the following definition.

Definition 1.1.11. Let H be a K-Hopf algebra. An element $h \in H$ is *grouplike* if $h \neq 0$ and $\Delta(h) = h \otimes h$.

The next useful result is a consequence of the definition of a Hopf algebra homomorphism.

Lemma 1.1.12. *Let H and J be K-Hopf algebras, and let $f\colon H \to J$ be a Hopf algebra homomorphism. If h is a grouplike element of H, then $f(h)$ is a grouplike element of J.*

We finally present the main source of Hopf algebras we need to study.

Example 1.1.13. Let N be a finite group, and consider the *group algebra*

$$K[N] = \left\{ \sum_{\eta \in N} k_\eta \eta \mid k_\eta \in K \right\},$$

which is a K-algebra with multiplication obtained linearising the group operation of N. As customary, we identify $\eta \in N$ with $1_K \eta$, so that $N \subseteq K[N]$. The assignments

$$\Delta(\eta) = \eta \otimes \eta, \qquad \varepsilon(\eta) = 1, \qquad S(\eta) = \eta^{-1}$$

for all $\eta \in N$ extend to linear maps that endow $K[N]$ with a K-Hopf algebra structure.

It is well known that the Hopf algebra properties of $K[N]$ reflect the group properties of N. First, there exists a bijective correspondence between

- the (normal) subgroups of N;
- the (normal) Hopf subalgebras of $K[N]$.

Explicitly, the (normal) subgroup M of N corresponds to the (normal) Hopf subalgebra $K[M]$ of $K[N]$. If in particular M is normal in N, then the map

$$K[N]/K[M] \to K[N/M], \quad \overline{\sum_{\eta \in N} k_\eta \eta} \mapsto \sum_{\eta \in N} k_\eta \overline{\eta}$$

is a Hopf algebra isomorphism.

Second, it is immediate to check that the grouplike elements of $K[N]$ are exactly the elements of N.

Third, if $f\colon N \to M$ is a group homomorphism, then

$$K[N] \to K[M], \quad \sum_{\eta\in N} k_\eta \eta \mapsto \sum_{\eta\in N} k_\eta f(\eta)$$

is a Hopf algebra homomorphism, which we can denote again by f. In addition, by Lemma 1.1.12, one can check that all the Hopf algebra homomorphisms $K[N] \to K[M]$ arise in this way, and that $N \cong M$ if and only if $K[N] \cong K[M]$ as K-Hopf algebras.

Finally, if N is isomorphic to the direct product of two subgroups M and M', then $K[N] \cong K[M] \otimes K[M']$ as K-Hopf algebras.

Remark 1.1.14. Let H be a finite-dimensional K-Hopf algebra. Then the grouplike elements of H are linearly independent and form a group, denoted by $\mathrm{GP}(H)$, under the Hopf algebra multiplication; see [Chi00, Propositions 1.6 and 1.7]. In particular, if the order of $\mathrm{GP}(H)$ equals $\dim_K H$, then one can readily deduce that $H \cong K[\mathrm{GP}(H)]$ as Hopf algebras. We make this isomorphism an identification, and thus in the following we say that a finite-dimensional K-Hopf algebra H is a *group algebra* exactly when

$$\dim_K H = |\,\mathrm{GP}(H)|.$$

1.2 Hopf–Galois theory

We proceed with the definition of a Hopf–Galois structure and some first important properties, mainly following [Chi00]. A possible reference for the well known results in Galois theory we state is [Win74].

1.2.1 From Galois to Hopf–Galois

In order to understand the motivations behind the definitions of Hopf–Galois structures, it is convenient to start from a reformulation of the definition of a Galois extension. Recall that a finite extension L/K of fields is *Galois* if its degree $[L : K]$ equals the order of the group G of K-algebra automorphisms of L. If this is the case, then G is called the *Galois group* of L/K. Note that there is a natural action of the group algebra $K[G]$ on L, extending linearly the action of G on L. The following result is a consequence of the linear independence of characters; see [Chi00, Example 2.6].

Proposition 1.2.1. *Let L/K be a finite extension of fields, and let G be the group of K-algebra automorphisms of L. Then the following are equivalent:*

- *L/K is Galois (with Galois group G).*

- *The L-linear map*

$$L \otimes_K K[G] \to \mathrm{End}_K(L), \quad \ell \otimes \sum_{\tau \in G} k_\tau \tau \mapsto \left(x \mapsto \ell \sum_{\tau \in G} k_\tau \tau(x) \right).$$

  is bijective.

This proposition yields a definition of a Galois extension just in terms of group algebras; as mentioned, the structure of a group algebra that best captures the group properties of the underlying group is that of a Hopf algebras. This suggests the possibility to replace the group algebra with a more general Hopf algebra, together with an action that mimics the properties of the Galois action.

Definition 1.2.2. Let L/K be a finite extension of fields, and let H be a K-Hopf algebra. We say that L is a *(left) H-module algebra* if there exists an action $\cdot$ of H on L such that L is a left H-module and for all $k \in K$, $h \in H$, and $x, y \in L$,

$$k(h \cdot x) = (kh) \cdot x = h \cdot (kh), \qquad h \cdot (xy) = \sum (h_1 \cdot x)(h_2 \cdot y), \qquad h \cdot 1_L = \varepsilon(h) 1_L.$$

The first requirement in Definition 1.2.2 makes the K-linear structures of H and L compatible in the obvious way; equivalently, the map

$$H \otimes L \to L, \qquad h \otimes x \mapsto h \cdot x$$

needs to be K-linear. The other requirements show that this definition is modelled on the behaviour of Galois extensions, as in the case in which L/K is Galois with Galois group G and $H = K[G]$, these conditions translate into

$$\sigma(xy) = \sigma(x)\sigma(y), \qquad \sigma(1_L) = 1_L.$$

for all $\sigma \in G$ and $x, y \in L$.

We are now in the right position to give the main definition.

Definition 1.2.3. Let L/K be a finite extension, and let H be a K-Hopf algebra. We say that L/K is *H-Galois* if the following hold:

- L is an H-module algebra.
- The linear map

$$L \otimes_K H \to \mathrm{End}_K(L), \quad \ell \otimes h \mapsto (x \mapsto \ell(h \cdot x)).$$

  is bijective.

The pair $(H, \cdot)$ is a *Hopf–Galois structure* on L/K.

Remark 1.2.4. Given a finite extension L/K of fields, we make the following standard identification: two Hopf–Galois structures $(H, \cdot)$ and $(J, \cdot)$ on L/K are

identified if and only if there exists a Hopf algebra isomorphism $\varphi\colon H \to J$ such that for all $h \in H$ and $x \in L$,

$$\varphi(h) \cdot x = h \cdot x. \tag{1.1}$$

In particular, if $(H, \cdot)$ is a Hopf–Galois structure on L/K and J is a K-Hopf algebra such that there exists a Hopf algebra isomorphism $\varphi\colon H \to J$, then we can employ (1.1) to obtain a Hopf–Galois structure $(J, \cdot)$ on L/K that equals $(H, \cdot)$.

Example 1.2.5. Let L/K be a finite Galois extension with Galois group G. Then L/K is $K[G]$-Galois by Proposition 1.2.1, and the Hopf–Galois structure we obtain in this way is the *classical structure*.

From Definition 1.2.3, we can derive two properties of a Hopf algebra H such that there exists an H-Galois extension L/K of fields. First, the bijection

$$L \otimes_K H \to \mathrm{End}_K(L)$$

immediately implies that

$$\dim_K L = \dim_K H.$$

In particular, the Hopf algebra H is finite-dimensional. Second, one can check that H is necessarily cocommutative; see the discussion in [Chi00, 2.19].

1.2.2 The Hopf–Galois correspondence

Once the definition of a Hopf–Galois structure is given, it feels natural to enquire whether typical results of Galois theory can be generalised or reinterpreted. We state here a variation of the fundamental theorem of Galois theory in Hopf–Galois theory. Recall that given an intermediate field F of a finite Galois extension L/K, the extension L/F is Galois, and F is *normal* if also F/K is Galois.

Theorem 1.2.6 (Fundamental theorem of Galois theory)**.** *Let L/K be a finite Galois extension with Galois group G. Then there exists an inclusion-reversing bijective correspondence between*

- *the (normal) subgroups of G;*
- *the (normal) intermediate fields of L/K.*

Specifically, a (normal) subgroup T of G corresponds to the (normal) intermediate field

$$L^T = \{x \in L \mid \tau(x) = x \text{ for all } \tau \in T\}$$

of L/K, and L/L^T is Galois with Galois group T. In addition, when T is normal, the Galois group of L^T/K is (identified with) G/T.

We can rewrite this result just in terms of the group algebra and its action. Take a finite Galois extension L/K with Galois group G, and consider the classical structure $(K[G], \cdot)$ on L/K. If J is a (normal) Hopf subalgebra of $K[G]$, then there exists a (normal) subgroup T of G such that $J = K[T]$, and a straightforward calculation shows that

$$L^T = \{x \in L \mid j \cdot x = \varepsilon(j)x \text{ for all } j \in J\}.$$

With this observation in mind, we can take a finite extension L/K, consider a Hopf–Galois structure $(H, \cdot)$ on L/K, and, given a Hopf subalgebra J of H, define

$$L^J = \{x \in L \mid j \cdot x = \varepsilon(j)x \text{ for all } j \in J\}.$$

One can check, as in the classical case, that L^J is an intermediate field of L/K. For example, if $0 \neq x \in L^J$, then also $x^{-1} \in L^J$: for all $j \in J$, recalling that $j = \sum \varepsilon(j_1)j_2$ and also $j_1 \in J$, we get

$$\begin{aligned}\varepsilon(j)1_L = j \cdot 1_L = j \cdot (xx^{-1}) &= \sum (j_1 \cdot x)(j_2 \cdot x^{-1}) \\ &= \sum (\varepsilon(j_1)x)(j_2 \cdot x^{-1}) = x\left(\sum \varepsilon(j_1)j_2 \cdot x^{-1}\right) = x(j \cdot x^{-1}),\end{aligned}$$

that is,

$$j \cdot x^{-1} = \varepsilon(j)x^{-1}.$$

In addition, it is straightforward to check that L is an $L^J \otimes J$-module algebra, with action

$$(\ell \otimes j) \cdot x = \ell(j \cdot x).$$

Similarly, when J is normal in H, then L^J is an H/J-module algebra, with the following action: for all $x \in L^J$ and $\overline{h} \in H/J$,

$$\overline{h} \cdot x = h \cdot x.$$

We just check here that this is indeed well-defined. First, if $h' = h + \sum h_i j_i$ with $h_i \in H$ and $j_i \in J^+$, then

$$h \cdot x - h' \cdot x = (\sum h_i j_i) \cdot x = \sum h_i \cdot (\varepsilon(j_i)x) = 0.$$

Second, we need to check that $h \cdot x \in L^J$. So take $j \in J$, and note that the equality $J^+H = HJ^+$ by Corollary 1.1.10 implies that there exist $h_i \in H$ and $j_i \in J^+$ such that

$$(j - \varepsilon(j)1_J)h = \sum_i h_i j_i,$$

We conclude that

$$j \cdot (h \cdot x) - \varepsilon(j)(h \cdot x) = (j - \varepsilon(j)1_J)(h \cdot x) = \left(\sum_i h_i j_i\right) \cdot x = 0,$$

that means $h \cdot x \in L^J$.

The following result, which is a weaker version of Theorem 1.2.6 in the context of Hopf–Galois structures, combines [CS69, Theorem 7.6], [GP87, Theorem 5.1], [Gre92, section II, Lemma 1.6], and [Byo02, Lemma 4.1].

Theorem 1.2.7. *Let L/K be a finite extension of fields, and let H be a K-Hopf algebra such that L/K is H-Galois. Then the assignment*

$$J \to L^J = \{x \in L \mid j \cdot x = \varepsilon(j)x \text{ for all } j \in J\}$$

gives an inclusion-reversing injective correspondence from the Hopf subalgebras of H to the intermediate fields of L/K. In addition, if J is a Hopf subalgebra of H, then L/L^J is $L^J \otimes J$-Galois, and if J is also normal in H, then L^J/K is H/J-Galois.

The correspondence in Theorem 1.2.7 is the *Hopf–Galois correspondence*. The following is an immediate corollary.

Corollary 1.2.8. *Let L/K be a finite extension, and let H be a K-Hopf algebra such that L/K is H-Galois. If J is a Hopf subalgebra of H, then*

$$\dim_K J = [L : L^J].$$

Remark 1.2.9. When considered in the classical context, the Hopf–Galois correspondence yields the usual Galois correspondence between subgroups of the Galois group and intermediate fields, which is bijective. However, in general, the Hopf–Galois correspondence is injective but not necessarily surjective. One of the main consequences of the description of Hopf–Galois structures via skew braces that we present in the final chapter is to propose novel methods to find and construct examples of Hopf–Galois structures with a bijective Hopf–Galois correspondence on Galois extensions, increasing a list that before contained only a few items [Chi17, GP87, KKTU19].

The following definition introduces an invariant capturing some behaviour of the Hopf–Galois correspondence, as it is the ratio of the intermediate fields in the image of the Hopf–Galois correspondence to all the intermediate fields.

Definition 1.2.10. Let L/K be a finite extension, and let H be a K-Hopf algebra such that L/K is H-Galois. The *Hopf–Galois correspondence ratio* is

$$\mathrm{HGC}(L/K, H) = \frac{|\{\text{Hopf subalgebras of } H\}|}{|\{\text{intermediate fields of } L/K\}|}.$$

It is clear that the Hopf–Galois correspondence ratio measure how far the Hopf–Galois correspondence is to be bijective, and it equals 1 exactly when all the intermediate fields are in the image of the Hopf–Galois correspondence. This invariant, in the context of Galois extensions, has been mainly considered in recent works of Childs [Chi17, Chi18, Chi21].

1.3 Galois descent

The theory of Galois descent for Hopf algebras is well-known. A sketch of the proof of the main result can be found, for example, in [Chi00, 2.12], based on Morita equivalences [CR81, section 3D]. We proceed here with a more direct and elementary treatment, which arises from the analogous result for vector spaces, given for example in [Win74, section 3.2].

1.3.1 From vector spaces to Hopf algebras

Galois descent is in some sense the inverse of extension of scalars. Let L/K be a finite Galois extension with Galois group G. If V is a K-vector space, then it is well-known that $L \otimes V$ is an L-vector space. In the same way, if H is a K-Hopf algebra, then $L \otimes H$ is a L-Hopf algebra, with operations inherited by those of H. In addition, a K-Hopf algebra homomorphism

$$f\colon H \to J$$

yields an L-Hopf algebra homomorphism

$$\mathrm{id} \otimes f\colon L \otimes H \to L \otimes J, \quad \ell \otimes h \mapsto \ell \otimes f(h),$$

and f is injective (respectively surjective) if and only if $\mathrm{id} \otimes f$ is injective (respectively surjective).

Galois descent asks about the opposite situation, inquiring whether a given L-Hopf algebra H can be obtained as $L \otimes J$ for some K-Hopf algebra J. It is convenient to start from the case of vector spaces.

Definition 1.3.1. Let V be an L-vector space. A group action of G on V is *semilinear* if for all $\sigma \in G$, $v, w \in V$, and $\ell \in L$,

$$\sigma(v + w) = \sigma(v) + \sigma(w), \qquad \sigma(\ell v) = \sigma(\ell)\sigma(v).$$

The requirement for an action of G on an L-vector space V to be semilinear implies that

$$V^G = \{v \in V \mid \sigma(v) = v \text{ for all } \sigma \in G\}$$

is a K-vector space. Similarly, if V and W are L-vector spaces with a semilinear action of G and an L-linear map $f\colon V \to W$ is a *G-equivariant*, that is,

$$f(\sigma(v)) = \sigma(f(v))$$

for all $v \in V$ and $\sigma \in G$, then

$$f^G\colon V^G \to W^G, \quad v \mapsto f(v)$$

is a K-linear map.

As V^G is a K-vector space, it follows that $L \otimes V^G$ is an L-vector space, with a natural semilinear action of G obtained by the action of G on L. The following result is due to Speiser; see [Win74, Theorem 3.2.5].

Theorem 1.3.2 (Speiser's theorem)**.** *Let V be an L-vector space with a semilinear action of G. Then the map*

$$L \otimes V^G \to V, \quad \ell \otimes v \mapsto \ell v$$

is a G-equivariant L-linear bijection.

As a consequence, we derive that if V and W are L-vector spaces with a semilinear action of G, then a G-equivariant L-linear map $f\colon V \to W$ is injective (respectively surjective) if and only if $f^G\colon V^G \to W^G$ is injective (respectively surjective). In addition, we obtain that the diagonal action of G on $V \otimes_L W$ is semilinear and the K-linear map

$$V^G \otimes W^G \to (V \otimes_L W)^G, \quad v \otimes w \mapsto v \otimes w$$

is bijective.

We consider now the case of Hopf algebras.

Definition 1.3.3. Let H be an L-Hopf algebra. A semilinear action of G on H is *Hopf semilinear* if for all $\sigma \in G$ and $h, j \in H$,

$$\begin{aligned} \sigma(hj) &= \sigma(h)\sigma(j), \\ \sigma(1_H) &= 1_H \\ \sum \sigma(h_1) \otimes \sigma(h_2) &= \sum \sigma(h)_1 \otimes \sigma(h)_2 \\ \sigma(\varepsilon(h)) &= \varepsilon(\sigma(h)) \\ \sigma(S(h)) &= S(\sigma(h)). \end{aligned}$$

In other words, in Definition 1.3.3 we require that the action of G on a K-Hopf algebra H respects the Hopf algebra structure of H, meaning that the maps $\mathbf{m}, \mathbf{i}, \Delta, \varepsilon, S$ of H are G-equivariant (where the action of G on $H \otimes H$ is diagonal). In particular, this implies that H^G is not just a K-vector space, but also a K-Hopf algebra with structure induced by that of H.

For the algebra structure, this is particularly easy to see; if $h, j \in H^G$ and $\sigma \in G$, then

$$\sigma(hj) = \sigma(h)\sigma(j) = hj,$$

which shows that $hj \in H^G$. Similarly, $\sigma(1_H) = 1_H$ implies that $1_H \in H^G$.

For the Hopf algebra, the situation is slightly more delicate. The condition relating the action and the comultiplication implies if $h \in H^G$, then $\Delta(h) \in (H \otimes_L H)^G$; to obtain a map $H^G \to H^G \otimes H^G$, we may employ the L-linear isomorphism

$$H^G \otimes H^G \to (H \otimes_L H)^G, \quad h \otimes j \mapsto h \otimes j,$$

which follows by Theorem 1.3.2. In other words, if $h \in H^G$, then we can assume that $\Delta(h) = \sum h_1 \otimes h_2$ with $h_1, h_2 \in H^G$, and define

$$\Delta^G\colon H^G \to H^G \otimes H^G, \quad h \mapsto \sum h_1 \otimes h_2.$$

Once this map is defined, we can use again the properties of the Hopf algebra H to deduce analogue properties for H^G, which is then a K-Hopf algebra. In particular, if H is cocommutative, then also H^G is cocommutative.

At this point, one can note that the isomorphism described in Speiser's theorem respects also the Hopf algebra structure, in order to derive the following result.

Theorem 1.3.4 (Speiser's theorem for Hopf algebras)**.** *Let H be an L-Hopf algebra with a Hopf semilinear action of G. Then the map*

$$L \otimes H^G \to H, \quad \ell \otimes h \mapsto \ell h$$

is a G-equivariant L-Hopf algebra isomorphism.

We list here some known results we can derive from this theorem. For convenience, we also provide some quick proofs. First, we consider substructures and quotients. Given a Hopf semilinear action of G on a K-Hopf algebra H, we say that a Hopf subalgebra J of H is *G-invariant* if the action of G on H restricts to an action on J. (The same definition can also be given for subgroups of a group N with an action of G via automorphisms).

Proposition 1.3.5. *Let H be an L-Hopf algebra with a Hopf semilinear action of G. Then there exists a bijective correspondence between*

- *the G-invariant (normal) Hopf subalgebras of H;*
- *the (normal) Hopf subalgebras of H^G.*

Specifically, a G-invariant (normal) Hopf subalgebra J of H corresponds to the (normal) Hopf subalgebra J^G of H^G.

Proof. If J is a G-invariant Hopf subalgebra of H, then the inclusion

$$J \hookrightarrow H, \quad j \mapsto j$$

is an injective G-equivariant L-Hopf algebra homomorphism, which yields an injective K-Hopf algebra homomorphism

$$J^G \hookrightarrow H^G, \quad j \mapsto j.$$

This immediately implies that J^G is a Hopf subalgebra of H^G. Now note that J is normal in H if and only if for all $h \in H$ and $j \in J$,

$$\sum h_1 j S(h_2) \in J.$$

If $h \in H^G$, then $h_1, h_2 \in H^G$, so that given $j \in J^G$, we obtain

$$\sum h_1 j S(h_2) \in J \cap H^G = J^G.$$

Conversely, let P be a K-Hopf subalgebra of H^G. If we denote by φ the L-Hopf algebra isomorphism

$$\varphi \colon L \otimes H^G \to H,$$

then we find that $\varphi(L \otimes P) = J$ is an L-Hopf subalgebra of H. But the equality $\varphi(L \otimes J^G) = J$ and the fact that φ is a bijection imply that $P = J^G$. An easy computation shows that if $P = J^G$ is normal in H^G, then $L \otimes P$ is normal in $L \otimes H^G$. We conclude that $J = \varphi(L \otimes P)$ is normal in $H = \varphi(L \otimes H^G)$. ☐

Proposition 1.3.6. *Let H be an L-Hopf algebra with a Hopf semilinear action of G, and let J be a G-invariant normal Hopf subalgebra of H. Then there exists a Hopf semilinear action of G on H/J and the map*

$$H^G/J^G \to (H/J)^G, \quad h + H^G(J^G)^+ = \overline{h} \mapsto \overline{h} = h + HJ^+$$

is a K-Hopf algebra isomorphism.

Proof. It is immediate to check that $\sigma(j) \in J^+$ for all $\sigma \in G$ and $j \in J^+$; this implies that the action of G on H/J given by

$$\sigma(\overline{h}) = \overline{\sigma(h)}$$

is a well-defined Hopf semilinear action. We deduce that the natural surjective L-Hopf algebra homomorphism

$$\pi\colon H \to H/J,$$

with kernel HJ^+, is also G-equivariant. We obtain a surjective K-Hopf algebra homomorphism

$$\pi^G\colon H^G \to (H/J)^G.$$

We need to check that the kernel of π^G, which clearly is $(\ker \pi)^G$, equals $H^G(J^G)^+$, or equivalently, that the obvious linear map

$$H^G \otimes (J^G)^+ \to \ker \pi^G$$

is surjective. This follows from the surjectivity of the composition

$$H^G \otimes (J^G)^+ = H^G \otimes (J^+)^G \to (H \otimes_L J^+)^G \to \ker \pi^G,$$

where in the first equality we have used the fact that the action of G respects the counit, the map in the middle is a bijection as mentioned before, and the surjectivity of the last map follows by Galois descent and surjectivity of

$$H \otimes J^+ \to \ker \pi.$$ □

We see now how we can control the grouplike elements.

Proposition 1.3.7. *Let H be an L-Hopf algebra with a Hopf semilinear action of G. Then the grouplike elements of H^G are the grouplike elements of H that are fixed by the action of G.*

Proof. This easily follows by the description of the comultiplication of H^G. □

Finally, we can extend some results from the setting of vector spaces to that of Hopf algebras. In these formulations, they do not need the full power of Theorem 1.3.4, but just the observation that the Hopf algebra structures are preserved.

Proposition 1.3.8. *Let H and J be L-Hopf algebras with a Hopf semilinear action of G. If*

$$\varphi\colon H \to J$$

is a G-equivariant L-Hopf algebra isomorphism, then

$$\varphi^G\colon H^G \to J^G$$

is a K-Hopf algebra isomorphism.

Proof. We have already mentioned the first part of the result in the context of vector spaces. It is just a matter of checking that if φ respects the Hopf algebra structure of H and J, then φ^G respect the Hopf algebra structure of H^G and J^G, as these are induced by those of H and J, respectively. □

Proposition 1.3.9. *Let H and J be L-Hopf algebras with a Hopf semilinear action of G. Then the map*

$$H^G \otimes J^G \to (H \otimes_L J)^G, \quad h \otimes j \to h \otimes j$$

is a K-Hopf algebra isomorphism.

Proof. We have already mentioned that this map is a K-linear bijection. It is just a matter of computation to check that this respects the Hopf algebra structures of the objects involved. □

1.3.2 Descent of group algebras

As an application, we derive some results for descent of group algebras. Let us take a finite Galois extension L/K with Galois group G and a finite group N, and consider the group algebra $L[N]$. If G acts on N via automorphisms, then we can define an action of G on $L[N]$ as follows:

$$\sigma\left(\sum_{\eta\in N} \ell_\eta \eta\right) = \sum_{\eta\in N} \sigma(\ell_\eta)\sigma(\eta).$$

It is straightforward to check that this action of G on $L[N]$ is Hopf semilinear. In addition, every Hopf semilinear action of G on $L[N]$ arises in this way, as such an action needs to preserve the grouplike elements of $L[N]$ (precisely as in Lemma 1.1.12).

In particular, exactly as the group properties of N reflects the Hopf algebra properties of $L[N]$, we obtain that the behaviour of an action of G on N via automorphisms captures the behaviour of the associated Hopf semilinear action of G on $L[N]$. This means that if G acts on N via automorphisms, so on $L[N]$ Hopf semilinearly, then we can rewrite Example 1.1.13 exactly as it is, just adding the appropriate words related to the actions of G. For example, there exists a bijective correspondence between

- the G-invariant (normal) subgroups of N;
- the G-invariant (normal) Hopf subalgebras of $L[N]$.

So let N be a finite group with an action of G via automorphism, and consider the group algebra $L[N]$. We obtain a K-Hopf algebra

$$L[N]^G = \left\{ \sum_{\eta \in N} \ell_\eta \eta \in L[N] \mid \sigma(\ell_\eta) = \ell_{\sigma(\eta)} \text{ for all } \sigma \in G \text{ and } \eta \in N \right\}$$

such that

$$L \otimes L[N]^G \to L[N], \quad \left(\ell \otimes \sum_{\eta \in N} \ell_\eta \eta \right) \mapsto \ell \sum_{\eta \in N} \ell_\eta \eta$$

is an L-Hopf algebra isomorphism. If we combine these observations with the consequences of Galois descent mentioned in the previous section, we can describe the Hopf algebra structure of $L[N]^G$.

Corollary 1.3.10. *Let N be a finite group with an action of G via automorphisms. Then there exist a bijective correspondence between*

- *the G-invariant (normal) subgroups of N;*
- *the (normal) Hopf subalgebras of $L[N]^G$.*

Specifically, a (normal) subgroup M of N corresponds to the (normal) Hopf subalgebra $L[M]^G$ of $L[N]^G$.

Corollary 1.3.11. *Let N be a finite group with an action of G via automorphisms, and let M be a G-invariant normal subgroup of N. Then the map*

$$L[N]^G / L[M]^G \to L[N/M]^G, \quad \overline{\sum_{\eta \in N} \ell_\eta \eta} \mapsto \sum_{\eta \in N} \ell_\eta \overline{\eta}.$$

is a K-Hopf algebra isomorphism.

For the next result, recall also Remark 1.1.14.

Corollary 1.3.12. *Let N be a finite group with an action of G via automorphisms. Then the grouplike elements of $L[N]^G$ are the elements of N that are fixed by G. In particular, $L[N]^G$ is a group algebra if and only if G acts on N trivially, and if this is the case, then $L[N]^G = K[N]$.*

Corollary 1.3.13. *Let N and M be finite groups with an action of G via automorphisms. If*

$$\varphi \colon N \to M$$

is a G-equivariant group isomorphism, then

$$L[N]^G \to L[M]^G, \quad \sum_{\eta \in N} \ell_\eta \eta \mapsto \sum_{\eta \in N} \ell_\eta \varphi(\eta)$$

is a K-Hopf algebra isomorphism. In addition, all the K-Hopf algebra isomorphisms between $L[N]^G$ and $L[M]^G$ arise in this way.

Corollary 1.3.14. *Let N be a finite group with an action of G via automorphisms, and suppose that N is the direct product of two G-invariant subgroups M and M'. Then*

$$L[N]^G \cong L[M]^G \otimes L[M']^G$$

as K-Hopf algebras.

1.4 Hopf–Galois structures and regular subgroups

We conclude this chapter by mentioning two main results describing Hopf–Galois structures in group-theoretic terms: the Greither–Pareigis theorem [GP87] and Byott's translation [Byo96]. While both can be stated for finite separable extensions, we focus our attention on the Galois case. We mainly follow [Chi00, Chapter 2], where an overview on regular subgroups is also given.

1.4.1 Regular subgroups

We begin with a quick reminder on regular subgroups, a standard notion in group theory. Let G be a finite group, and denote by $\mathrm{Perm}(G)$ the group of bijective maps $G \to G$.

Definition 1.4.1. A subgroup N of $\mathrm{Perm}(G)$ is *regular* if the map

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

is bijective.

Example 1.4.2 (Cayley's theorem)**.** We denote by λ the *left regular representation* of G:

$$\lambda\colon G \to \mathrm{Perm}(G), \quad \sigma \mapsto \lambda(\sigma)\colon \tau \mapsto \sigma\tau.$$

Similarly, we denote by ρ the *right regular representation* of G:

$$\rho\colon G \to \mathrm{Perm}(G), \quad \sigma \mapsto \rho(\sigma)\colon \tau \mapsto \tau\sigma^{-1}.$$

Then $\lambda(G)$ and $\rho(G)$ are regular subgroup of $\mathrm{Perm}(G)$, which coincide if and only if G is abelian.

Definition 1.4.3. The *holomorph* $\mathrm{Hol}(G)$ of G is the normaliser of $\lambda(G)$ in $\mathrm{Perm}(G)$.

A well-known result in group theory shows that $\mathrm{Hol}(G)$ is isomorphic to the semidirect product of $\lambda(G)$ and $\mathrm{Aut}(G)$ in $\mathrm{Perm}(G)$, so that there exists an isomorphism

$$G \rtimes \mathrm{Aut}(G) \to \mathrm{Hol}(G), \quad (\sigma, \alpha) \mapsto \lambda(\sigma)\alpha.$$

The natural semidirect product $G \rtimes \mathrm{Aut}(G)$, for this reason, is usually referred to as the *abstract holomorph* of G.

1.4.2 The Greither–Pareigis theorem

We state here the main theorem of [GP87], specialised to the case in which the extensions considered are Galois.

Let L/K be a finite Galois extension with Galois group G, and let N be a regular subgroup of $\mathrm{Perm}(G)$. Suppose that N is normalised by $\lambda(G)$. Then $\lambda(G)$ acts on N via conjugation, and thus we obtain an action of G on N via automorphisms. This action extends to a Hopf semilinear action of G on $L[N]$, and by Galois descent, the L-Hopf algebra $L[N]$ descends to the K-Hopf algebra

$$L[N]^G = \left\{ \sum_{\eta \in N} \ell_\eta \eta \in L[N] \mid \sigma(\ell_\eta) = \ell_{\lambda(\sigma)\eta\lambda(\sigma)^{-1}} \text{ for all } \sigma \in G \text{ and } \eta \in N \right\}.$$

Theorem 1.4.4 (Greither–Pareigis)**.** *Let L/K be a finite Galois extension with Galois group G. Then there exists a bijective correspondence between*

- *the regular subgroups of* $\mathrm{Perm}(G)$ *normalised by* $\lambda(G)$*;*
- *the Hopf–Galois structures on L/K.*

Specifically, a regular subgroup N of $\mathrm{Perm}(G)$ *normalised by* $\lambda(G)$ *corresponds to the Hopf–Galois structure $(L[N]^G, \cdot)$ on L/K, where*

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

Definition 1.4.5. Let L/K be a finite Galois extension with Galois group G, and consider a Hopf–Galois structure on L/K, corresponding to a regular subgroup N of $\mathrm{Perm}(G)$. The *type* of the Hopf–Galois structure is the isomorphism class of N.

There are always two standard Hopf–Galois structures of type G on a finite Galois extension with Galois group G, corresponding to $\rho(G)$ and $\lambda(G)$; see [Chi00, Example 6.9]

Example 1.4.6. Let L/K be a finite Galois extension with Galois group G, and consider $N = \rho(G)$. As $\rho(G)$ and $\lambda(G)$ commute, meaning that the action of $\lambda(G)$ on $\rho(G)$ is trivial, we easily derive that

$$H = L[\rho(G)]^G = L^G[\rho(G)] = K[\rho(G)],$$

with action on L given by

$$\left(\sum_{\tau \in G} k_\tau \rho(\tau) \right) \cdot x = \sum_{\tau \in G} k_\tau \tau(x).$$

In particular, the group isomorphism

$$G \to \rho(G), \quad \sigma \to \rho(\sigma)$$

yields a Hopf algebra isomorphism

$$K[G] \to K[\rho(G)]$$

which respects the actions on L, and thus we conclude that $\rho(G)$ corresponds to the classical structure on L/K.

Example 1.4.7. Let L/K be a finite Galois extension with Galois group G, and consider $N = \lambda(G)$. This yields a Hopf–Galois structure on L/K, called the *canonical nonclassical structure*. Note that G acts on G via conjugation, and the map

$$G \to \lambda(G), \quad g \mapsto \lambda(g)$$

is a G-equivariant group isomorphism that yields a K-Hopf algebra isomorphism

$$L[G]^G \to L[\lambda(G)]^G$$

by Corollary 1.3.13. As $L[\lambda(G)]^G$ acts on L via

$$\left(\sum_{\sigma\in G} k_\sigma \lambda(\sigma)\right) \cdot x = \sum_{\sigma\in G} k_\sigma \sigma^{-1}(x),$$

we conclude that the canonical nonclassical structure is $(L[G]^G, \cdot)$, where G acts on G via conjugation, so that

$$L[G]^G = \left\{ \sum_{\tau\in G} \ell_\tau \tau \in L[G] \mid \sigma(\ell_\tau) = \ell_{\sigma\tau\sigma^{-1}} \text{ for all } \sigma, \tau \in G \right\},$$

and the action on L is given by

$$\left(\sum_{\sigma\in G} k_\sigma \sigma\right) \cdot x = \sum_{\sigma\in G} k_\sigma \sigma^{-1}(x).$$

The results developed in the previous section can be employed to describe the structures of these Hopf algebras. For example, the following result can be obtained.

Theorem 1.4.8. *Let L/K be a finite Galois extension with Galois group G, and let N be a regular subgroup of* $\mathrm{Perm}(G)$ *normalised by $\lambda(G)$. Then there exists a bijective correspondence between*

- *the subgroups of N normalised by $\lambda(G)$;*
- *the Hopf subalgebras of $L[N]^G$.*

This result appeared explicitly first in [CRV16a], but it was also implicitly used in [GP87, Theorem 5.3] to present the following interesting behaviour of the canonical nonclassical structure.

Theorem 1.4.9. *Let L/K be a finite Galois extension with Galois group G. Then the image of the Hopf–Galois correspondence for the canonical nonclassical structure on L/K consists exactly of the normal intermediate fields of L/K.*

As immediate corollary, one finds an instance of bijective Hopf–Galois correspondence. Recall that a group is *Hamiltonian* if it is not abelian and each of its subgroups is normal.

Corollary 1.4.10. *Let L/K be a finite Galois extension with Hamiltoninan Galois group G. Then the canonical nonclassical structure on L/K has a bijective Hopf–Galois correspondence.*

1.4.3 Byott's translation

As initially mentioned by Childs [Chi89] and then made precise by Byott [Byo96], there exists a way translate the Greither–Pareigis result in order to work in holomorphs of groups instead of more general permutation groups. This has the advantage that in general the holomorph is sensibly smaller than the full permutation group. Again, we state the result in the case of Galois extensions.

Definition 1.4.11. Let G and N be finite groups. A group homomorphism

$$\alpha\colon N \to \mathrm{Perm}(G)$$

is a *regular embedding* if α is injective and $\alpha(N)$ is a regular subgroup of $\mathrm{Perm}(G)$.

Note that given a regular embedding $\alpha\colon G \to \mathrm{Perm}(N)$, we can define the map

$$\alpha_*\colon N \to G, \quad \alpha_*(\eta) = \alpha(\eta)[1_G],$$

which is a bijection by definition of regular subgroups. The following result is contained in [Byo96, section 2]; see also the appendix of [SV18].

Theorem 1.4.12 (Byott's translation)**.** *Let G and N be finite groups of the same order. Then there exists a bijective correspondence between*

- *the regular embeddings $\alpha\colon N \to \mathrm{Perm}(G)$ such that $\alpha(N)$ is normalised by $\lambda(G)$;*
- *the regular embeddings $\beta\colon G \to \mathrm{Hol}(N)$.*

Specifically, a regular embedding $\alpha\colon N \to \mathrm{Perm}(G)$ such that $\alpha(N)$ is normalised by $\lambda(G)$ corresponds to the regular embedding

$$\beta\colon G \to \mathrm{Hol}(N), \quad \beta(\sigma) = \alpha_*^{-1}\lambda(\sigma)\alpha_*.$$

Conversely, a regular embedding $\beta\colon G \to \mathrm{Hol}(N)$ corresponds to the regular embedding

$$\alpha\colon N \to \mathrm{Perm}(G), \quad \alpha(\eta) = \beta_*^{-1}\lambda(\eta)\beta_*.$$

In particular, if L/K is a finite Galois extension with Galois group G and N is a group of the same order of G, then we can obtain a Hopf–Galois structure of type N starting from every regular subgroup of $\mathrm{Hol}(N)$ isomorphic to G. Explicitly, if T is such a subgroup, then the composition

$$\beta\colon G \to T \hookrightarrow \mathrm{Hol}(N)$$

is a regular embedding, so it yields a map

$$\alpha\colon N \to \mathrm{Perm}(G)$$

such that $\alpha(N)$ is a regular subgroup of $\mathrm{Perm}(G)$ normalised by $\lambda(G)$ and isomorphic to N. Via the Greither–Pareigis theory, we derive a Hopf–Galois structure of type N on L/K.

A main consequence of this result is a quantitative result that simplifies the problem of counting the Hopf–Galois structure of a given type on a Galois extension. Given finite groups N and G of the same order, we denote by $e(G,N)$ the number of Hopf–Galois structures of type N on a Galois extension with Galois group G, and by $f(G,N)$ the number of regular subgroups of $\mathrm{Hol}(N)$ isomorphic to G. Byott obtained the following result [Byo96, Corollary], which simplifies the task of finding the number of Hopf–Galois structures of a given type, as $\mathrm{Hol}(G)$ is smaller than $\mathrm{Perm}(G)$ and often easier to describe.

Corollary 1.4.13 (Byott)**.** *Let G and N be finite groups of the same order. Then the following equality holds:*

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

Chapter 2

Skew Braces

This chapter is devoted to skew braces, algebraic structures introduced by Guarnieri and Vendramin [GV17], building on previous work of Rump [Rum07a] and Cedó, Jespers, and Okniński [CJO14]. Skew braces have received particular attention lately due to their various connections with radical rings, regular subgroups of the holomorph, solutions of the Yang–Baxter equation, and Hopf–Galois structures. While our main goal in the thesis is to present a new version of the connection with Hopf–Galois structures, we try to give a more general description in this chapter, presenting new results related to (construction of) certain classes of skew braces and some structural properties. In the first section, we present some preliminaries, following mainly [CSV19, GV17, SV18]. After the first section, we state and prove some results contained in our papers [CS21, CS22, CS23, ST23a], sometimes adding a new point of view or some slight generalisations.

2.1 Preliminaries

2.1.1 First definitions and properties

Definition 2.1.1. A *skew (left) brace* is a triple $(A, +, \circ)$, where $(A, +)$ and $(A, \circ)$ are groups such that, for all $a, b, c \in A$,

$$a \circ (b + c) = (a \circ b) - a + (a \circ c).$$

Notation 2.1.2. In general, we denote a skew brace by the same symbol of the underlying set: when we say that A is a skew brace, we are tacitly meaning a skew brace $(A, +, \circ)$. The group $(A, +)$, which is not necessarily abelian, is called the *additive group* and written in additive notation; for example, $-a$ is the inverse and na is the nth power of a in $(A, +)$. Similarly, the group $(A, \circ)$ is called the *multiplicative group* and written in multiplicative notation; for example, a^{-1} is the inverse and a^n is the nth power of a in $(A, \circ)$.

By an easy application of the defining property, the identities of the groups $(A, +)$ and $(A, \circ)$ coincide; we may refer to this common element by 0 or 1, depending on the context.

As in what follows various different group structures on the same set may be considered, we specify the group structure when well-known notations concerning groups are used, in order to avoid confusion. For example, given a group $(A, \star)$, we write

- $Z(A, \star)$ for the centre;
- $[-, -]_\star$ for the commutator;
- $\langle - \rangle_\star$ for the subgroup generated by subsets or elements;
- $\mathrm{Aut}(A, \star)$ for the automorphism group, and $\mathrm{Inn}(A, \star) = \{\iota_\star(a) \mid a \in A\}$ for the subgroup of inner automorphisms, where $\iota_\star(a)$ denotes conjugation-by-a in $(A, \star)$.

Definition 2.1.3. A skew brace A is

- *trivial* if $a \circ b = a + b$ for all $a, b \in A$;
- *almost trivial* if $a \circ b = b + a$ for all $a, b \in A$.

This definition is motivated by the following example. Recall that, given a group $(A, +)$, we write $(A, +_{\mathrm{op}})$ for the *opposite group* of $(A, +)$, where

$$a +_{\mathrm{op}} b = b + a.$$

Example 2.1.4. Let $(A, +)$ be a group.

- The triple $(A, +, +)$ is a trivial skew brace, denoted by $\mathrm{Triv}(A)$ when the group operation of $(A, +)$ is understood. It is clear that all the trivial skew braces can be obtained in this way.
- The triple $(A, +, +_{\mathrm{op}})$ is an almost trivial skew brace. It is clear that all the almost trivial skew braces can be obtained in this way.

Definition 2.1.5. Given a class $\mathfrak{X}$ of groups, we say that a skew brace is of $\mathfrak{X}$ *type* if the additive group belongs to $\mathfrak{X}$.

Example 2.1.6. The skew braces of abelian type are exactly the *braces* in the sense of Rump [Rum07a]. The original definition was later reformulated in terms more similar to Definition 2.1.1 in [CJO14, Definition 1].

Definition 2.1.7. A skew brace A is *two-sided* if for all $a, b, c \in A$,

$$(a + b) \circ c = (a \circ c) - c + (b \circ c).$$

Example 2.1.8. A skew brace A such that $(A, \circ)$ is abelian is two-sided.

Example 2.1.9. Let R be a *radical ring*, that is, a ring that coincides with its Jacobson radical. By [Hun80, Chapter IX, Theorem 2.3], this is equivalent to asking that $(R, \circ)$ is a group, where

$$r \circ s = r + rs + s.$$

As showed in [Rum07a], the triple $(R, +, \circ)$ is a two-sided brace of abelian type, and every two-sided skew brace of abelian type arises in this way.

Definition 2.1.10. Let A and B be skew braces. A map $f\colon A \to B$ is a *skew brace homomorphism* if for all $a, b \in A$,

$$f(a + b) = f(a) + f(b), \qquad f(a \circ b) = f(a) \circ f(b).$$

The *kernel* of f is

$$\ker f = \{a \in A \mid f(a) = 0\}.$$

When $f\colon A \to B$ is bijective, we say that f is a *skew brace isomorphism*, or a *skew brace automorphism* of A when $B = A$. The automorphisms of a skew brace A form a group, which is denoted by $\mathrm{Aut}(A)$ or $\mathrm{Aut}(A, +, \circ)$.

Definition 2.1.11. Let A be a skew brace. A *subskew brace* B of A is a subset that is a subgroup of both $(A, +)$ and $(A, \circ)$.

Clearly, if B is a subskew brace of a skew brace A, then also $(B, +, \circ)$ is a skew brace, denoted again by B.

To define additional substructures, we need to consider a suitable map for skew braces, usually denoted by λ in the literature. Take a skew brace A, and for all $a \in A$, write

$$\gamma(a)\colon A \to A, \quad b \mapsto {}^{\gamma(a)}b = -a + (a \circ b).$$

The map γ obtained in this way is called the *gamma function* of A; as showed in [GV17, Proposition 1.9], this is a group homomorphism

$$\gamma\colon (A, \circ) \to \mathrm{Aut}(A, +).$$

It follows that given a skew brace A, for all $a, b \in A$,

$$a \circ b = a + {}^{\gamma(a)}b, \qquad a + b = a \circ {}^{\gamma(a^{-1})}b, \qquad a^{-1} = {}^{\gamma(a^{-1})}(-a).$$

These equalities are used without reference in the following.

Note that gamma functions can be used to construct or characterise skew braces, in the following way; see [CCDC20, Theorem 2.2].

Theorem 2.1.12. *Let $(A, +)$ be a group. Then there exists a bijective correspondence between*

- *the functions $\gamma\colon A \to \mathrm{Aut}(A, +)$ such that for all $a, b \in A$,*

$$\gamma(a + {}^{\gamma(a)}b) = \gamma(a)\gamma(b);$$

- *the operations* $\circ$ *such that* $(A, +, \circ)$ *is a skew brace.*

Specifically, a function γ *corresponds to the operation* $\circ$ *given by* $a \circ b = a + {}^{\gamma(a)}b$.

With the gamma functions, we can define some important substructures of skew braces.

Definition 2.1.13. Let A be a skew brace. A subskew brace I of A is

- a *left ideal* if ${}^{\gamma(a)}i \in I$ for all $a \in A$ and $i \in I$;
- a *strong left ideal* if I is a left ideal and is normal in $(A, +)$;
- an *ideal* if I is a strong left ideal and is normal in $(A, \circ)$.

Remark 2.1.14. It is clear that, by the definition of the function γ of a skew brace A, in order to define a left ideal B is enough to suppose that B is a subgroup of one of the group structures that is invariant under the action of $(A, \circ)$ via γ.

Note also that the ideals I are precisely the structures over which is possible to take quotients, as the definition implies that $a + I = a \circ I$ for all $a \in A$. In particular, it follows that the sets $(A, +)/(I, +)$ and $(A, \circ)/(I, \circ)$ are equal, and we obtain in this way a skew brace $(A/I, +, \circ)$, denoted again by A/I.

Example 2.1.15. As to be expected, the ideals are exactly the kernels of the skew brace homomorphisms:

- If A and B are skew braces and $f\colon A \to B$ is a skew brace homomorphism, then $\ker f$ is an ideal of A.
- If A is a skew brace and I is an ideal of A, then

$$\pi\colon A \to A/I, \quad a \mapsto \overline{a} = a + I = a \circ I$$

  is a skew brace homomorphism such that $\ker f = I$.

Remark 2.1.16. If I is a left ideal of a skew brace A, then we say that I is *trivial* if I is trivial as skew brace. The same idea works for all the notions introduced in the next subsection.

Remark 2.1.17. Mimicking the analogous proofs for groups, or employing the general description of universal algebra, one can easily derive that the isomorphism theorems hold for skew braces.

Example 2.1.18. Let A be a skew brace, and write

$$\mathrm{Fix}(A) = \{a \in A \mid {}^{\gamma(b)}a = a \text{ for all } b \in A\}.$$

Then $\mathrm{Fix}(A)$ is a left ideal of A; see Proposition [CSV19, Proposition 1.6].

Example 2.1.19. Let A be a skew brace. Define the *socle* of A as

$$\mathrm{Soc}(A) = \{a \in A \mid a + b = b + a = a \circ b \text{ for all } b \in A\}.$$

It is clear that

$$\mathrm{Soc}(A) = \ker \gamma \cap Z(A, +).$$

Then $\mathrm{Soc}(A)$ is an ideal of A; see [GV17, Lemma 2.5].

Example 2.1.20. Let A be a skew brace. Define the *annihilator* of A as

$$\mathrm{Ann}(A) = \{a \in A \mid a + b = b + a = a \circ b = b \circ a \text{ for all } b \in B\}.$$

It is clear that

$$\mathrm{Ann}(A) = \mathrm{Soc}(A) \cap Z(A, \circ).$$

The annihilator was introduced in [CCS19], where it is mentioned that $\mathrm{Ann}(A)$ is an ideal of A.

Motivated by the multiplication of radical rings, we can give the following definition.

Definition 2.1.21. Let A be a skew brace. The *star operation* of A is given by

$$a * b = -a + (a \circ b) - b = {}^{\gamma(a)}b - b.$$

The star operation of a skew brace A measures how far apart the operations are, as $a * b = 0$ if and only if $a + b = a \circ b$, and it coincides with the ring multiplication when A can be obtained by a radical ring. For all subsets X and Y of A, we write

$$X * Y = \langle x * y \mid x \in X \text{ and } y \in Y \rangle_+$$

and $A^2 = A * A$, so that $A^2 = 0$ if and only if A is trivial. More precisely, it is clear that A^2 is the smallest ideal of A such that A/A^2 is trivial; see [CSV19, Proposition 2.3].

On the model of groups, we can talk about direct and semidirect products of skew braces; for the second notion, we take the definition of [SV18, Corollary 2.36], but we remark that a more general concept appeared recently in [BFP23].

Definition 2.1.22. Let A and B be skew braces, and consider the set

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}.$$

- The *direct product* of A and B, denoted again by $A \times B$, is the skew brace $(A \times B, +, \circ)$, where

$$(a, b) + (a', b') = (a + a', b + b'), \qquad (a, b) \circ (a', b') = (a \circ a', b \circ b').$$

- Let $\alpha \colon (B, \circ) \to \mathrm{Aut}(A)$ be a group homomorphism. The *semidirect product* of A and B, denoted by $A \rtimes B$, is the skew brace $(A \times B, +, \circ)$, where

$$(a, b) + (a', b') = (a + a', b + b'), \qquad (a, b) \circ (a', b') = (a \circ \alpha_b(a'), b \circ b').$$

A routine calculation shows that indeed the (semi)direct product of skew braces is actually a skew brace. Note that the definition of direct product of skew brace can be easily extended to any finite number of skew braces, and the direct product of two skew braces is the semidirect product with respect to the trivial action. We also remark that the gamma function of the direct product A of skew braces A_i is given by the gamma functions of the skew braces A_i in the obvious way, so that if the skew braces A_i are finite and have coprime cardinality, then the left ideals of A are exactly the direct product of the left ideals of the A_i.

To conclude this part, we introduce opposite skew braces, following [KT20].

Definition 2.1.23. Let A be a skew brace. The *opposite skew brace* of A is the skew brace $(A, +_{\mathrm{op}}, \circ)$, denoted by A_{op}.

As showed in [KT20, Proposition 3.1], the opposite skew brace A_{op} of a skew brace A is actually a skew brace. In general, we use the subscript op to refer to typical notions of skew brace related to A_{op}. For example, the gamma function γ_{op} of A_{op} is given by

$$^{\gamma_{\mathrm{op}}(a)}b = -a +_{\mathrm{op}} (a \circ b) = (a \circ b) - a = a - a + (a \circ b) - a,$$

which means that $\gamma_{\mathrm{op}}(a) = \iota_+(a)\gamma(a)$. As immediate consequence, the strong left ideals of A are exactly the left ideals of A that are also left ideals of A_{op}.

Similarly,

$$a *_{\mathrm{op}} b = -b + (a \circ b) - a.$$

Example 2.1.24. Let $(A, +, +)$ be a trivial skew brace, so that $\gamma(a) = \mathrm{id}$ for all $a \in A$. Then the opposite skew brace $(A, +_{\mathrm{op}}, +)$ is an almost trivial skew brace. For all $a, b \in A$,

$$\gamma_{\mathrm{op}}(a) = \iota_+(a), \qquad a *_{\mathrm{op}} b = [-b, a]_+.$$

Note that $A = A_{\mathrm{op}}$ if and only if A is a skew brace of abelian type. The internal structures of A and A_{op} are strongly related, as the following result, whose proof is immediate, shows.

Proposition 2.1.25. *Let A be a skew brace. Then the ideals of A and A_{op} coincide.*

As an application, we find that $(A_{\mathrm{op}})^2$ is an ideal of A; explicitly,

$$(A_{\mathrm{op}})^2 = \langle a *_{\mathrm{op}} b \mid a, b \in A \rangle_+ \subseteq A.$$

To lighten the notation, we denote this ideal by A^2_{op}, without any risk of confusion as we never consider the opposite skew brace of A^2 in what follows. We also mention that A^2_{op} is the smallest ideal of A such that A/A^2_{op} is almost trivial.

2.1.2 Series for skew braces

We summarise here some known results related to notions of skew braces obtained via suitable series of substructures.

Definition 2.1.26. Let A be a skew brace. A *subideal series* (*ideal series*, respectively) $\{I_m\}_m$ of A is a chain of subskew braces

$$0 = I_{n+1} \subseteq I_n \subseteq \cdots \subseteq I_2 \subseteq I_1 = A$$

such that I_{m+1} is an ideal of I_m (of A, respectively) for all m.

Given a class $\mathfrak{X}$ of skew braces, we say that a (sub)ideal series is an $\mathfrak{X}$ series if the skew brace I_m/I_{m+1} belongs to $\mathfrak{X}$ for all m.

To construct some canonical examples of series, we take inspiration from ring theory, employing the star operation of a skew brace. However, as the star operation is not necessarily associative, in order to employ it to define, on the model of rings, subideal series, it is important to "pick a side".

The first notion we present appeared in [KSV21] under the name of solubility for skew brace. However, we reserve the term soluble for a more particular class of skew braces, introduced in [BBERJSPC23], which we consider below.

Definition 2.1.27. Let A be a skew brace. Define $A_1 = A$ and for all $m \geq 1$,

$$A_{m+1} = A_m * A_m.$$

We say that A is *polytrivial (of class n)* if there exists n such that $A_{n+1} = 0$ (and n is minimal with this property).

The fact that given a skew brace A, the ideal A^2 is the smallest such that A/A^2 is trivial, immediately shows that the series $\{A_m\}_m$ is a trivial subideal series of A and that the following result holds.

Proposition 2.1.28. *Let A be a skew brace. Then the following are equivalent:*

- *There exists a trivial subideal series of A.*
- *There exists n such that $A_n = 0$.*

This easily yields the following well-known result.

Lemma 2.1.29. *Let A be a skew brace, and let I be an ideal of A. Then A is polytrivial if and only if I and A/I are polytrivial.*

Definition 2.1.30. A skew brace A is *metatrivial* if A is polytrivial of class at most two.

It is clear that a skew brace A is metatrivial if and only if A^2 is trivial, if and only if there exists an ideal I such that A/I and I are trivial skew braces.

We list now some classes of polytrivial skew braces. The first two were introduced in [CSV19].

Definition 2.1.31. Let A be a skew brace. Define $A^{(1)} = A$ and for all $n \geq 1$,

$$A^{(m+1)} = A^{(m)} * A.$$

We say that A is *right nilpotent (of class n)* if there exists n such that $A^{(n+1)} = 0$ (and n is minimal with this property).

As shown in [CSV19, Proposition 2.1], the series of the $\{A^{(n)}\}_n$ is a trivial ideal series of a skew brace A. The following result is a consequence of [CSV19, Lemma 2.5].

Lemma 2.1.32. *Let A be a skew brace, and let I be an ideal of A. Then for all $m \geq 1$,*

$$(A/I)^{(m)} = (A^{(m)} + I)/I.$$

Definition 2.1.33. Let A be a skew brace. Define $A^1 = A$ and for all $n \geq 1$,

$$A^{m+1} = A * A^m.$$

We say that A is *left nilpotent (of class n)* if there exists n such that $A^{n+1} = 0$ (and n is minimal with this property).

As showed in [CSV19, Proposition 2.2], the series of the $\{A^n\}_n$ is a trivial subideal series of a skew brace A. The following result is a consequence of [CSV19, Lemma 2.23].

Lemma 2.1.34. *Let A be a left nilpotent skew brace, and let I be an ideal of A. Then A/I is left nilpotent.*

Example 2.1.35. Let A be a skew brace with cardinality p^n, where p is a prime. Then A is left nilpotent of class at most n; see [Rum07a, Corollary of Proposition 8] and [CSV19, Proposition 4.4].

Given a skew brace A, an easy induction shows that A_m is contained in $A^{(m)}$ and A^m for all $m \geq 1$. In particular, skew braces that are left or right nilpotent of class at most n are also polytrivial of class at most n.

The following result is [CSV19, Theorem 4.8].

Theorem 2.1.36. *Let A be a finite skew brace of nilpotent type. Then A is left nilpotent if and only if $(A, \circ)$ is nilpotent.*

Example 2.1.37. Let R be a radical ring. Then $r * s = rs$ is the ring multiplication, so that R, viewed as a skew brace, is right nilpotent or left nilpotent if and only if R is a nilpotent ring.

The notions introduced so far are in some sense modelled on nilpotency of rings. In [BJ23], Bonatto and Jedlicka employed the perspective of universal algebra to define commutators in the context of skew braces, with the aim to mimic concepts typical of groups in this setting. The result was later generalised by Bourn, Facchini, and Pompili [BFP23], via the point of view of semiabelian categories.

Definition 2.1.38. Let A be a skew brace, and let I, J be ideals of A. The *commutator* $[I, J]$ of I and J is the smallest ideal of A containing

$$[I, J]_+,\ [I, J]_\circ,\ I * J.$$

Note that if A is a skew brace, then $[A, A] = 0$ if and only if A is a trivial skew brace of abelian type. This motivates the following definition.

Definition 2.1.39. A skew brace A is *abelian* if A is a trivial skew brace of abelian type.

By construction, therefore, we derive that $[A, A]$ is the smallest ideal of a skew brace A such that $A/[A, A]$ is abelian. It is quite easy to check that

$$[A, A] = \langle [A, A],\ A * A\rangle_+.$$

Once this commutator is defined, we have natural notions of solubility and nilpotency. The first appeared in [BBERJSPC23], while the second in [BJ23].

Definition 2.1.40. Let A be a skew brace. Define $\partial^1(A) = A$ and for all $n \geq 1$,

$$\partial^{m+1}(A) = [\partial^m(A), \partial^m(A)].$$

We say that A is *soluble (of class n)* if there exists n such that $\partial^{n+1}(A) = 0$ (and n is minimal with this property).

The fact that given a skew brace A, the ideal $[A, A]$ is the smallest such that $A/[A, A]$ is abelian, immediately shows that the series $\{\partial^m(A)\}_m$ is an abelian ideal series of A and that the following result holds.

Proposition 2.1.41. *Let A be a skew brace. Then the following are equivalent:*

- *There exists an abelian ideal series of A.*
- *There exists n such that $\partial^n(A) = 0$.*

Note that, in particular, if a skew brace A is soluble, then also $(A, +)$ and $(A, \circ)$ are soluble.

Definition 2.1.42. A skew brace A is *metabelian* if A is soluble of class at most two.

It is clear that a skew brace A is metabelian if and only if $[A, A]$ is abelian, if and only if there exists an ideal I such that A/I and I are abelian skew braces.

Finally, we can deal also with a different notion of nilpotency for skew braces.

Definition 2.1.43. Let A be a skew brace. Define $\Gamma_1(A) = A$ and for all $m \geq 2$,

$$\Gamma_{m+1}(A) = [\Gamma_m(A), A].$$

We say that A is *nilpotent (of class n)* if there exists n such that $\Gamma_{n+1}(A) = 0$ (and n is minimal with this property).

This notion was introduced in [BJ23] under the name of central nilpotency, and later in [JVAV23] under the name of annihilator nilpotency, because of its relation with the annihilator of a skew brace [BJ23, Theorem 2.7]. An easy induction shows that given a skew brace A, there is an inclusion $\partial_m(A) \subseteq \Gamma_m(A)$, so that if A is nilpotent of class at most n, then A is soluble of class at most n.

The following result relates various notions of nilpotency; see [BJ23, Corollary 2.9] and [JVAV23, Corollary 2.15].

Theorem 2.1.44. *Let A be a skew brace. Then the following are equivalent:*

- *A is nilpotent.*
- *A is left and right nilpotent of nilpotent type.*

If this is the case, then also $(A, \circ)$ is nilpotent.

Example 2.1.45. Let A be a trivial skew brace. Then $A * A = 0$ and $[A, A] = [A, A]_+$, so that A is

- polytrivial, left nilpotent, and right nilpotent of class at most one;
- soluble (respectively nilpotent) of class n if and only if $(A, +)$ is soluble (respectively nilpotent) of class n.

Example 2.1.46. Let A be an almost trivial skew brace. Then $A * A = [A, A]_+ = [A, A]$, so that A is

- polytrivial of class n if and only if A is soluble of class n, if and only if $(A, +)$ is soluble of class n;
- right nilpotent of class n if and only if A is left nilpotent of class n, if and only if A is nilpotent of class n, if and only if $(A, +)$ is nilpotent of class n.

2.1.3 Skew braces and the Yang–Baxter equation

The interest in set-theoretic solutions of the Yang–Baxter equation, as a simplification of its linear solutions, goes back to Drinfel'd [Dri92]. Compared to the linear version, set-theoretic solutions are easier to study and classify. Nonetheless, set-theoretic solutions can be linearised and are also omnipresent in the study of link and knot invariants. Here we quickly review the well-known connection between skew braces and the Yang–Baxter equation.

Definition 2.1.47. A *set-theoretic solution of the Yang–Baxter equation* is a pair (X, r), where X is a nonempty set and $r\colon X \times X \to X \times X$ a bijective map that satisfies

$$(r \times \mathrm{id}_X)(\mathrm{id}_X \times r)(r \times \mathrm{id}_X) = (\mathrm{id}_X \times r)(r \times \mathrm{id}_X)(\mathrm{id}_X \times r).$$

The solution (X, r) is *nondegenerate* if for all $x \in X$, the maps $\sigma_x, \tau_x\colon X \to X$ defined by $r(x, y) = (\sigma_x(y), \tau_y(x))$ are bijective.

As customary, we shortly refer to a nondegenerate set-theoretic solution of the Yang–Baxter equation as a *solution*.

Definition 2.1.48. Let (X, r) and (Y, s) be solutions. A *solution homomorphism* $f\colon (X, r) \to (Y, s)$ is a map $f\colon X \to Y$ such that $(f \times f)r = s(f \times f)$.

Given a solution (X, r), it is easily checked that also (X, r^{-1}) is again a solution. For all $x \in X$, we define $\hat{\sigma}_x, \hat{\tau}_x\colon X \to X$ by $r^{-1}(x, y) = (\hat{\sigma}_x(y), \hat{\tau}_y(x))$.

The following definition was introduced in [ESS99].

Definition 2.1.49. Let (X, r) be a solution. The *structure group* of (X, r) is the group

$$(G(X, r), \circ) = \langle X \mid x \circ y = \sigma_x(y) \circ \tau_y(x) \text{ for all } x, y \in X \rangle.$$

There are two main ways to relate skew braces and solutions. We present here two theorems that combine many fundamental results in the literature and are used freely later. Most of the first result is due to Guarnieri and Vendramim [GV17, Theorem 3.1], as generalisation of previous work of Rump [Rum07a]; the part on opposite skew brace is [KT20, Theorem 4.1].

Theorem 2.1.50. *Let A be a skew brace. Then (A, r_A) is a solution, where*

$$r(a, b) = ({}^{\gamma(a)}b, ({}^{\gamma(a)}b)^{-1} \circ a \circ b),$$

with inverse solution $(A_{\mathrm{op}}, r_{A_{\mathrm{op}}})$. In addition, every skew brace homomorphism $f\colon A \to B$ induces a solution homomorphism $f\colon (A, r_A) \to (B, r_B)$.

For the second, we refer to [GV17] and the recent survey [Ven23].

Theorem 2.1.51. *Let (X, r) be a solution. Then there exists an operation $+$ such that $(G(X, r), +, \circ)$ is a skew brace, denoted by $G(X, r)$, with the following properties:*

- *The map*
$$\iota\colon (X, r) \to (G(X, r), r_{G(X,r)}), \quad x \to x$$
is a solution homomorphism.
- *Both the additive and multiplicative group of $G(X, r)$ are generated by $\iota(X)$.*

Definition 2.1.52. A solution is *injective* if ι is an injective map.

Example 2.1.53. If (X, r) is a solution, then $(\iota(X), r)$ is a solution, where

$$r(\iota(x), \iota(y)) = (\iota \times \iota)r(x, y).$$

In addition, the skew braces $G(X, r)$ and $G(\iota(X), r)$ are isomorphic, so that $(\iota(X), r)$ is injective; see [LV19, Proposition 7.6].

2.2 Homomorphic skew braces and bi-skew braces

In this section we propose a systematic analysis of two related classes of skew braces, following the discussion of paper [ST23a].

2.2.1 Some structural results

The first class was introduced under a slightly different name in [BNY22].

Definition 2.2.1. A skew brace A is *homomorphic* if $\gamma\colon (A,+) \to \mathrm{Aut}(A,+)$ is a group homomorphism.

We begin by showing a characterisation of these skew braces in term of nilpotency; see [ST23a, Theorem 3.13].

Theorem 2.2.2. *Let A be a skew brace. Then the following are equivalent:*

- *A is homomorphic.*
- *$\gamma(a+b) = \gamma(a \circ b)$ for all $a, b \in A$.*
- *$\gamma({}^{\gamma(a)}b) = \gamma(b)$ for all $a, b \in A$.*
- *A^2 is contained in $\ker\gamma$.*

Proof. Let $a, b \in A$. The equality

$$\gamma(a \circ b) = \gamma(a)\gamma(b)$$

implies that A is homomorphic if and only if $\gamma(a+b) = \gamma(a \circ b)$.

Suppose that A is homomorphic. Then

$$\gamma(a)\gamma(b) = \gamma(a \circ b) = \gamma(a + {}^{\gamma(a)}b) = \gamma(a)\gamma({}^{\gamma(a)}b),$$

that is, $\gamma({}^{\gamma(a)}b) = \gamma(b)$. In addition,

$$\gamma(a * b) = \gamma(a)^{-1}\gamma(a)\gamma(b)\gamma(b)^{-1} = 1,$$

that is, $A^2 \subseteq \ker\gamma$.

Conversely, suppose first that $\gamma({}^{\gamma(a^{-1})}b) = \gamma(b)$. Then

$$\gamma(a+b) = \gamma(a \circ {}^{\gamma(a^{-1})}b) = \gamma(a)\gamma({}^{\gamma(a^{-1})}b) = \gamma(a)\gamma(b).$$

Suppose now that $\ker\gamma$ contains A^2. As A/A^2 is a trivial skew brace, we obtain $(a+b) \in (a \circ b) \circ A^2$, meaning that there exists $c \in A^2$ such that $a + b = a \circ b \circ c$. We derive

$$\gamma(a+b) = \gamma(a \circ b \circ c) = \gamma(a)\gamma(b)\gamma(c) = \gamma(a)\gamma(b). \qquad \square$$

Remark 2.2.3. Let A be a skew brace. Then $A^2 \subseteq \ker\gamma$ if and only if $A^{(3)} = 0$. This means that the homomorphic skew braces are exactly the right nilpotent skew braces of class at most two. As a consequence, homomorphic skew braces are metatrivial, as already shown in [BNY22, Theorem 2.12].

Note also the following easy fact.

Lemma 2.2.4. *Let A be a homomorphic skew brace. Then $\ker\gamma$ is an ideal of A and $A/\ker\gamma$ is a trivial skew brace.*

Proof. The first claim follows from the fact that

$$\gamma\colon A \to \mathrm{Triv}(\mathrm{Aut}(A,+))$$

is a skew brace homomorphism. The second from the fact that $A^2 \subseteq \ker\gamma$. □

The second class of skew braces we consider was introduced by Childs [Chi19].

Definition 2.2.5. A skew brace A is a *bi-skew brace* if also $(A,\circ,+)$ is a skew brace.

While at first sight the two classes are defined in ways that do not appear similar, in [Car20, Theorem 3.1], Caranti showed the following result, giving the first analogy between bi-skew braces and homomorphic skew braces.

Theorem 2.2.6. *Let A be a skew brace. Then A is a bi-skew brace if and only*

$$\gamma\colon (A,+) \to \mathrm{Aut}(A,+)$$

is a group antihomomorphism.

As a consequence, we can derive the analogous theorem of Theorem 2.2.2; see [ST23a, Theorem 2.6].

Theorem 2.2.7. *Let A be a skew brace. Then the following are equivalent:*

- *A is a bi-skew brace.*
- *$\gamma(a+b) = \gamma(b\circ a)$ for all $a,b\in A$.*
- *$\gamma({}^{\gamma_{\mathrm{op}}(a)}b) = \gamma(b)$ for all $a,b\in A$.*
- *A^2_{op} is contained in $\ker\gamma$.*

Proof. Let $a,b\in A$. The equality

$$\gamma(a\circ b) = \gamma(a)\gamma(b)$$

implies that A is a bi-skew brace if and only if $\gamma(a+b) = \gamma(b\circ a)$.

Suppose that A is a bi-skew brace. Then

$$\gamma(a)\gamma(b) = \gamma(a\circ b) = \gamma(a+{}^{\gamma(a)}b) = \gamma({}^{\gamma(a)}b)\gamma(a),$$

that is, $\gamma({}^{\gamma_{\mathrm{op}}(a)}b) = \gamma(a)^{-1}\gamma({}^{\gamma(a)}b)\gamma(a) = \gamma(b)$. In addition,

$$\gamma(a *_{\mathrm{op}} b) = \gamma(a)^{-1}\gamma(a)\gamma(b)\gamma(b)^{-1} = 1,$$

that is, $A^2_{\mathrm{op}} \subseteq \ker\gamma$.

Conversely, suppose first that $\gamma({}^{\gamma_{\mathrm{op}}(a^{-1})}b) = \gamma(b)$. Then

$$\gamma(b+a) = \gamma(a +_{\mathrm{op}} b) = \gamma(a \circ {}^{\gamma_{\mathrm{op}}(a^{-1})}b) = \gamma(a)\gamma({}^{\gamma_{\mathrm{op}}(a^{-1})}b) = \gamma(a)\gamma(b).$$

Suppose now that $\ker\gamma$ contains A^2_{op}. As A/A^2_{op} is an almost trivial skew brace, we obtain $(a+b) \in (b \circ a) \circ A^2$, meaning that there exists $c \in A^2$ such that $a + b = b \circ a \circ c$. The assumption then implies

$$\gamma(a+b) = \gamma(b \circ a \circ c) = \gamma(b)\gamma(a)\gamma(c) = \gamma(b)\gamma(a). \qquad \square$$

As a slight variation of the analogous result for homomorphic skew braces, we obtain the following result.

Lemma 2.2.8. *Let A be a bi-skew brace. Then $\ker\gamma$ is an ideal of A and $A/\ker\gamma$ is an almost trivial skew brace.*

Proof. The first claim follows from the fact that

$$\gamma\colon A \to \mathrm{Triv}(\mathrm{Aut}(A,+))_{\mathrm{op}}$$

is a skew brace homomorphism. The second from the fact that $A^2_{\mathrm{op}} \subseteq \ker\gamma$. $\square$

The connection between the two classes is evident from these formulations, and the following result can be easily derived; see also [Car20, Lemma 3.7].

Lemma 2.2.9. *Let A be a skew brace. Then any two of the following statements imply the third:*

- *A is homomorphic.*
- *A is a bi-skew brace.*
- *$\gamma(A)$ is abelian.*

Remark 2.2.10. Note that in the case that A is a homomorphic skew brace or a bi-skew brace, then $\gamma(A)$ is abelian if one of $(A,+)$ and $(A,\circ)$ is abelian.

Example 2.2.11. Trivial skew braces and almost trivial skew braces are homomorphic bi-skew braces.

Example 2.2.12. Recall that every radical ring can be thought of as a skew brace of abelian type. As the star operation of R coincides with the ring multiplication, we can apply Theorem 2.2.2 (or better, Remark 2.2.3) to deduce that R is homomorphic (or equivalently a bi-skew brace) if and only if $R^3 = 0$. This generalises [Chi19, Proposition 4.1], in which R is assumed to be finite.

In the last section of this chapter we propose various examples of these classes of skew braces. We focus now on some of their structural properties. First, while homomorphic skew braces are always right nilpotent, the same does not hold for bi-skew braces. This can be easily controlled by the nilpotency of a suitable group; see [ST23a, Theorem 3.6].

Theorem 2.2.13. *Let $A \neq 0$ be a bi-skew brace. Then A is right nilpotent of class n if and only if $\gamma(A)$ is a nilpotent group of class $n-1$.*

Proof. By Lemma 2.1.32, for all $m \geq 2$,

$$(A/\ker\gamma)^{(m)} = (A^{(m)} + \ker\gamma)/\ker\gamma,$$

so that $(A/\ker\gamma)^{(n)} = 0$ if and only if $A^{(n)} \subseteq \ker\gamma$, which is equivalent to $A^{(n+1)} = 0$. We obtain that A is right nilpotent of class n if and only if $A/\ker(\gamma)$ is right nilpotent of class $n-1$, in the case $A \neq 0$.

Now, the almost trivial skew brace $A/\ker(\gamma)$ is right nilpotent of class n if and only if the group $(A/\ker(\gamma), \circ)$ is nilpotent of class n, and $(A/\ker(\gamma), \circ)$ is clearly isomorphic to $\gamma(A)$. □

We state now two corollaries; see [ST23a, Corollaries 3.7 and 3.8].

Corollary 2.2.14. *Let A be a bi-skew brace such that one of $(A,+)$ and $(A,\circ)$ is nilpotent. Then A is right nilpotent.*

Proof. It suffices to note that $\gamma(A)$ is a quotient of both $(A,+)$ and $(A,\circ)$, and then to apply Theorem 2.2.13. □

Corollary 2.2.15. *Let A be a left nilpotent bi-skew brace. Then A is right nilpotent.*

Proof. If A is left nilpotent, then also the skew brace $A/\ker\gamma$ is left nilpotent by Lemma 2.1.34. As $A/\ker\gamma$ is almost trivial, this is equivalent to the group $(A/\ker\gamma, \circ) \cong \gamma(A)$ being nilpotent. The result then follows from Theorem 2.2.13. □

In a similar way, the same group controls the polytriviality of a bi-skew brace; see [ST23a, Proposition 3.9].

Proposition 2.2.16. *Let A be a bi-skew brace. Then A is a polytrivial skew brace if and only if $\gamma(A)$ is a soluble group.*

Proof. We apply Lemma 2.1.29 with $I = \ker\gamma$, which is a trivial ideal such that $A/\ker\gamma$ is almost trivial by Lemma 2.2.8. In particular, the quotient $A/\ker(\gamma)$ is polytrivial if and only if the group $(A/\ker(\gamma), \circ)$ is soluble. We conclude again via the group isomorphism $(A/\ker(\gamma), \circ) \cong \gamma(A)$. □

We deal with the categorical notions of solubility and nilpotency. First, we present a generalisation of [ST23a]. In order to do this, we need a technical lemma, which gives a result of transitivity regarding solubility for skew braces.

Lemma 2.2.17. *Let A be a skew brace, and let I be an ideal of A. If I is a trivial skew brace of soluble type and A/I is soluble, then A is soluble.*

Proof. As A/I is soluble, we can employ an abelian series of A/I to obtain a series of ideals

$$I = B_{n+1} \subseteq B_n \subseteq \cdots \subseteq B_2 \subseteq B_1 = A$$

of A such that B_m/B_{m+1} is abelian for all m. Take now the derived series $\{I_m\}_m$ of the group $(I,+) = (I,\circ)$, in the usual group-theoretic sense. Every I_m defined in this way is characteristic in $(I,+) = (I,\circ)$, which is normal in both $(A,+)$ and $(A,\circ)$, hence I_i is also normal in both. Moreover, for all $a \in A$, the function $\gamma(a)$, when restricted to I, yields an automorphism of I, and hence every I_n is an ideal of A with the property that I_m/I_{m+1} is abelian. We conclude that

$$0 = I_{n'+1} \subseteq I_{n'} \subseteq \cdots \subseteq I_2 \subseteq I \subseteq B_n \subseteq \cdots \subseteq B_2 \subseteq B_1 = A$$

is an abelian series for A. □

Theorem 2.2.18. *Let A be a skew brace that is homomorphic or a bi-skew brace. Then the following are equivalent:*

- *A is a soluble skew brace.*
- *$(A,+)$ is a soluble group.*
- *$(A,\circ)$ is a soluble group.*

Proof. Clearly, if A is soluble, then also $(A,+)$ and $(A,\circ)$ are soluble.

Conversely, suppose that $(A,+)$ or $(A,\circ)$ is soluble. By Lemma 2.2.4 or Lemma 2.2.8, the skew brace $A/\ker\gamma$ is trivial or almost trivial (and thus soluble) and $\ker\gamma$ is a trivial ideal. Therefore we can conclude by applying Lemma 2.2.17. □

Remark 2.2.19. In particular, Theorem 2.2.18 implies that homomorphic skew braces and bi-skew braces satisfy Byott's conjecture; see [Byo15], [Ven19, Problem 2.46], and [ST23a, Theorem 3.11].

Remark 2.2.20. In section 2.5, we propose various constructions of skew braces $(A,+,\circ)$ that are both homomorphic skew braces and bi-skew braces, starting from a group $(A,+)$. In particular, every time we start from a soluble group, we always obtain soluble skew braces from these constructions.

A similar, but weaker, result can be derived for nilpotency

Theorem 2.2.21. *Let A be a skew brace that is homomorphic or a bi-skew brace. Suppose that A is finite. Then the following are equivalent:*

- *A is a nilpotent skew brace.*
- *$(A,+)$ and $(A,\circ)$ are nilpotent groups.*

Proof. If A is nilpotent, then also $(A,+)$ and $(A,\circ)$ are nilpotent by Theorem 2.1.44.

Conversely, if $(A,+)$ and $(A,\circ)$ are nilpotent and A is finite, then A is left nilpotent by Theorem 2.1.36, so right nilpotent by Corollary 2.2.15 in the bi-skew brace case (or by Theorem 2.2.2 and Remark 2.2.3 in the case of homomorphic skew braces). We conclude that A is nilpotent again by Theorem 2.1.44. □

We conclude these analogies by showing that one can use the semidirect product of skew braces to obtain two slightly different known constructions, one yielding homomorphic skew braces and one yielding bi-skew braces; see [ST23a, Examples 3.17 and 3.18].

Example 2.2.22. Let G and T be groups, and let T act by automorphisms on G, via an action denoted by α. This yields a group homomorphism

$$\alpha\colon (B,\circ) \to \mathrm{Aut}(A), \quad t \mapsto \alpha_t,$$

where $A = \mathrm{Triv}(G)$ and $B = \mathrm{Triv}(T)$. We obtain a skew brace $A \rtimes B$, with

$$\begin{aligned}(g,t) + (g',t') &= (gg',tt'),\\ (g,t) \circ (g',t') &= (g\alpha_t(g'),tt').\end{aligned}$$

We have recovered in this way [GV17, Example 1.4]. Note that for the skew brace $A \rtimes B$,

$$\gamma(g,t) = (\alpha_t, \mathrm{id}).$$

In particular, $A \rtimes B$ is a homomorphic skew brace, and it is a bi-skew brace if and only if $[T,T] \subseteq \ker\alpha$, as an immediate computation shows.

Example 2.2.23. Let G and T be groups, and let T act by automorphisms on G, via an action denoted by α. This yields a group homomorphism

$$\alpha\colon (B,\circ) \to \mathrm{Aut}(A),$$

where $A = \mathrm{Triv}(G)$ and $B = \mathrm{Triv}(T)_{\mathrm{op}}$. We obtain a skew brace $A \rtimes B$, with

$$\begin{aligned}(g,t) + (g',t') &= (gg',t't),\\ (g,t) \circ (g',t') &= (g\alpha_t(g'),tt').\end{aligned}$$

We have recovered in this way [Chi19, Proposition 7.1]. Note that for the skew brace $A \rtimes B$,

$$\gamma(g,t) = (\alpha_t, \iota(t)),$$

where $\iota(t)$ denotes conjugation-by-t in T. In particular, $A \rtimes B$ is a bi-skew brace, and it is homomorphic if and only if $[T,T] \subseteq \ker(\alpha) \cap Z(T)$. Note that when T is abelian, this construction coincides with the one in Example 2.2.22.

2.2.2 Two skew braces in a bi-skew brace

Let A be a bi-skew brace. We use the symbol $A_{\leftrightarrow}$ to denote the skew brace $(A,\circ,+)$, and we use the same subscript to denote skew brace notions related to the skew brace $A_{\leftrightarrow}$. For example, the gamma function $\gamma_{\leftrightarrow}$ of $A_{\leftrightarrow}$ is given by

$${}^{\gamma_{\leftrightarrow}(a)}b = a^{-1} \circ (a+b) = -(a^{-1}) + (a^{-1} \circ b),$$

meaning that $\gamma_{\leftrightarrow}(a) = \gamma(a)^{-1} = \gamma(a^{-1})$. We see here that the skew braces A and $A_{\leftrightarrow}$ share various properties. For the next result, see [ST23a, Lemma 3.1].

Lemma 2.2.24. *Let A be a bi-skew brace. Then the (left) ideals of A and $A_{\leftrightarrow}$ coincide.*

Proof. Let I be a subskew brace of A (and thus also of $A_{\leftrightarrow}$). As $\gamma_{\leftrightarrow}(a) = \gamma(a)^{-1} = \gamma(a^{-1})$, it is clear that ${}^{\gamma(a)}i \in I$ for all $a \in A$ and $i \in I$ if and only if ${}^{\gamma_{\leftrightarrow}(b)}i \in I$ for all $b \in A$ and $i \in I$. We derive that I is a left ideal of A if and only if I is a left ideal of $A_{\leftrightarrow}$, and I is an ideal of both A and A_{op} when I is also a normal subgroup of both $(A, +)$ and $(A, \circ)$. □

Lemma 2.2.25. *Let A be a bi-skew brace, and let I be a subskew brace of A. Then $A * I = A *_{\leftrightarrow} I$. If furthermore I is an ideal, then $I * A = I *_{\leftrightarrow} A$.*

Proof. Suppose that I is a subskew brace of A. Take $a \in A$ and $i \in I$. We note that

$$a^{-1} *_{\leftrightarrow} i = {}^{\gamma_{\leftrightarrow}(a^{-1})}i \circ i^{-1} = {}^{\gamma(a)}i \circ i^{-1},$$

from which we derive that

$$\begin{aligned} a * i = {}^{\gamma(a)}i - i &= ({}^{\gamma(a)}i \circ i^{-1} \circ i) - i \\ &= ({}^{\gamma(a)}i \circ i^{-1}) + {}^{\gamma({}^{\gamma(a)}i \circ i^{-1})}i - i \\ &= (a^{-1} *_{\leftrightarrow} i) + ((a^{-1} *_{\leftrightarrow} i) * i). \end{aligned}$$

Hence $a^{-1} *_{\leftrightarrow} i = (a * i) - ((a^{-1} *_{\leftrightarrow} i) * i) \in A * I$, and thus $A *_{\leftrightarrow} I \subseteq A * I$. By a symmetric argument, we also obtain $A * I \subseteq A *_{\leftrightarrow} I$.

Suppose now that I is also an ideal. As I is also in ideal of $A_{\leftrightarrow}$ by Lemma 2.2.24, we derive

$$(i^{-1} *_{\leftrightarrow} a) * a \in (I *_{\leftrightarrow} A) * A \subseteq I * A,$$

which implies, with the same argument as before but swapping the role of a and i, that $i^{-1} *_{\leftrightarrow} a \in I * A$. Again by a symmetric argument, the results follows. □

As a consequence, we derive the following theorem, which completes [ST23a, Propositions 3.3 and 3.4].

Theorem 2.2.26. *Let A be a bi-skew brace. Then A is $\star$ of class n if and only if $A_{\leftrightarrow}$ is $\star$ of class n. Here $\star$ is one of the following: polytrivial; left nilpotent; right nilpotent; nilpotent; soluble.*

Proof. Lemmas 2.2.24 and Lemma 2.2.25 shows that the series defining the property $\star$ of A coincide with the series defining the property $\star$ of $A_{\leftrightarrow}$. □

2.2.3 Applications to the Yang–Baxter equation

The goal of this subsection is to explore the meaning of homomorphic skew braces and bi-skew braces in relation to solutions of the Yang–Baxter equation. We follow here [ST23a, section 5].

As consequences of the description of these classes of skew braces via the gamma function, we immediately see that the information for a skew brace to

be bi-skew or homomorphic is not lost in the associated solution. Recall that given a solution (X, r), we write

$$r(x, y) = (\sigma_x(y), \tau_y(x))$$

for all $x, y \in X$.

Proposition 2.2.27. *Let A be a skew brace.*

- *A is homomorphic if and only if the solution (A, r_A) satisfies, for all $a, b \in A$,*
$$\sigma_{\sigma_a(b)} = \sigma_b.$$
- *A is a bi-skew brace if and only if the solution (A, r_A) satisfies, for all $a, b \in A$,*
$$\sigma_{\hat{\sigma}_a(b)} = \sigma_b.$$

Proof. The result follows by applying the characterisations presented in Theorems 2.2.2 and 2.2.7, together with the fact that for all $a, b \in A$,

$$\sigma_a(b) = {}^{\gamma(a)}b, \qquad \hat{\sigma}_a(b) = {}^{\gamma_{\mathrm{op}}(a)}b. \qquad \square$$

We approach now the opposite situation, characterising the solutions (X, r) such that $G(X, r)$ is a homomorphic skew brace or a bi-skew brace, under the additional assumption that (X, r) is injective. In [ST23a, Theorem 5.4], the result is given and proved in the context of bi-skew braces. For completeness, we state also the result in the context of homomorphic skew braces. We just provide the proof in this case, as it is a slight modification of the proof of [ST23a, Theorem 5.4].

Theorem 2.2.28. *Let (X, r) be an injective solution.*

- *The skew brace $G(X, r)$ is homomorphic if and only if $\sigma_{\sigma_x(y)} = \sigma_y$ for all $x, y \in X$.*
- *The skew brace $G(X, r)$ is a bi-skew brace if and only if $\sigma_{\hat{\sigma}_x(y)} = \sigma_y$ for all $x, y \in X$.*

Proof. As mentioned, we just prove the first claim. The implication from left to right is a consequence of the fact that (X, r) is injective and Proposition 2.2.27.

Now assume that for all $x, y \in X$, we have that $\sigma_{\sigma_x(y)} = \sigma_y$. Write $G = G(X, r)$. As the map

$$i \colon (X, r) \hookrightarrow (G, r_G), \quad x \mapsto x$$

is a solution homomorphism, we obtain that for all $x, y \in X$, considered as generators of G,

$$\gamma({}^{\gamma(x)}y) = \gamma(y).$$

In particular, as X generates the multiplicative group $(G, \circ)$, it follows that

$$\gamma({}^{\gamma(g)}y) = \gamma(y).$$

for all $g \in G$. For a word

$$w = \epsilon_1 x_1 + \cdots + \epsilon_n x_n$$

with $x_i \in X$ and $\epsilon_i \in \{-1, 1\}$, we claim that

$$\gamma(w) = \gamma(x_1)^{\epsilon_1} \dots \gamma(x_n)^{\epsilon_n}.$$

As also $(G, +)$ is generated by X, this would prove that

$$\gamma \colon (G, +) \to \mathrm{Aut}(G, +)$$

is a group homomorphism, and therefore G is a homomorphic brace. We prove this claim by induction on n. For $n = 1$ and $\epsilon_1 = 1$ the statement is trivial. To also cover the case where $n = 1$ and $\epsilon_1 = -1$, we have to prove that $\gamma(-x) = \gamma(x)^{-1}$ for all $x \in X$. For this, writing $a = -x$, we note

$$\gamma(-x)^{-1} = \gamma(a)^{-1} = \gamma(a^{-1}) = \gamma\left({}^{\gamma(a^{-1})}(-a)\right) = \gamma\left({}^{\gamma(a^{-1})}(x)\right) = \gamma(x).$$

Now assume that the statement holds for words of length $n - 1$, and let

$$w = \epsilon_1 x_1 + \cdots + \epsilon_n x_n.$$

If we write $v = \epsilon_1 x_1 + \cdots + \epsilon_{n-1} x_{n-1}$, then

$$\begin{aligned}\gamma(w) = \gamma(v + \epsilon_n x_n) &= \gamma(v \circ {}^{\gamma(v^{-1})}(\epsilon_n x_n)) = \gamma(v)\gamma({}^{\gamma(v^{-1})}(\epsilon_n x_n)) \\ &= \gamma(x_1)^{\epsilon_1} \cdots \gamma(x_{n-1})^{\epsilon_{n-1}} \gamma({}^{\gamma(v^{-1})} x_n)^{\epsilon_n} \\ &= \gamma(x_1)^{\epsilon_1} \cdots \gamma(x_n)^{\epsilon_n}.\end{aligned}$$

□

Corollary 2.2.29. *Let (X, r) be a solution.*

- *If $\sigma_{\sigma_x(y)} = \sigma_y$ for all $x, y \in X$, then $G(X, r)$ is homomorphic.*
- *If $\sigma_{\hat{\sigma}_x(y)} = \sigma_y$ for all $x, y \in X$, then $G(X, r)$ is a bi-skew brace*

Proof. Apply Theorem 2.2.28 to the injective solution $(\iota(X), r)$. □

2.3 Skew braces with cyclic infinite multiplicative group

The main goal of this section, which is based on [ST23a, section 4], is to give a solution to [Ven19, Problem 2.27].

Notation 2.3.1. For all n, we denote by $\mathbb{Z}^n$ the direct product of n copies of the additive group of integers $\mathbb{Z}$, the free abelian group of rank n, and by $\mathbb{Z}/n\mathbb{Z}$ (or by C_n) the cyclic group of order n.

Problem 2.3.2. Classify isomorphism classes of skew left braces with multiplicative group isomorphic to $\mathbb{Z}$.

While this section concerns infinite skew braces, and thus is not directly connected to Hopf–Galois structures, it still finds its place after the previous section, as the resolution of the problem depends on the fact that a suitable skew brace is a bi-skew brace.

First, when the skew braces in questions are of abelian type, the result is known by [CSV19, Theorem 5.5].

Theorem 2.3.3. *Let A be a skew brace of abelian type with multiplicative group isomorphic to $\mathbb{Z}$. Then A is a trivial skew brace.*

Actually, we can see how this result is part of a more general behaviour. The next result is [ST23a, Proposition 4.2].

Theorem 2.3.4. *Let A be a skew brace of abelian type with multiplicative group isomorphic to $\mathbb{Z}^n$. Then also the additive group of A is isomorphic to $\mathbb{Z}^n$, and A is right nilpotent of class at most n.*

Proof. Note that A is also a radical ring, whose multiplication is the star operation. In particular, as $(A, \circ)$ is finitely generated abelian, we can apply [Wat68, Theorem 3], that in this setting states that also the abelian group $(A, +)$ is finitely generated. This forces the ranks of $(A, +)$ and $(A, \circ)$ to coincide, as showed in [AD95a, Theorem B]. We deduce that $(A, +)$ is finitely generated abelian of rank n. Let T be the (necessarily finite) torsion subgroup of $(A, +)$. As T is a characteristic subgroup of $(A, +)$, it is a left ideal of A, so also a finite subgroup of $(A, \circ)$, and thus T is trivial. It follows that $(A, +) \cong \mathbb{Z}^n$.

Now for a prime p, let $I_p \cong (p\mathbb{Z})^n$ be the characteristic subgroup of $(A, +)$ generated by all the p-powers of the elements of A, also an ideal of A. Then A/I_p has order p^n, and therefore A/I_p is left nilpotent of class at most n (as in Example 2.1.35). But A/I_p is a two-sided skew brace of abelian type, so the star operation, being the multiplication of a ring, is associative. We derive that A/I_p is also right nilpotent of class at most n, or equivalently, that $A^{(n+1)} \subseteq I_p$. We conclude that

$$A^{(n+1)} \subseteq \bigcap_{p \text{ prime}} I_p = 0. \qquad \square$$

Note that Theorem 2.3.3 is a consequence of Theorem 2.3.4, applied with $n = 1$, and that we can also derive the following result.

Corollary 2.3.5. *Let A be a skew brace of abelian type with multiplicative group isomorphic to $\mathbb{Z}^2$. Then A is a homomorphic bi-skew brace.*

Proof. It follows from Theorem 2.3.4 that A is right nilpotent of class at most two, that is, A is homomorphic by Theorem 2.2.2. As $(A, \circ)$ is abelian, we find that A is also a bi-skew brace by Lemma 2.2.9. □

We go back to the motivating problem, by considering some skew braces with additive group cyclic infinite. We take the additive group $(\mathbb{Z}, +)$, and we define

$$n \circ m = n + (-1)^n m.$$

Note that $(\mathbb{Z}, \circ)$ is isomorphic to the infinite dihedral group

$$\langle x, y \mid y^2 = 1,\ yxy = x^{-1} \rangle \cong \mathbb{Z} \rtimes \mathbb{Z}_2,$$

and as shown in the proof of [Rum07b, Proposition 6], the following result holds.

Proposition 2.3.6. *The operation $\circ$ is the unique one on $\mathbb{Z}$ such that $(\mathbb{Z}, +, \circ)$ is a nontrivial skew brace.*

A direct computation shows that that $(\mathbb{Z}, +, \circ)$ is a (homomorphic) bi-skew brace, so also $(\mathbb{Z}, \circ, +)$ is a skew brace. Moreover, the two group automorphisms of $(\mathbb{Z}, +)$, the identity and the inversion $f\colon a \to -a$, are easily seen to be also automorphisms of $(\mathbb{Z}, \circ)$, and thus of the skew brace $(\mathbb{Z}, \circ, +)$.

Lemma 2.3.7. *The skew braces $(\mathbb{Z}, \circ, +)$ and $(\mathbb{Z}, \circ_{\mathrm{op}}, +)$ are not isomorphic.*

Proof. A skew brace isomorphism $(\mathbb{Z}, \circ, +) \to (\mathbb{Z}, \circ_{\mathrm{op}}, +)$ should also be an isomorphism of $(\mathbb{Z}, +)$. As $(\mathbb{Z}, \circ)$ is not abelian, the only candidate is the inversion f. But in this case, f would be both a group homomorphism and antihomomorphism of $(\mathbb{Z}, \circ)$, implying again that $(\mathbb{Z}, \circ)$ is abelian. □

In this way, we have obtained three nonisomorphic skew braces with multiplicative group $(\mathbb{Z}, +)$. In the remainder of this section, we prove that we have already found them all. In order to do this, we need two useful results. The first is a technical lemma.

Lemma 2.3.8. *Let A be a skew brace with abelian multiplicative group. Then $X * Y = Y *_{\mathrm{op}} X$ for all $X, Y \subseteq A$.*

Proof. It suffices to note that for all $a, b \in A$,

$$a * b = -a + (a \circ b) + -b = -a + (b \circ a) + -b = b *_{\mathrm{op}} a.$$ □

The second is [Nas19, Lemma 4.5], stated with a slightly more strict assumptions.

Lemma 2.3.9. *Let A be a skew brace with abelian multiplicative group. Then $(A^2, +)$ is abelian.*

Theorem 2.3.10. *Let A be a skew brace such that $(A, \circ)$ is an infinite cyclic group, with generator $x \in A$. Then the additive operation of A is given by one of the following:*

$$x^n + x^m = x^{n+m} = x^n \circ x^m, \tag{2.1}$$

$$x^n + x^m = x^{n+(-1)^n m}, \tag{2.2}$$

$$x^n + x^m = x^{m+(-1)^m n}. \tag{2.3}$$

In particular, there are exactly three isomorphism classes of skew braces with multiplicative group isomorphic to $\mathbb{Z}$.

Proof. If A is of abelian type, then Theorem 2.3.3 implies that A is trivial, so the additive operation is given by (2.1).

From now on, we assume that $(A, +)$ is not abelian. We claim that one of A and A_{op} is a bi-skew brace. If this is the case, then one of $(A, \circ, +)$ and $(A, \circ, +_{\mathrm{op}})$ is a nontrivial skew brace of infinite cyclic type, and by Proposition 2.3.6, this implies that the operation of $(A, +)$ is given by (2.2) or (2.3).

We prove now the claim. As A is nontrivial, $A^2 \neq 0$. On the other side, as A is a two-sided skew brace, we can apply Lemma 2.3.9 to deduce that $(A^2, +)$ is abelian, and thus $A^2 \neq A$. This means that A^2 is necessarily a trivial skew brace by Theorem 2.3.3. We also note that A/A^2 is a finite trivial skew brace of cyclic type, so that both its additive and multiplicative groups are generated by the class of x.

To show that one of A and A_{op} is a bi-skew brace, it is sufficient by Lemma 2.2.9 to check that that A or A_{op} is homomorphic, which by Theorem 2.2.2 and Lemma 2.3.8 reduces to show that $A *_{\mathrm{op}} A^2 = 0$ or $A * A^2 = 0$. Given a generator x of $(A, \circ)$, the map $\gamma(x)$ restricts to an automorphism of $(A^2, +)$, which is an infinite cyclic group. If $\gamma(x)$ restricts to the identity, then $A * A^2 = 0$. Suppose now that

$$^{\gamma(x)}a = -a$$

for all $a \in A^2$. Note that if y is a generator of $(A^2, +)$, then x and y generate the nonabelian group $(A, +)$. In particular, x and y do not commute, and writing ϕ for conjugation-by-x restricted to $(A^2, +)$, this implies that ϕ is the inversion map. We conclude that

$$^{\gamma_{\mathrm{op}}(x)}a = x + {}^{\gamma(x)}a - x = x - a - x = \phi(-a) = a,$$

which means that $A *_{\mathrm{op}} A^2 = 0$. □

2.4 Inner skew braces

We deal now with a class of skew braces that implicitly has appeared, in some instances, in the literature, trying to give a more systematic approach to its analysis. We first give a definition and show how various known skew braces belong to this class; we also present some properties that easily follow by the

definition, and that still have to appear. After, we follow the discussion in [CS23] to give a characterisation of skew braces in this class in cohomological terms, in order to answer a question that arises from the results in [BG22].

2.4.1 Definition, examples, and some properties

Definition 2.4.1. A skew brace A is *inner* if $\gamma(a) \in \mathrm{Inn}(A,+)$ for all $a \in A$.

Given an inner skew brace A, for all $a \in A$, there exists an element $\psi(a) \in A$ such that $\gamma(a) = \iota_+(\psi(a))$. In particular, we can always find a map $\psi\colon A \to A$ such that

$$a \circ b = a + \psi(a) + b - \psi(a).$$

This fact suggests the following notation.

Notation 2.4.2. Given a group $(A,+)$ and a map $\psi\colon A \to A$, we write

$$a \circ_\psi b = a + \psi(a) + b - \psi(a).$$

for all $a, b \in A$. In particular, every time we consider an inner skew brace A, there exists a suitable map $\psi\colon A \to A$ such that $\circ = \circ_\psi$. Note that two maps $\psi, \phi\colon A \to A$ satisfy $\circ_\psi = \circ_\phi$ if and only if $\psi(a) - \phi(a) \in Z(A,+)$ for all $a \in A$, by Theorem 2.1.12.

Many easy and well-known examples of skew braces are inner. Recall that a *Rota–Baxter operator* [GLS21] on a group $(A,+)$ is a map $\mathfrak{B}\colon A \to A$ such that for all $a, b \in A$,

$$\mathfrak{B}(a + \mathfrak{B}(a) + b - \mathfrak{B}(a)) = \mathfrak{B}(a) + \mathfrak{B}(b).$$

The following result is [BG22, Proposition 3.1], and it is based on [GLS21, Proposition 2.13].

Proposition 2.4.3. *Let $(A,+)$ be a group, and let $\mathfrak{B}\colon A \to A$ be a Rota–Baxter operator on $(A,+)$. Then $(A,+,\circ_{\mathfrak{B}})$ is an inner skew brace.*

Example 2.4.4. Let $(A,+)$ be a group.

- The trivial map
$$A \to A, \quad a \mapsto 0$$
is a Rota–Baxter operator on $(A,+)$, which yields the trivial skew brace $(A,+,+)$.
- The inversion map
$$A \to A, \quad a \mapsto -a$$
is a Rota–Baxter operator on $(A,+)$, which yields the almost trivial skew brace $(A,+,+_{\mathrm{op}})$.

Example 2.4.5. Let $(A,+)$ be a group, and let $\psi\colon (A,+) \to (A,+)$ be a group homomorphism such that $\psi(A)$ is abelian. Then ψ is a Rota–Baxter operator on $(A,+)$, and thus $(A,+,\circ_\psi)$ is a skew brace; this construction was initially considered in [Koc21], where it was shown that $(A,+,\circ_\psi)$ is also a bi-skew brace.

Example 2.4.6. Let $(A,+)$ be a group admitting an exact factorisation

$$A = B + C,$$

where B and C are subgroups of $(A,+)$. This means that for all $a \in A$, there exist unique $b \in B$ and $c \in C$ such that $a = b + c$. Define $\mathfrak{B}\colon A \to A$ by

$$\mathfrak{B}(b+c) = -c.$$

Then $\mathfrak{B}$ is a Rota–Baxter operator on $(A,+)$, as mentioned in [GLS21, Lemma 2.6], and hence $(A,+,\circ_{\mathfrak{B}})$ is an inner skew brace. Explicitly,

$$(b+c) \circ_{\mathfrak{B}} (b'+c') = b + b' + c' + c.$$

This skew brace was introduced in [GV17, Example 1.6], where it was also shown that $(A,\circ_{\mathfrak{B}}) \cong B \times C$.

We show that the skew braces obtained via Rota–Baxter operators are not necessarily bi-skew braces or homomorphic skew braces.

Lemma 2.4.7. *Let $(A,+)$ be a nonabelian simple group admitting an exact factorisation $A = B + C$ with $B \neq A$ and $C \neq A$. Then there exists an inner skew brace $(A,+,\circ)$ that is not homomorphic nor a bi-skew brace.*

Proof. Consider the skew brace $(A,+,\circ_{\mathfrak{B}})$ of Example 2.4.6, with

$$\mathfrak{B}(b+c) = -c.$$

As $Z(A,+) = 0$, the skew brace $(A,+,\circ_{\mathfrak{B}})$ is homomorphic (a bi-skew brace, respectively) if and only if $\mathfrak{B}\colon (A,+) \to (A,+)$ is a group homomorphism (antihomomorphism, respectively). Suppose that $\mathfrak{B}$ is a group homomorphism. Then for all $b \in B$ and $c \in C$, given $c + b = b' + c' \in B + C$, we have

$$\mathfrak{B}(c+b) = \mathfrak{B}(b'+c') = -c'$$

and

$$\mathfrak{B}(c) + \mathfrak{B}(b) = -c.$$

We find that $c' = c$, that is, $c + b - c = b' \in B$. But as $(A,+)$ is simple, we find a contradiction.

The case in which $\mathfrak{B}$ is a group antihomomorphism is similar. □

Example 2.4.8. The alternating group A_5 is simple and admits an exact factorisation via the alternating subgroup $\langle (123), (12)(34)\rangle \cong A_4$ and the cyclic $\langle (12345)\rangle \cong C_5$. The previous lemma yields an inner skew brace A with $(A,+) \cong A_5$ and $(A,\circ) \cong A_4 \times C_5$ that is not a homomorphic skew brace nor a bi-skew brace.

Remark 2.4.9. In the literature, particular attention has been devoted to skew braces of abelian type. We remark that studying inner skew braces, we are in some sense considering the opposite situation, as an inner brace of abelian type group is necessarily trivial. More generally, an inner skew brace A with $\circ = \circ_{\psi}$ is trivial if and only if $\psi(A) \subseteq Z(A,+)$.

Let A be an inner skew brace. The fact that there exists $\psi\colon A \to A$ such that $\gamma(a) = \iota_+(\psi(a))$ for all $a \in A$ has some consequences on the structure on A. First, it is clear that every normal subgroup of $(A,+)$ is a strong left ideal of A. Second, for all $a, b \in A$,

$$a * b = {}^{\gamma(a)}b - b = [\psi(a), b]_+.$$

This implies that $[A,A] = [A,A]_+$ and yields the following results.

Lemma 2.4.10. *Let A be an inner skew brace. Then*

$$\operatorname{Ann}(A) = \operatorname{Soc}(A) = \{a \in Z(A,+) \mid \psi(a) \in Z(A,+)\}.$$

Proof. Note that

$$\begin{aligned}\ker\gamma &= \{a \in A \mid \psi(a) + b - \psi(a) = b \text{ for all } b \in A\}\\ &= \{a \in A \mid \psi(a) \in Z(A,+)\},\end{aligned}$$

and this implies that

$$\operatorname{Soc}(A) = \{a \in Z(A,+) \mid \psi(a) \in Z(A,+)\}.$$

In addition, if $a \in Z(A,+)$ is such that $\psi(a) \in Z(A,+)$, then also $a \in Z(A,\circ)$. In particular, we find that

$$\operatorname{Ann}(A) = \operatorname{Soc}(A) \cap Z(A,\circ) = \operatorname{Soc}(A). \qquad \square$$

Proposition 2.4.11. *Let A be an inner skew brace of nilpotent type. Then A is left nilpotent.*

Proof. We show, by induction, that $A^n \subseteq \mathcal{L}^n$, where $\mathcal{L}^n$ denotes the nth term of the lower central series of $(A,+)$. For $n = 2$,

$$A^2 = A * A \subseteq [\psi(A), A]_+ \subseteq [A,A]_+ = \mathcal{L}^2.$$

Suppose now that the result holds for some $n \geq 2$. Then

$$A^{n+1} = A * A^n \subseteq [\psi(A), A^n]_+ \subseteq [A, \mathcal{L}^n]_+ = \mathcal{L}^{n+1}. \qquad \square$$

Remark 2.4.12. While $(A,+)$ being nilpotent is a sufficient condition for $(A,+,\circ)$ to be left nilpotent, we remark that it is not a necessary condition. The easiest example to consider is a trivial skew brace $(A,+,+)$ with $(A,+)$ not nilpotent.

As homomorphic skew braces and left nilpotent bi-skew braces are always right nilpotent (by Remark 2.2.3 and Corollary 2.2.15), we immediately derive the following result, which is an easy consequence of Theorem 2.1.44.

Corollary 2.4.13. *Let A be an inner skew brace that is homomorphic or a bi-skew brace. Then the following are equivalent:*

- *A is nilpotent.*

- *A is of nilpotent type.*

Proof. If A is nilpotent, then $(A,+)$ is nilpotent by Theorem 2.1.44.

Conversely, suppose that $(A,+)$ is nilpotent. Then A is left nilpotent by Proposition 2.4.11, and thus A is also right nilpotent by Corollary 2.2.15 in the bi-skew brace case (or by Theorem 2.2.2 in the case of homomorphic skew braces). We conclude that A is nilpotent again by Theorem 2.1.44 □

Remark 2.4.14. In section 2.5, we propose various constructions of inner skew braces $(A,+,\circ)$ that are both homomorphic and bi-skew braces, starting from a group $(A,+)$. In particular, every time we start from a nilpotent group, we always obtain nilpotent skew braces from these constructions.

2.4.2 A cohomological characterisation

As mentioned in Proposition 2.4.3, every Rota–Baxter operator yields an inner skew brace. We address here the question whether the converse holds.

Definition 2.4.15. An inner skew brace A is *Rota–Baxter* if there exists a Rota–Baxter operator $\mathfrak{B}$ on $(A,+)$ such that $\circ = \circ_{\mathfrak{B}}$.

Question 2.4.16. Is every inner skew brace a Rota–Baxter skew brace?

We give an answer to this question by giving a cohomological characterisation of inner skew braces, following the discussion of [CS23].

Consider an inner skew brace A, so that

$$\gamma\colon A \to \mathrm{Inn}(A,+), \quad a \mapsto \iota_+(\psi(a)).$$

for some $\psi\colon A \to A$. As for all $a,b \in A$,

$$\gamma(a\circ b) = \gamma(a)\gamma(b),$$

we derive that

$$\psi(a+\psi(a)+b-\psi(a)) \equiv \psi(a\circ b) \equiv \psi(a)\psi(b) \pmod{Z(A,+)}.$$

An easy situation occurs when $Z(A,+)=0$. In this case, we find

$$\psi(a+\psi(a)+b-\psi(a)) = \psi(a\circ b) = \psi(a)\psi(b),$$

which means that ψ is a Rota–Baxter operator; see [BG22, Proposition 3.13].

In order to approach the problem in its generality, we need to recall certain group-theoretic constructions, following for example [Wei69, Chapter V].

First, take a group G and an abelian group M. Recall that a map

$$\kappa\colon G\times G \to M$$

is a 2-*cocycle* (for the trivial action of G on M) if for all $a,b,c \in G$,

$$\kappa(a,bc)+\kappa(b,c) = \kappa(ab,c)+\kappa(a,b),$$

and a 2-*coboundary* is a map of the form

$$\delta(\sigma)\colon G \times G \to M, \quad (a,b) \mapsto \sigma(a) + \sigma(b) - \sigma(ab),$$

where $\sigma\colon G \to M$ is a map. Every 2-coboundary is a 2-cocycle, and we can define the *second cohomology group* as

$$\mathbf{H}^2(G,M) = \frac{\{\text{2-cocycles } G \times G \to M\}}{\{\text{2-coboundaries } G \times G \to M\}}.$$

If κ is a 2-cocycle, then we can endow the set $M \times G$ with a group structure:

$$(m,g)(m',g') = (m + m + \kappa(g,g'), gg').$$

We denote the group we obtain by $M \times_\kappa G$. It sits in a short exact sequence

$$0 \to M \xrightarrow{\iota} M \times_k G \xrightarrow{\pi} G \to 0,$$

of groups, where $\iota(m) = (m - \kappa(1,1), 1)$ and $\pi(m,g) = g$.

Theorem 2.4.17. *Let A be an inner skew brace, let $\psi\colon A \to A$ such that $\gamma(a) = \iota_+(\psi(a))$ for all $a \in A$, and define*

$$\kappa(a,b) = \psi(a) + \psi(b) - \psi(a \circ b) \in Z(A,+)$$

for all $a, b \in A$. Then the following hold:

- *The map $\kappa\colon (A,\circ) \times (A,\circ) \to Z(A,+)$ is a 2-cocycle, whose class in $\mathbf{H}^2((A,\circ), Z(A,+))$ does not depend on the choice of ψ.*
- *The following are equivalent:*
  - *A is a Rota–Baxter skew brace.*
  - *The class of κ in $\mathbf{H}^2((A,\circ), Z(A,+))$ is trivial.*
  - *The short exact sequence*

    $$0 \to Z(A,+) \to Z(A,+) \times_\kappa (A,\circ) \to (A,\circ) \to 0$$

    splits.

  If this is the case, and thus $\kappa = \delta(\sigma)$ is a 2-coboundary, then a Rota–Baxter operator $\mathfrak{B}$ on $(A,+)$ such that $\circ = \circ_{\mathfrak{B}}$ is given by

  $$\mathfrak{B}(a) = \psi(a) - \sigma(a).$$

Proof. First, we remark that $\kappa(a,b) \in Z(A,+)$, as

$$\psi(a \circ b) \equiv \psi(a)\psi(b) \pmod{Z(A,+)}.$$

Expanding the equality

$$\psi((a \circ b) \circ c) = \psi(a \circ (b \circ c))$$

one finds that κ is a 2-cocycle. More explicitly,

$$\begin{aligned}\psi((a \circ b) \circ c) &= -\kappa(a \circ b, c) + \psi(a \circ b) + \psi(c) \\ &= -\kappa(a \circ b, c) - \kappa(a, b) + \psi(a) + \psi(b) + \psi(c)\end{aligned}$$

and

$$\begin{aligned}\psi(a \circ (b \circ c)) &= -\kappa(a, b \circ c) + \psi(a) + \psi(b \circ c) \\ &= -\kappa(a, b \circ c) + \psi(a) - \kappa(b, c) + \psi(b) + \psi(c),\end{aligned}$$

and as the values of κ are central, the claim follows.

If $\psi' \colon A \to A$ is another map such that $\iota(\psi'(a)) = \gamma(a)$, then

$$\sigma(a) = \psi'(a) - \psi(a) \in Z(A, +),$$

and we find that

$$\begin{aligned}\kappa'(a, b) &= \psi'(a) + \psi'(b) - \psi'(a \circ b) = \psi(a) + \psi(b) - \psi(a \circ b) + \delta(\sigma)(a, b) \\ &= \kappa(a, b) + \delta(\sigma)(a, b),\end{aligned}$$

which means that κ and κ' are in the same class.

Now suppose that A is a Rota–Baxter skew brace. This means that there exists $\mathfrak{B} \colon A \to A$ such that, for all $a, b \in A$,

$$\mathfrak{B}(a) \equiv \psi(a) \pmod{Z(A, +)}$$

and

$$\mathfrak{B}(a \circ b) = \mathfrak{B}(a) + \mathfrak{B}(b).$$

The first condition implies that the 2-cocycle k' attached to $\mathfrak{B}$ is in the same class of κ, while the second that this class is trivial.

Conversely, suppose that the class of κ is trivial. Then $\kappa = \delta(\sigma)$ for some $\sigma \colon A \to Z(A, +)$. This means that

$$\sigma(a) + \sigma(b) - \sigma(a \circ b) = \kappa(a, b) = \psi(a) + \psi(b) - \psi(a \circ b),$$

and we obtain that

$$\mathfrak{B} \colon A \to A, \quad a \mapsto \psi(a) - \sigma(a)$$

is a Rota–Baxter operator on $(A, +)$ such that $\circ = \circ_{\mathfrak{B}}$.

Finally, the fact that the class of κ is trivial if and only if the short exact sequence

$$0 \to Z(A, +) \to Z(A, +) \times_{\kappa} (A, \circ) \to (A, \circ) \to 0$$

splits is a standard result in group cohomology; see [Wei69, Chapter V]. □

We can construct here an explicit example of an inner skew brace A that is not a Rota–Baxter skew brace; see [CS23, section 5].

Example 2.4.18. Let p be an odd prime, and let G be the Heisenberg group of order p^3:

$$G = \langle u, v, k : u^p, v^p, k^p, [u,v]k^{-1}, [u,k], [v,k] \rangle.$$

Every element of G can be written uniquely as

$$u^i v^j k^q,$$

with $0 \leq i, j, q < p$.

Let $(A, +) = E \times G$, where $E = \langle x, y \rangle$ is an elementary abelian group of order p^2, so that A has order p^5. Write $Z = Z(A, +) = E \times \langle k \rangle$. Consider the map

$$\psi \colon A \to A, \quad (x^i y^j, g) \mapsto (1, u^i v^j).$$

As $(A, +)/Z$ is an elementary abelian group of order p^2 generated by the classes of $(1, u)$ and $(1, v)$, we derive that the composition

$$(A, +) \xrightarrow{\psi} A \to (A, +)/Z,$$

is a group homomorphism with abelian image. Thus we can apply Proposition 2.5.12 below to obtain an inner skew brace $(A, +, \circ_\psi)$

We now compute the class of the 2-cocycle κ associated with this skew brace. For all $0 \leq i, j, m, n < p$ and $g, t \in G$, there exists $a \in G$ such that

$$\begin{aligned} \psi((x^i y^j, g) + \psi(x^i y^j, g) + (x^m y^n, t) - \psi(x^i y^j, g)) &= \psi(x^{i+m} y^{j+n}, a) \\ &= (1, u^{i+m} v^{j+n}). \end{aligned}$$

On the other hand,

$$\begin{aligned} \psi(x^i y^j, g) + \psi(x^m y^n, t) &= (1, u^i v^j) + (1, u^m v^n) \\ &= (1, u^{i+m} v^j [v^{-j}, u^{-m}] v^n) \\ &= (1, u^{i+m} v^{j+n} k^{-jm}). \end{aligned}$$

So the relevant 2-cocycle here is

$$\kappa(x^i y^j g, x^m y^n t) = (1, k^{-jm}),$$

with image in $\langle k \rangle \subseteq Z$.

We claim that the class of κ in $\mathbf{H}^2((A, \circ_\psi), Z)$ is nontrivial. This would yield that A is not a Rota–Baxter skew brace. So let $V = Z \times_\kappa (A, \circ_\psi)$, and consider the central extension

$$0 \to Z \xrightarrow{\iota} V \to (A, \circ_\psi) \to 0 \tag{2.4}$$

associated with the cocycle κ; here $\iota(e, k^q) = ((e, k_q), 0_A)$. Write $\tilde{x} = (x, 1)$ and $\tilde{y} = (y, 1)$ in A. In V the following hold:

$$\begin{aligned} [(0_Z, \tilde{x}), (0_Z, \tilde{y})] &= (0_Z, \tilde{x})(0_Z, \tilde{y})((0_Z, \tilde{y})(0_Z, \tilde{x}))^{-1} \\ &= (0_Z, \tilde{x}\tilde{y})(\kappa(\tilde{x}, \tilde{y}), 0_A)((\kappa(\tilde{y}, \tilde{x}), 0_A)(0_Z, \tilde{y}\tilde{x}))^{-1} \\ &= (0_Z, \tilde{x}\tilde{y})(0_Z, \tilde{y}\tilde{x})^{-1}(\kappa(\tilde{y}, \tilde{x}), 0_A)^{-1} \\ &= (-\kappa(\tilde{y}, \tilde{x}), 0_A) = ((1, k), 0_A), \end{aligned}$$

so that $\iota(1 \times \langle k \rangle)$ is contained in the derived subgroup $[V, V]$ of V.

Assume by way of contradiction that the sequence (2.4) splits, and let C be a complement to $\iota(Z)$ in V, so that $V = \iota(Z)C$. Then V contains the maximal subgroup $\iota(E \times 1)C$, which needs to contain $[V, V]$, being a maximal subgroup in the p-group V. But this is a contradiction, as $[V, V]$ contains $\iota(1 \times \langle k \rangle)$, which is not contained in $\iota(E \times 1)C$.

This shows that (2.4) does not split, so that $(A, +, \circ_\psi)$ is not a Rota–Baxter skew brace by Theorem 2.4.17.

Remark 2.4.19. Another instance of this behaviour was presented in [CS23, section 6], where it was also showed in an explicit example how to reconstruct the Rota–Baxter operator, in the case of a Rota–Baxter skew brace.

2.5 Constructions and examples

This section is devoted to the construction of explicit examples of skew braces of the form $(A, +, \circ)$, starting from a group $(A, +)$. If the skew brace is also a bi-skew brace, this gives an immediate construction of a Hopf–Galois structure on a Galois extension with Galois group isomorphic to $(A, +)$, as we discuss in the next chapter. The presentation in this section summarises some of the results of the papers [CS21, CS22, ST23a].

2.5.1 Some characterisations via gamma functions

In principle, given a group $(A, +)$, one should construct a new operation $\circ$ on A, then check if this is a group operation and whether the skew brace axiom holds. But as already mentioned above, there is an alternative route, using gamma functions. As a consequence of Theorem 2.1.12, we can provide some characterisations of certain classes of skew braces, widely used (usually in an inplicit way) to produce the constructions of skew braces in [CS21, CS22, ST23a]. First, we consider homomorphic skew braces, looking at actions of a group on itself.

Proposition 2.5.1. *Let $(A, +)$ be a group. Then there exists a bijective correspondence between*

- *the group homomorphisms $\gamma \colon (A, +) \to \mathrm{Aut}(A, +)$ such that for all $a, b \in A$,*
$$\gamma({}^{\gamma(a)}b) = \gamma(b);$$
- *the operations $\circ$ such that $(A, +, \circ)$ is a homomorphic skew brace.*

Specifically, such a function γ corresponds to the operation $\circ$ given by $a \circ b = a + {}^{\gamma(a)}b$.

Proof. By Theorem 2.1.12, the operations $\circ$ such that $(A, +, \circ)$ is a skew brace correspond bijectively to the functions

$$\gamma \colon A \to \mathrm{Aut}(A, +)$$

such that for all $a, b \in A$,

$$\gamma(a + {}^{\gamma(a)}b) = \gamma(a)\gamma(b),$$

which reduces to

$$\gamma({}^{\gamma(a)}b) = \gamma(b);$$

when $\gamma\colon (A,+) \to \mathrm{Aut}(A,+)$ is a group homomorphism. As by definition $(A,+,\circ)$ is a homomorphic skew brace if and only if $\gamma\colon (A,+) \to \mathrm{Aut}(A,+)$ is a group homomorphism, the assertion follows. □

For bi-skew braces it is just a slight variation.

Proposition 2.5.2. *Let $(A,+)$ be a group. Then there exists a bijective correspondence between*

- *the group antihomomorphisms $\gamma\colon (A,+) \to \mathrm{Aut}(A,+)$ such that for all $a, b \in A$,*
$$\gamma({}^{\gamma(a)}b) = \gamma(a)\gamma(b)\gamma(a)^{-1}$$
- *the operations $\circ$ such that $(A,+,\circ)$ is a bi-skew brace.*

Specifically, such a function γ corresponds to the operation $\circ$ given by $a \circ b = a + {}^{\gamma(a)}b$.

Proof. By Theorem 2.1.12, the operations $\circ$ such that $(A,+,\circ)$ is a skew brace correspond bijectively to the functions

$$\gamma\colon A \to \mathrm{Aut}(A,+)$$

such that for all $a, b \in A$,

$$\gamma(a + {}^{\gamma(a)}b) = \gamma(a)\gamma(b),$$

which reduces to

$$\gamma({}^{\gamma(a)}b) = \gamma(a)\gamma(b)\gamma(a)^{-1}$$

when $\gamma\colon (A,+) \to \mathrm{Aut}(A,+)$ is a group antihomomorphism. As, by Theorem 2.2.6, $(A,+,\circ)$ is a homomorphic skew brace if and only if $\gamma\colon (A,+) \to \mathrm{Aut}(A,+)$ is a group homomorphism, the assertion follows. □

These two results can be easily combined, as follows, via Lemma 2.2.9.

Corollary 2.5.3. *Let $(A,+)$ be a group. Then there exists a bijective correspondence between*

- *the group homomorphisms $\gamma\colon (A,+) \to \mathrm{Aut}(A,+)$ with abelian image such that for all $a, b \in A$,*
$$\gamma({}^{\gamma(a)}b) = \gamma(b);$$
- *the operations $\circ$ such that $(A,+,\circ)$ is a homomorphic bi-skew brace.*

Specifically, such a function γ corresponds to the operation $\circ$ given by $a \circ b = a + {}^{\gamma(a)}b$.

Example 2.5.4. Consider the cyclic group $(\mathbb{Z}/8\mathbb{Z}, +)$ of order 8, and take the group homomorphism

$$\gamma\colon (\mathbb{Z}/8\mathbb{Z}, +) \to \mathrm{Aut}(\mathbb{Z}/8\mathbb{Z}, +), \quad a \mapsto (b \mapsto 3^a b).$$

It is clear that the image of γ is abelian. In addition, the fact that

$$3^{3^a} = 3$$

in $\mathbb{Z}/8\mathbb{Z}$ for all $a \in \mathbb{Z}/8\mathbb{Z}$ immediately implies that $\gamma({}^{\gamma(a)}b) = \gamma(b)$ for all $a, b \in A$. We conclude that $(\mathbb{Z}/8\mathbb{Z}, +, \circ)$ is a homomorphic bi-skew brace, where

$$a \circ b = a + 3^a b.$$

The skew brace $(\mathbb{Z}/8\mathbb{Z}, +, \circ)$ was considered in [Bac15, Theorem 3.1], where it was shown that $(\mathbb{Z}/8\mathbb{Z}, \circ)$ is isomorphic to the quaternion group of order 8.

In a similar way, also the inner skew braces can be characterised. In the following, given a group $(A, +)$ and a map $\phi\colon A \to (A, +)/Z(A, +)$, we write, with a little abuse of notion,

$$a \circ_\phi b = a + \phi(a) + b - \phi(a).$$

Here with $\phi(a)$ we mean $\phi'(a)$, where $\phi'\colon A \to A$ is a *lifting* of ϕ, that is, a map $\phi'\colon A \to A$ such that $\phi'(a) + Z(A, +) = \phi(a)$ for all $a \in A$. Note that, despite the fact that the choice of the lifting is not unique, this operation is well-defined. Concretely, we are considering

$$a \circ_\phi b = a + {}^{\gamma(a)}b,$$

where γ is given by the composition

$$\gamma\colon A \to (A, +)/Z(A, +) \to \mathrm{Inn}(A, +).$$

Proposition 2.5.5. *Let $(A, +)$ be a group. Then there exists a bijective correspondence between*

- *the functions $\phi\colon A \to (A, +)/Z(A, +)$ such that for all $a, b \in A$,*

$$\phi(a + \phi(a) + b - \phi(a)) = \phi(a) + \phi(b).$$

- *the operations $\circ$ such that $(A, +, \circ)$ is an inner skew brace.*

Specifically, such a function γ corresponds to the operation $\circ_\phi$.

Proof. This results follows from Theorem 2.1.12 and the group isomorphism

$$(A, +)/Z(A, +) \cong \mathrm{Inn}(A, +), \quad \overline{a} \mapsto \iota_+(a). \qquad \square$$

As a final result, we obtain inner skew braces that are homomorphic and bi-skew braces.

Corollary 2.5.6. *Let $(A,+)$ be a group. Then there exists a bijective correspondence between*

- *the group homomorphisms $\phi\colon (A,+) \to (A,+)/Z(A,+)$ with abelian image;*
- *the inner homomorphic bi-skew braces of the form $(A,+,\circ)$.*

Specifically, a function ϕ corresponds to the operation $\circ_\phi$.

Proof. This result follows as a combination of Corollary 2.5.3 and Proposition 2.5.5. □

2.5.2 Some explicit constructions

We employ now these results to obtain new examples of skew braces. We begin with inner skew braces. We fix a group $(A,+)$ with centre Z, and we write $[B,C]$ for the commutator subgroup of two subsets B and C of A. As always, if $\psi\colon A \to A$ is a map, then we write

$$a \circ_\psi b = a + \psi(a) + b - \psi(a).$$

One can inquiry under what assumptions on ψ we get a (necessarily inner) skew brace $(A,+,\circ_\psi)$. The following result is implicitly contained and widely used in [CS21, CS23].

Proposition 2.5.7. *Let $\psi\colon A \to A$ be a map. Then the following are equivalent:*

- *$(A,+,\circ_\psi)$ is a skew brace.*
- *For all $a,b \in A$,*

$$\psi(a + \psi(a) + b - \psi(a)) \equiv \psi(a) + \psi(b) \pmod{Z}.$$

Proof. Note that $(A,+,\circ_\psi)$ is a skew brace if and only if the composition

$$\phi\colon A \xrightarrow{\psi} A \to A/Z$$

satisfies the property stated in Proposition 2.5.5, which translate exactly in the desired equation. □

This result suggests how the defining property of Rota–Baxter operators interacts so nicely with skew braces. We can immediately derive again Proposition 2.4.3.

Corollary 2.5.8. *Let $\mathfrak{B}$ be a Rota–Baxter operator on $(A,+)$. Then $(A,+,\circ_{\mathfrak{B}})$ is a skew brace.*

Proof. We can readily apply the previous proposition to $\mathfrak{B}$, as

$$\mathfrak{B}(a + \mathfrak{B}(a) + b - \mathfrak{B}(a)) = \mathfrak{B}(a) + \mathfrak{B}(b)$$

for all $a, b \in A$ by definition. □

The situation is particularly simplified when the map $\psi\colon (A,+) \to (A,+)$ is a group homomorphism. The next result is [CS21, Theorem 1.2] and generalises the construction in [Koc21].

Theorem 2.5.9. *Let $\psi\colon (A,+) \to (A,+)$ be a group homomorphism.*

- *The following are equivalent:*
  - *$(A,+,\circ_\psi)$ is a skew brace.*
  - *$\psi[\psi(A), A] \subseteq Z$.*

  If this is the case, then $(A,+,\circ_\psi)$ is homomorphic.
- *The following are equivalent:*
  - *$(A,+,\circ_\psi)$ is a bi-skew brace.*
  - *$\psi[A, A] \subseteq Z$.*

  If this is the case, then $(A,+,\circ_\psi)$ is homomorphic.

Proof. By Proposition 2.5.7, to check the first equivalence we need to check whether for all $a, b \in A$,

$$\psi(a + \psi(a) + b - \psi(a)) \equiv \psi(a) + \psi(b) \pmod{Z}.$$

As ψ is a group homomorphism, we can rewrite this as

$$\psi[\psi(a), b] = \psi(\psi(a)) + \psi(b) - \psi(\psi(a)) - \psi(b) \equiv 0 \pmod{Z}$$

which gives the desired condition. Note that this skew brace is always homomorphic as $\psi\colon (A,+) \to (A,+)$ is a group homomorphism; see Proposition 2.5.1. In addition, by Proposition 2.5.2, $(A,+,\circ_\psi)$ is a bi-skew brace if and only if $\gamma(A)$ is abelian, that is,

$$\psi(a) + \psi(b) \equiv \psi(b) + \psi(a) \pmod{Z}.$$

From this, the second equivalence immediately follows. □

Example 2.5.10. Let $\psi\colon (A,+) \to (A,+)$ be a group homomorphism with abelian image. By Theorem 2.5.9, we immediately obtain that $(A,+,\circ_\psi)$ is an inner homomorphic bi-skew brace. We have recovered the construction of [Koc21].

Corollary 2.5.11. *Suppose that $(A,+)$ is nilpotent of class two, and consider a group homomorphism $\psi\colon (A,+) \to (A,+)$. Then $(A,+,\circ_\psi)$ is an inner homomorphic bi-skew brace.*

Proof. The result follows by Theorem 2.5.9 as $\psi[A,A] \subseteq [A,A] \subseteq Z$. □

Note that also the condition of ψ being a group homomorphism can be relaxed; the following result is mentioned in [ST23a, Example 6.12].

Proposition 2.5.12. *Let $\psi\colon A \to A$ be a map such that the composition*

$$(A,+) \xrightarrow{\psi} A \to (A,+)/Z$$

is a group homomorphism with abelian image. Then $(A,+,\circ_\psi)$ is a homomorphic bi-skew brace.

Proof. The result easily follows applying Corollary 2.5.6 with

$$\phi\colon A \xrightarrow{\psi} A \to (A,+)/Z.$$ □

Corollary 2.5.13. *Suppose that $(A,+)$ is nilpotent of class two, and for all $n \geq 0$ define*

$$\psi_n\colon A \to A, \quad a \mapsto na.$$

Then $(A,+,\circ_{\psi_n})$ is a homomorphic bi-skew brace for all $n \geq 0$

Proof. The result follows by Proposition 2.5.12, as $(A,+)/Z$ is abelian and

$$(A,+) \to (A,+)/Z, \quad a \mapsto \overline{na}$$

is a group homomorphism. □

We remark that not all homomorphic inner skew braces can be obtained by the construction of Theorem 2.5.9, as [CS21, Example 5.4] shows. We present here a simplified version of this example, which we have also considered in relation to Rota–Baxter operators in the previous section.

Example 2.5.14. Let p be an odd prime, and suppose that $(A,+) = E \times G$, where $E = \langle x, y\rangle$ is an elementary abelian group of order p^2 and $G = \langle u, v, k\rangle$ is the the Heisenberg group of order p^3. If we take the map

$$\psi\colon A \to A, \quad (x^i y^j, g), \mapsto (1, u^i v^j)$$

then $(A,+,\circ_\psi)$ is an inner skew brace, as in Example 2.4.18.

Now suppose that there exists a group homomorphism $\varphi\colon (A,+) \to (A,+)$ such that $\circ_\psi = \circ_\varphi$. This implies, for all $h \in A$,

$$(x,1) + \psi(x,1) + h - \psi(x,1) = (x,1) + \varphi(x,1) + h - \varphi(x,1).$$

As $\psi(x,1) = (1,u)$ and $(A,+)$ is nilpotent of class 2, we derive

$$0 = [(1,u) - \varphi(x,1), h],$$

that this,

$$(1,u) - \varphi(x,1) = z_1 \in Z(A,+).$$

Similarly, one deduces that

$$(1, v) - \varphi(y, 1) = z_2 \in Z(A, +).$$

The contradiction follows from this equality:

$$\begin{aligned} 0 = \varphi[(x, 1), (y, 1)] &= [\varphi(x, 1), \varphi(y, 1)] = [(1, u) - z_1, (1, v) - z_2] \\ &= [(1, u), (1, v)] \neq 0. \end{aligned}$$

Note that the same reasoning shows that φ is also not a group antihomomorphism.

So far, we have focused our attention on inner skew braces. This means that these constructions just yield trivial skew braces if we start from abelian groups. We now consider a different construction, involving bilinear maps, that can also be applied with abelian groups. These result are inspired by [CS22], but with some slight differences.

Let us denote by $\mathcal{B}$ the set of bilinear maps

$$\beta \colon (A, +) \times (A, +) \to Z$$

such that for all $a, b, c \in A$,

$$\beta(\beta(a, b), c) = \beta(a, \beta(b, c)) = 0.$$

For all $\beta \in \mathcal{B}$, define

$$a \circ_\beta b = a + b + \beta(a, b).$$

Theorem 2.5.15. *Let $\beta \in \mathcal{B}$. Then $(A, +, \circ_\beta)$ is a homomorphic bi-skew brace.*

Proof. We prove the result via Corollary 2.5.3. For all $a \in A$, consider

$$\gamma(a) \colon b \to b + \beta(a, b).$$

We begin by checking that $\gamma(a)$ is a bijection: for all $b \in B$, note that

$${}^{\gamma(a)}(b - \beta(a, b)) = b - \beta(a, b) + \beta(a, b) - \beta(a, \beta(a, b)) = b,$$

and if ${}^{\gamma(a)}b = {}^{\gamma(a)}c$, then

$$c - b = \beta(a, b) - \beta(a, c) = -\beta(a, c - b),$$

which substituting for $c - b$ in the right-hand side implies that

$$c - b = \beta(a, \beta(a, c - b)) = 0.$$

We can now show that $\gamma(a)$ is a homomorphism of $(A, +)$: for all $a, b, c \in A$,

$$\begin{aligned} {}^{\gamma(a)}(b + c) &= b + c + \beta(a, b + c) = b + c + \beta(a, b) + \beta(a, c) \\ &= b + \beta(a, b) + c + \beta(b, c) = {}^{\gamma(a)}b + {}^{\gamma(a)}c. \end{aligned}$$

Similarly

$$\begin{aligned} {}^{\gamma(a)\gamma(b)}c &= c + \beta(b,c) + \beta(a,c) + \beta(a,\beta(b,c)) \\ &= c + \beta(a+b,c) = {}^{\gamma(a+b)}c \\ &= c + \beta(b+a,c) = {}^{\gamma(b)\gamma(a)}c \end{aligned}$$

where we have used that

$$\beta(a+b,c) = \beta(a,c) + \beta(b,c) = \beta(b,c) + \beta(a,c) = \beta(b+a,c)$$

because β takes values in $\mathbb{Z}$. This implies that

$$\gamma\colon (A,+) \to \mathrm{Aut}(A,+)$$

is a group homomorphism with abelian image. To conclude by Corollary 2.5.3, we note that for all $a,b,c \in A$,

$${}^{\gamma({}^{\gamma(a)}b)}c = {}^{\gamma(b+\beta(a,b))}c = c + \beta(b,c) + \beta(\beta(a,b),c) = c + \beta(b,c) = {}^{\gamma(b)}c. \qquad \square$$

Example 2.5.16. Suppose that $(A,+)$ is the additive group of a ring of characteristic p^n, with p prime and n even. For all $r \in A$, consider

$$\beta_r\colon A \times A \to A, \quad \beta_r(a,b) = rp^{n/2}ab.$$

It is just a matter of computation to check that $\beta \in \mathcal{B}$. We find in this way a skew brace $(A,+,\circ_{\beta_r})$, where explicitly

$$a \circ_{\beta_r} b = a + b + rp^{n/2}ab.$$

We can apply this when $(A,+)$ is the cyclic group $\mathbb{Z}/p^2\mathbb{Z}$ of order p^2, where p is a prime. For $r = 0$, we clearly obtain the trivial skew brace; for $r = 1,\dots,p-1$, instead, we obtain $p-1$ isomorphic skew braces. Indeed, a skew brace isomorphism

$$(\mathbb{Z}/p^2\mathbb{Z},+,\circ_{\beta_1}) \to (\mathbb{Z}/p^2\mathbb{Z},+,\circ_{\beta_r})$$

is given by

$$a \mapsto r^{-1}a.$$

Compare this with [Bac15, Proposition 2.4].

Example 2.5.17. Suppose that $(A,+)$ is the additive group of a ring with unity, and for all $r \in A$, define the following function:

$$\beta\colon (A \times A) \times (A \times A) \to (A \times A), \quad ((a,b),(x,y)) \mapsto (0,rax).$$

It is just a matter of computation to check that $\beta \in \mathcal{B}$, so that by Theorem 2.5.15, we find a skew brace $(A \times A,+,\circ_{\beta_r})$, where explicitly

$$(a,b) \circ_{\beta_r} (x,y) = (a+x, b+y+rax).$$

We can apply this when $(A,+)$ is the cyclic group $\mathbb{Z}/p\mathbb{Z}$ of order p, where p is a prime. For $r=0$, we clearly obtain the trivial skew brace; for $r=1,\dots,p-1$, instead, we obtain $p-1$ isomorphic skew braces. Indeed, a skew brace isomorphism

$$(\mathbb{Z}/p\mathbb{Z}^2,+,\circ_{\beta_1})\to(\mathbb{Z}/p\mathbb{Z}^2,+,\circ_{\beta_r})$$

is given by

$$(a,b)\mapsto(a,rb).$$

Compare this again with [Bac15, Proposition 2.4].

The previous example suggests the next one, that can be obtained following the lines of the proof of Theorem 2.5.15.

Example 2.5.18. Let p be a prime, let $0\leq m\leq n$ be integers, and consider the ring

$$R=\mathbb{Z}/p^n\mathbb{Z}\times\mathbb{Z}/p^m\mathbb{Z}$$

Define

$$\beta\colon R\times R\to R,\quad \beta((a,b),(x,y))=(0,ax).$$

Note that this is well-defined, as $n\geq m$. The fact that $(R,+,\circ_\beta)$ is a homomorphic bi-skew brace follows exactly as in the proof of Theorem 2.5.15.

We conclude by mentioning how the constructions related to inner skew braces and bilinear maps can be combined, giving a slight generalisation of the main construction of [CS22]. Given a map $\psi\colon A\to A$ and a bilinear map $\beta\in\mathcal{B}$, we define

$$a\circ_{\psi,\beta}b=a+\psi(a)+b-\psi(a)+\beta(a,b).$$

We are interested on skew braces of the form $(A,+,\circ_{\psi,\beta})$.

Proposition 2.5.19. *Let $\psi\colon A\to A$ be a map such that the composition $(A,+)\xrightarrow{\psi}A\to A/Z$ is a group homomorphism with abelian image, and let $\beta\in\mathcal{B}$ such that for all $a,b\in A$*

$$\psi(\beta(a,b))\in Z.$$

Then $(A,+,\circ_{\psi,\beta})$ is a homomorphic bi-skew brace.

Proof. We prove the result via Corollary 2.5.3. For all $a\in A$, write

$$\gamma(a)=\iota(\psi(a))\alpha(a),$$

where

$$\alpha(a)\colon b\to b+\beta(a,b).$$

By Proposition 2.5.12 and Theorem 2.5.15, we find that $\gamma(a)\in\mathrm{Aut}(A,+)$ for all $a\in A$. In addition, an easy check shows that $\iota(\psi(a))$ and $\alpha(b)$ commute in $\mathrm{Aut}(A,+)$ for all $a,b\in A$, and this implies that γ is a group homomorphism from both $(A,\circ)$ and $(A,+)$ to $\mathrm{Aut}(A,+)$ with abelian image.

To conclude, we need a final verification. Note that for all $a, b \in A$,

$$\iota(\psi({}^{\gamma(a)}b)) = \iota(\psi(\psi(a) + b + \beta(a,b) - \psi(a))) = \iota(\psi(b))$$

by assumptions on ψ and on β. Similarly,

$$\alpha({}^{\gamma(a)}b) = \alpha(b)$$

by an easy application of the properties of α (and β). We conclude that $(A, +, \circ_{\psi,\beta})$ is a homomorphic skew brace. □

Example 2.5.20. Suppose that $(A, +)$ is nilpotent of class two, and consider group homomorphisms $\psi, \phi \colon (A, +) \to (A, +)$. Define

$$\beta \colon A \times A \to A, \quad (a, b) = [\phi(a), \phi(b)].$$

Clearly $\beta(a, b) \in [A, A] \subseteq Z$. The fact that $\beta \in \mathcal{B}$ follows by the observations that

$$\beta(\beta(a, b), c)) = [\psi[\psi(a), \psi(b)], \psi(c)] = 0,$$

as $\psi[\psi(a), \psi(b)] \in Z$, and similarly for the other way around. Then $(A, +, \circ_{\psi,\beta})$ is a homomorphic bi-skew brace by Proposition 2.5.19, as for all $a, b \in A$,

$$\psi[\varphi(a), \varphi(b)] \in [A, A] \subseteq Z.$$

Chapter 3

Connecting Hopf–Galois Structures and Skew Braces

In this final chapter, we deal with the connection between Hopf–Galois structures and skew braces. After having recalled some known facts and the previous connection, we introduce a new version, with the goal to make it bijective, explicit, and more structural. As applications, we derive some of the main theorems in Hopf–Galois theory from this new perspective; we describe the Hopf algebras appearing in terms of skew braces, finding an interpretation of standard notions and substructures of them; and we discuss the Hopf–Galois correspondence, finding new classes of examples for which it is bijective. We conclude the chapter with a "take-home" theorem, in which we summarise the results developed in a general way. The result of these sections are taken from [ST23b], with some slight generalisations or additions.

3.1 The previous connection

The previous connection between Hopf–Galois structures and skew braces, initially hinted by Bachiller [Bac16] and then made precise by Byott and Vendramin in the appendix of [SV18], is due to the connections of both topics with regular subgroups of the holomorph. We begin by recalling a standard group-theoretic construction: if M is a group, X is a set, and there exists a bijection

$$\theta\colon M \to X,$$

then we can obtain, via *transport of structure*, a group structure on X as follows:

$$xy = \theta(\theta^{-1}(x)\theta^{-1}(y)).$$

As a consequence, the map θ is now also a group isomorphism.

Transport of structure appears in the connection between regular subgroups and skew braces. The next result is [GV17, Theorem 4.2], but with a slight

variation; indeed, to simplify the computation in the following, we assume directly the holomorph to sit inside a permutation group, rather than being an abstract group (see also [CS21, section 7]). In what follows, we continue to adopt the same notation of the previous chapter, highlighting explicitly the group operation where there is risk of confusion.

Theorem 3.1.1. *Let $(A,+)$ be a group. Then there exists a bijective correspondence between*

- *the operations $\circ$ such that $(A,+,\circ)$ is a skew brace;*
- *the regular subgroups of* $\mathrm{Hol}(A,+)$.

Specifically, an operation $\circ$ such that $(A,+,\circ)$ is a skew brace corresponds to the regular subgroup $\lambda_\circ(A)$ of $\mathrm{Hol}(A,+)$. *Conversely, a regular subgroup M of* $\mathrm{Hol}(A,+)$ *corresponds to the operation $\circ$ on A obtained by the bijection*

$$\theta\colon M \to A, \quad \mu \mapsto \mu[0_A],$$

via transport of structure; in addition, the equality $M = \lambda_\circ(A)$ holds.

We can now connect skew braces with Hopf–Galois structures, following the discussion the appendix of [SV18].

Let L/K be a finite Galois extension with Galois group G, and consider a Hopf–Galois structure on L/K, corresponding to a regular subgroup $(N,+)$ of $\mathrm{Perm}(G)$ normalised by $\lambda(G)$ by the Greither–Pareigis theorem. The natural inclusion of N in $\mathrm{Perm}(G)$ is regular embedding

$$\alpha\colon N \to \mathrm{Perm}(G),$$

and as we have the bijection

$$\alpha_*\colon N \to G, \quad \eta \mapsto \eta[1_G],$$

we obtain via Byott's translation a regular embedding

$$\beta\colon G \to \mathrm{Hol}(N,+), \quad \sigma \mapsto \alpha_*^{-1}\lambda(\sigma)\alpha_*.$$

In particular, the image $\beta(G)$ of β is a regular subgroup of $\mathrm{Hol}(N,+)$, which yields by Theorem 3.1.1 an operation $\circ$ such that $(N,+,\circ)$ is a skew brace. To make this more explicit, we need to specify the map

$$\theta\colon \beta(G) \to N, \quad \beta(\sigma) \mapsto \beta(\sigma)[0_N].$$

By the definition of α_*, it follows that

$$\beta(\sigma)[0_N] = (\alpha_*^{-1}\lambda(\sigma)\alpha_*)[0_N] = \alpha_*^{-1}(\sigma),$$

so the inverse of θ is exactly $\beta\alpha_*$. We conclude that

$$\eta \circ \mu = \theta(\theta^{-1}(\eta)\theta^{-1}(\mu)) = \alpha_*^{-1}\beta^{-1}(\beta(\alpha_*(\eta)\alpha_*(\mu)) = \alpha_*^{-1}(\alpha_*(\eta)\alpha_*(\mu)),$$

that is, the operation $\circ$ on N can be obtained directly by transport of structure via the bijection

$$\alpha_*^{-1}\colon G \to N.$$

This more direct route is used, for example, in [KT20]. In [NZ19], in a similar way, the bijection

$$\alpha_*\colon N \to G, \quad \eta \mapsto \eta[1_G]$$

is used to construct directly a group operation $+$ on G such that $(G, +, \circ)$ is a skew brace, where $\circ$ denotes the original group operation of the Galois group G. Clearly, the two procedures give two skew braces that are isomorphic via the map α_*.

Conversely, let A be a skew brace such that there exists a group isomorphism $\varphi\colon G \to (A, \circ)$. The composition

$$G \xrightarrow{\varphi} (A, \circ) \to \lambda_\circ(A) \to \mathrm{Hol}(A, +)$$

is a regular embedding

$$\beta\colon G \to \mathrm{Hol}(A, +), \quad \sigma \mapsto \lambda_\circ(\varphi(\sigma))$$

which yields a Hopf–Galois structure on L/K of type $(A, +)$ by Byott's translation. We can explicitly write this in Greither–Pareigis terms, as already mentioned for example in [NZ19, Proposition 2.1]. Note indeed that the associated bijection

$$\beta_*\colon G \to A, \quad \sigma \mapsto \beta(\sigma)(0_A) = \varphi(\sigma)$$

equals φ. Therefore, by Byott's translation, we obtain a regular embedding

$$\alpha\colon (A, +) \to \mathrm{Perm}(G), \quad a \mapsto \varphi^{-1}\lambda_+(a)\varphi$$

such that $\alpha(A)$ is normalised by $\lambda(G)$. Note that if we transport the structure of $(A, +)$ on G via the bijection

$$\varphi^{-1}\colon A \to G,$$

we obtain a group $(G, +)$ such that for all $a \in A$ and $\sigma \in G$,

$$(\varphi^{-1}\lambda_+(a)\varphi)(\sigma) = \varphi^{-1}(a) + \sigma,$$

which means that $\alpha(a) = \lambda_+(\varphi^{-1}(a))$, and thus $\alpha(A) = \lambda_+(G)$. We conclude that if we denote by $\circ$ the group operation of the Galois group G and we employ the bijection

$$\varphi^{-1}\colon A \to G$$

to obtain an operation $+$ on G, so that $(G, +, \circ)$ is a skew brace, then the regular subgroup associated with A via Byott's translation is exactly $\lambda_+(G)$.

Remark 3.1.2. We underline that the skew brace A (up to isomorphism) can be used, via this construction, to obtain possibly more than one Hopf–Galois structure on L/K; this reflects the possibility of changing the choice of φ. The precise number was quantified in [NZ19, Corollary 2.4]; see Corollary 3.3.3 below.

All the previous discussion, together with the observation that the types of the skew braces and Hopf–Galois structures considered coincide by construction, yields the following result.

Theorem 3.1.3. *Let N and G be finite groups. Then the following statements are equivalent:*

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

The first natural examples already show a peculiar behaviour of this connection.

Example 3.1.4. Let L/K be a finite Galois extension with Galois group G, and suppose that $(N,+)$ is a regular subgroup of $\mathrm{Perm}(G)$ normalised by $\lambda(G)$.

- Take $(N,+) = \rho(G)$, which corresponds to the classical structure via the Greither–Pareigis theorem. In this case

  $$\alpha_* \colon \rho(G) \to G, \quad \rho(\sigma) = \sigma^{-1}$$

  so we obtain the almost trivial skew brace $(N,+,+_{\mathrm{op}})$, as

  $$\rho(\sigma) \circ \rho(\tau) = \alpha_*^{-1}(\alpha_*(\rho(\sigma))\alpha_*(\rho(\tau))) = \alpha_*^{-1}(\sigma^{-1}\tau^{-1}) = \rho(\tau) + \rho(\sigma).$$

- Take $(N,+) = \lambda(G)$, which corresponds to the canonical nonclassical structure via the Greither–Pareigis theorem. In this case

  $$\alpha_* \colon \lambda(G) \to G, \quad \lambda(\sigma) = \sigma$$

  so we obtain the trivial skew brace $(N,+,+)$, as

  $$\lambda(\sigma) \circ \lambda(\tau) = \alpha_*^{-1}(\alpha_*(\lambda(\sigma))\alpha_*(\lambda(\tau))) = \alpha_*^{-1}(\sigma\tau) = \lambda(\sigma) + \lambda(\tau).$$

With the aim of studying the Hopf–Galois correspondence via skew braces, Childs [Chi18] introduced a new substructure for skew braces.

Definition 3.1.5. Let A be a skew brace. A subgroup B of $(A,+)$ is $\circ$-*stable* if for all $a \in A$ and $b \in B$,

$$(a \circ b) - a \in B.$$

The following result is [Chi18, Theorem 4.3] and employs the aforementioned connection and the definition of $\circ$-stable subgroups

Theorem 3.1.6. *Let A be a skew brace, and let L/K be a finite Galois extension with Galois group G such that there exists a group isomorphism $\varphi \colon G \to (A,\circ)$. Consider the Hopf–Galois structure $(H,\cdot)$ on L/K obtained from this data. There exists a bijective correspondence between*

- *the Hopf subalgebras of H;*
- *the $\circ$-stable subgroup of $(A, +)$.*

This result was employed to study the Hopf–Galois correspondence ratio in many examples [Chi18, Chi21], employing the fact that Hopf subalgebras correspond to intermediate fields via the Hopf–Galois correspondence. One of the consequences is the following proposition [Chi17, Proposition 4.3], which is based on a deep result of Kohl [Koh98].

Proposition 3.1.7 (Childs)**.** *Let L/K be a finite Galois extension with Galois group cyclic of odd prime power order. Then all the Hopf–Galois structures on L/K have a bijective Hopf–Galois correspondence.*

Other than this result, which can also be obtained via the Greither–Pareigis theorem, no new instances of bijective Hopf–Galois correspondences have been found, as claimed in the introduction of [Chi21]. A possible explanation for the lack of new examples could be given by the fact that the substrucures 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.

In this regard, Koch and Truman introduced the notion of opposite skew brace [KT20], and observed how given a skew brace A, the $\circ$-stable subgroups of $(A, +)$ coincide with the left ideals of A_{op}. The following result, a slight reformulation of [KT20, Theorem 5.6], can be obtained via this fact.

Theorem 3.1.8. *Let L/K be a finite Galois extension with Galois group G, and let $(H, \cdot)$ be a Hopf–Galois structure on L/K, corresponding to a regular subgroup $(N, +)$ of $\mathrm{Perm}(G)$. Consider the skew brace $(N, +, \circ)$ obtained by this data. Then there exists a bijective correspondence between*

- *the Hopf subalgebras of H;*
- *the left ideals of $(N, +_{\mathrm{op}}, \circ)$.*

This fact, together with the behaviour of the trivial and almost trivial skew brace, is a key insight about the fact that opposite skew braces may play a fundamental role in Hopf–Galois theory.

3.2 The new connection

This section contains the main result of the dissertation, which is [ST23b, Theorem 3.1]. In order to prove it, we need to state a proposition which is a variation of [GV17, Theorem 4.2] in two senses: we consider the right regular representation instead of the left regular representation, and we fix a multiplicative group instead of an additive one; see [CS22, section 7].

Proposition 3.2.1. *Let $(G, \circ)$ be a group. Then there exists a bijective correspondence between*

- *the operations* $+$ *such that* $(G,+,\circ)$ *is a skew brace;*
- *the regular subgroups of* $\mathrm{Perm}(G)$ *normalised by* $\lambda_\circ(G)$.

Specifically, an operation $+$ *such that* $(G,+,\circ)$ *is a skew brace corresponds to the regular subgroup* $\rho_+(G)$ *of* $\mathrm{Perm}(G)$. *Conversely, a regular subgroup* N *of* $\mathrm{Perm}(G)$ *normalised by* $\lambda_\circ(G)$ *corresponds to the operation* $+$ *on* G *obtained by transport of structure via the bijection*

$$\theta\colon N \to G, \quad \eta \mapsto \eta^{-1}[1_G],$$

and the equality $N = \rho_+(G)$ *holds.*

Proof. Suppose first that $+$ is an operation on $(G,\circ)$ such that $(G,+,\circ)$ is a skew brace. Clearly $\rho_+(G)$ is a regular subgroup of $\mathrm{Perm}(G)$ isomorphic to $(G,+)$. As also $(G,+_{\mathrm{op}},\circ)$ is a skew brace, we get that $\lambda_{+_{\mathrm{op}}}(G)$ is normalised by $\lambda_\circ(G)$, as seen in Theorem 3.1.1. But as the equality $\rho_+(G) = \lambda_{+_{\mathrm{op}}}(G)$ holds, we conclude that $\rho_+(G)$ is normalised by $\lambda_\circ(G)$.

Conversely, if N is a regular subgroup of $\mathrm{Perm}(G)$, then the bijection

$$\theta\colon N \to G, \quad \eta \mapsto \eta^{-1}[1_G]$$

yields, via transport of structure, a group operation $+$ on G. Explicitly, if

$$\nu\colon G \to N$$

is the inverse of θ, meaning that $\nu(\sigma)^{-1}$ is the unique element of N that maps 1_G to σ, then

$$\sigma + \tau = \theta(\nu(\sigma)\nu(\tau)) = \nu(\tau)^{-1}[\sigma],$$

meaning $N = \lambda_{+_{\mathrm{op}}}(G) = \rho_+(G)$. As N is also normalised by $\lambda_\circ(G)$, we obtain that $(G,+_{\mathrm{op}},\circ)$ is a skew brace by Theorem 3.1.1, and thus also $(G,+,\circ)$ is a skew brace. □

Let now L/K be a finite Galois extension with Galois group $(G,\circ)$, and let $+$ be an operation such that $(G,+,\circ)$ is a skew brace. Then $(G,\circ)$ acts on $(G,+)$ via the gamma function of $(G,+,\circ)$. This action extends to a Hopf semilinear action of G on $L[(G,+)]$, which, by Galois descent, descents to the K-Hopf algebra

$$L[(G,+)]^{(G,\circ)} = \left\{ \sum_{\tau\in G} \ell_\tau \tau \in L[(G,+)] \mid \sigma(\ell_\tau) = \ell_{(\gamma(\sigma)_\tau)} \text{ for all } \sigma,\tau \in G \right\}.$$

Notation 3.2.2. When there are various operations involved and there is risk of confusion, in order to lighten the notation, we write the operations appearing in the descriptions of the Hopf algebras as subscripts. For example, we denote $L[(G,+)]^{(G,\circ)}$ simply by $L[G_+]^{G_\circ}$.

Here we give the main result.

Theorem 3.2.3. *Let L/K be a finite Galois extension with Galois group $(G, \circ)$. Then there exists a bijective correspondence between*

- *the operations $+$ such that $(G, +, \circ)$ is a skew brace;*
- *the Hopf–Galois structures on L/K.*

Specifically, an operation $+$ such that $(G, +, \circ)$ is a skew brace corresponds to the Hopf–Galois structure $(L[G_+]^{G_\circ}, \cdot)$, where

$$\left(\sum_{\tau\in G} \ell_\tau\tau\right)\cdot x = \sum_{\tau\in G} \ell_\tau\tau(x).$$

Proof. The fact that there exists the claimed bijective correspondence is a consequence of Proposition 3.2.1 and the Greither–Pareigis theorem. We just need to show that the Hopf–Galois structures on L/K can be described in this way, as per Remark 1.2.4. So take an operation $+$ such that $(G, +, \circ)$ is a skew brace. Clearly the map

$$\rho_+ \colon (G, +) \to \rho_+(G), \quad \sigma \mapsto \rho_+(\sigma)$$

is a group isomorphism, and we claim that it is also $(G, \circ)$-equivariant, where the action of $(G, \circ)$ on $(G, +)$ is given by the gamma function of the skew brace $(G, +, \circ)$. It is enough to show that for all $\sigma, \tau \in G$,

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

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

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

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

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

By Corollary 1.3.13, we derive that

$$L[G_+]^{G_\circ} \to L[\rho_+(G)]^{G_\circ}, \quad \sum_{\tau\in G} \ell_\tau\tau \mapsto \sum_{\tau\in G} \ell_\tau\rho_+(\tau)$$

is a K-Hopf algebra isomorphism. To conclude, we need to find the action of $L[G_+]^{G_\circ}$ on L that respects this isomorphism:

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

□

Remark 3.2.4. We remark the similarity between the action of the Hopf algebras appearing in Theorem 3.2.3 and the classical Galois action of the group algebra.

Remark 3.2.5. Given a Hopf–Galois structure on L/K, we can attach to it a regular subgroup N of $\mathrm{Perm}(G)$ normalised by $\lambda_\circ(G)$ (by the Greither–Pareigis theorem) and an operation $+$ such that $(G, +, \circ)$ is a skew brace (by Theorem 3.2.3). The idea behind the proof of Theorem 3.2.3 is that we realise N as $\rho_+(G)$, and not as $\lambda_+(G)$, which would be the standard choice. In particular, the skew brace $(G, +, \circ)$ we obtain in this way is the opposite of that we would have obtained via the previous construction.

Remark 3.2.6. Note that by Theorem 3.2.3, the type of a Hopf–Galois structure on L/K is exactly the isomorphism class of the additive group of the skew brace corresponding to it. This feature is shared also by the previous version of the connection, as already mentioned.

We show here some examples; the first two show that the new connection solves the peculiar behaviour mentioned in Example 3.1.4.

Example 3.2.7. Let L/K be a finite Galois extension with Galois group G, and consider the trivial skew brace $\mathrm{Triv}(G)$. As the gamma function of this skew brace is given by

$$\gamma\colon G \to \mathrm{Aut}(G), \quad \sigma \mapsto \mathrm{id},$$

we find that the equality

$$H = L[G]^G = L^G[G] = K[G]$$

holds. As the action of H on L is given by the Galois action, we find that the trivial skew brace structure on the Galois group corresponds to the classical structure.

Example 3.2.8. Let L/K be a finite Galois extension with Galois group $(G, \circ)$, and consider the almost trivial skew brace $(G, \circ_{\mathrm{op}}, \circ)$. Here for all $\sigma, \tau \in G$,

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

so we find that

$$H = \left\{ \sum_{\tau \in G} \ell_\tau \tau \in L[G_{\circ_{\mathrm{op}}}] \mid \sigma(\ell_\tau) = \ell_{\sigma\circ\tau\circ\sigma^{-1}} \text{ for all } \sigma, \tau \in G \right\}.$$

As $\rho_{\circ_{\mathrm{op}}}(G) = \lambda_\circ(G)$, we derive in this way the canonical nonclassical structure on L/K. Concretely, the group isomorphism

$$(G, \circ_{\mathrm{op}}) \to (G, \circ), \quad \sigma \mapsto \sigma^{-1}$$

yields a K-Hopf algebra isomorphism that identifies this Hopf–Galois structure with that of Example 1.4.7.

Example 3.2.9. Let L/K be a finite Galois extension with cyclic Galois group $(G, \circ)$ of order $2n$, where $n \geq 3$ is odd, so that $(G, \circ) \cong C_n \times C_2$. Write

$$G = \{g^i t^j \mid i = 1, \ldots, n \text{ and } j = 0, 1\},$$

which means that g has order n and t has order 2, and define

$$g^i t^j + g^a t^b = g^{i+(-1)^j a} t^{j+b},$$

so that $(G, +) \cong C_n \rtimes C_2$ is dihedral. By Example 2.2.23 applied with the action via inversion of C_2 on C_n, we obtain that $(G, \circ, +)$ is a bi-skew brace, and therefore also $(G, +, \circ)$ is a skew brace. As $(G, \circ)$ is cyclic, it is enough to compute the values of the gamma function of $(G, +, \circ)$ on the generator $\sigma = gt$: for all $\tau = g^a t^b \in G$,

$$^{\gamma(\sigma)}\tau = -(gt) + (gt \circ g^a t^b) = gt + g^{1+a} t^{1+b} = g^{-a} t^b = \tau^{-1}.$$

We conclude that

$$H = \left\{ \sum_{\tau \in G} \ell_\tau \tau \in L[G_+] \mid \sigma(\ell_\tau) = \ell_{\tau^{-1}} \text{ for all } \tau \in G \right\}.$$

Example 3.2.10. Let L/K be a finite Galois extension with Galois group $(G, \circ)$, and consider an operation $+$ such that $(G, +, \circ)$ is an inner skew brace. Then there exists a map $\psi \colon G \to G$ such that for all $\sigma, \tau \in G$,

$$^{\gamma(\sigma)}\tau = \psi(\sigma) + \tau - \psi(\sigma).$$

In particular,

$$H = \left\{ \sum_{\tau \in G} \ell_\tau \tau \in L[G_+] \mid \sigma(\ell_\tau) = \ell_{\psi(\sigma)+\tau-\psi(\sigma)} \text{ for all } \sigma, \tau \in G \right\}.$$

Theorem 3.2.3 allows one to obtain bijectively all Hopf–Galois structures on a Galois extension, via skew braces constructed in a given "environment": the underlying set needs to be the Galois group. However, in some cases, it may be more convenient to work in a more general setting, considering abstract skew braces.

So let us take a skew brace A. If L/K is a finite Galois extension with Galois group G such that there exists a group isomorphism $\varphi \colon (A, \circ) \to G$, then the pair (A, φ) yields an operation $+_\varphi$ on G via transport of structure:

$$\sigma +_\varphi \tau = \varphi(\varphi^{-1}(\sigma) + \varphi^{-1}(\tau)).$$

In particular, denoting by $\circ$ the group operation of the Galois group G, we obtain that $(G, +_\varphi, \circ)$ is a skew brace, isomorphic to A via φ. This skew brace corresponds to a Hopf–Galois structure on L/K via Theorem 3.2.3. We obtain in this way that an abstract skew brace A yields a Hopf–Galois structure on

every Galois extension with Galois group isomorphic to $(A, \circ)$, once a group isomorphism is chosen. Note that the Hopf–Galois structure $(H, \cdot)$ obtained by a pair (A, φ) can be described explicitly, due to the skew brace isomorphism $\varphi\colon A \to (G, +_\varphi, \circ)$. If ϕ denotes the inverse of φ and γ denotes the gamma function of A, then

$$H = \left\{ \sum_{a \in A} \ell_a a \in L[A_+] \mid \sigma(\ell_a) = \ell_{\gamma(\phi(\sigma))a} \text{ for all } \sigma \in G \text{ and } a \in A \right\}$$

and

$$\left(\sum_{a \in A} \ell_a a \right) \cdot x = \sum_{a \in A} \ell_a \varphi(a)(x).$$

We define now a relation on the set of such pairs: given (A, φ) and (A', φ'), we say that

$$(A, \varphi) \sim (A', \varphi')$$

if for all $\sigma, \tau \in G$,

$$\sigma +_\varphi \tau = \sigma +_{\varphi'} \tau$$

that is, if $+_\varphi = +_{\varphi'}$. It is straightforward to check that it is an equivalence relation. Note that in this case A and A' are isomorphic as skew braces, but the equivalence relation is actually stronger than just isomorphism.

Theorem 3.2.11. *Let L/K be a finite Galois extension with Galois group G. Then there exists a bijective correspondence between*

- *the equivalence classes of pairs (A, φ) under the equivalence relation $\sim$, where A is a skew brace and $\varphi\colon (A, \circ) \to G$ is a group isomorphism;*
- *the Hopf–Galois structures on L/K.*

Proof. Denote by $\circ$ the group operation of G. By Theorem 3.2.3, it is enough to construct a suitable bijective correspondence between

- the operations $+$ such that $(G, +, \circ)$ is a skew brace;
- the equivalence classes of pairs (A, φ) under the equivalence relation $\sim$, where A is a skew brace and $\varphi\colon (A, \circ) \to G$ is a group isomorphism.

Given an operation $+$ such that $(G, +, \circ)$ is a skew brace, we simply take $A = (G, +, \circ)$ and φ to be the identity map.

Conversely, given a representative (A, φ) of an equivalence class, where A is a skew brace and $\varphi\colon (A, \circ) \to G$ is a group isomorphism, we just take the operation $+$ on G obtained via transport of structure by φ.

It is just a matter of standard calculations to show that these maps are well-defined and one the inverse of the each other. □

Example 3.2.12. Let A be a(n almost) trivial skew brace. It is easy to check that for all finite Galois extensions L/K with Galois group $G \cong (A, \circ)$ and for all choices of isomorphism $\varphi\colon (A, \circ) \to G$, the Hopf–Galois structure on L/K we obtain is the (canonical non)classical structure.

Remark 3.2.13. In the final section of the last chapter we have obtained various explicit ways to start from a group $(A, +)$ and obtain a bi-skew brace A of the form $(A, +, \circ)$. In particular, if L/K is a finite Galois extension with Galois group G such that there exists a group isomorphism $\varphi\colon (A, +) \to G$, then we can employ the pair $(A_{\leftrightarrow}, \varphi)$ to construct a Hopf–Galois structure on L/K. This means that all the constructions of this kind mentioned there yield explicit constructions of Hopf–Galois structures on a Galois extension with a given Galois group.

3.3 Known results from a new perspective

In this section, we show that from Theorems 3.2.3 and 3.2.11 we can derive again some known results in Hopf–Galois theory and its connection with skew brace theory.

First, note that as a consequence of Theorem 3.2.11, it is immediate to deduce that Theorem 3.1.3 holds.

Second, we can give a short proof of a result of Kohl [Koh19, Theorem 1.8].

Theorem 3.3.1 (Kohl)**.** *Let L/K be a finite Galois extension with Galois group G, and let N be a group of the same order of G. 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, then L/K has no Hopf–Galois structures of type N.*

Proof. If L/K has a Hopf–Galois structure of type N, then, by Theorem 3.2.3, there exists an operation $+$ such that $(G, +, \circ)$ is a skew brace with $(G, +) \cong N$, where $\circ$ denotes the original operation of the Galois group G. As every characteristic subgroup of $(G, +)$ is a left ideal of $(G, +, \circ)$, so also a subgroup of $(G, \circ)$, we immediately derive a contradiction. □

Third, we can give a new proof of Corollary 1.4.13, a consequence of Byott's translation, along the lines of the one described in [Chi00, section 7] but without involving regular subgroups. Let L/K be a finite Galois extension with Galois group G, and let N be a group of the same order as G. Recall that we denote by $e(G, N)$ the number of Hopf–Galois structures on L/K of type N and by $f(G, N)$ the number of regular subgroups of $\mathrm{Hol}(N)$ isomorphic to G.

Corollary 3.3.2. *The following equality holds:*

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

Proof. Denote by $\circ$ the group operation of G and by $+$ the group operation on N. By Theorem 3.2.3, the number $e(G,N)$ equals the number of operations $+$ such that $(G,+,\circ)$ is a skew brace with $(G,+)\cong(N,+)$, and by Theorem 3.1.1, the number $f(G,N)$ equals the number of operations $\circ$ such that $(N,+,\circ)$ is a skew brace with $(N,\circ)\cong(G,\circ)$.

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

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

For all $\varphi\in\mathcal{N}$, consider $(G,+_\varphi)$, where as before $+_\varphi$ is the operation obtained by φ via transport of structure, so that $\varphi\colon(N,+)\to(G,+_\varphi)$ is a group 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 from

$$\mathcal{N}'=\{\varphi\in\mathcal{N}\mid (G,+_\varphi,\circ)\text{ is a skew brace}\}$$

to

$$\mathcal{G}'=\{\psi\in\mathcal{G}\mid (N,+,\circ_\psi)\text{ is a skew brace}\}.$$

Note that the right action of $\operatorname{Aut}(N,+)$ on $\mathcal{N}'$ via composition satisfies the following properties:

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

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

Then we can compute the number of Hopf–Galois structures with given skew brace (up to isomorphism); this is [NZ19, Corollary 2.4], and the proof is inspired by that of [KT23, Corollary 3.1].

Corollary 3.3.3. *Let L/K be a finite Galois extension with Galois group G, and let A be a skew brace with $(A,\circ)\cong G$. Then there exist*

$$\frac{|\operatorname{Aut}(G)|}{|\operatorname{Aut}(A)|}$$

Hopf–Galois structures on L/K such that the corresponding skew brace is isomorphic to A.

Proof. Denote by $\circ$ the group operation of G. If $\varphi\colon(A,\circ)\to(G,\circ)$ is a group isomorphism, then we can use φ to construct an operation $+$ such that $(G,+,\circ)$ is a skew brace isomorphic to A, via transport of structure. Denoting by $\mathcal{S}$ the set of the operations $+'$ such that $(G,+',\circ)$ is a skew brace, we need to count how many skew braces in $\mathcal{S}$ are isomorphic to $(G,+,\circ)$; by Theorem 3.2.3, this

is the number we are looking for. There exists an action of $\mathrm{Aut}(G,\circ)$ on $\mathcal{S}$, via transport of structure:

$$\phi\colon +' \mapsto +'_\phi, \quad \sigma +'_\phi \tau = \phi(\phi^{-1}(\sigma) +' \phi^{-1}(\tau)).$$

Then the orbit of $(G,+,\circ)$ under this action consists precisely of the skew braces we need to count. As the stabiliser of $(G,+,\circ)$ under this action is exactly $\mathrm{Aut}(G,+,\circ)$, we derive the assertion. □

Corollary 3.3.3 can also be employed to construct explicitly the Hopf–Galois structures it mentions. Let L/K be a finite Galois extension with Galois group $(G,\circ)$, and for simplicity, consider a skew brace already of the form $(G,+,\circ)$. To find the Hopf–Galois structures on L/K whose corresponding skew brace is isomorphic to $(G,+,\circ)$, it is enough to write a set of representatives

$$\{\phi_1,\dots,\phi_n\} \subseteq \mathrm{Aut}(G,\circ)$$

of the coset space $\mathrm{Aut}(G,\circ)/\mathrm{Aut}(G,+,\circ)$. For every such ϕ_i, we obtain an operation $+_i$ such that $(G,+_i,\circ)$ is a skew brace, where

$$\sigma +_i \tau = \phi_i(\phi_i^{-1}(\sigma) + \phi_i^{-1}(\tau)).$$

In this way, we obtain all the skew braces, and thus the Hopf–Galois structures, we are looking for.

Example 3.3.4. Let L/K be a finite Galois extension with cyclic Galois group $(G,\circ)$ of order p^2, for p an odd prime. Denote by σ a generator of $(G,\circ)$, so that $G = \{\sigma^i \mid i = 0,\dots,p^2-1\}$ and

$$\sigma^i \circ \sigma^j = \sigma^{i+j}.$$

By the results of [Chi96], there are precisely p Hopf–Galois structures on L/K, one of which is the trivial structure. We have constructed, in Example 2.5.16, $p-1$ operations $+$ such that $(G,+,\circ)$ is a nontrivial skew brace, and these give us all the Hopf–Galois structures by Theorem 3.2.3. But suppose that we just have at our disposal (the isomorphism class of) a single skew brace; for example, we can take $(G,+,\circ)$ with

$$\sigma^i + \sigma^j = \sigma^{i+j+pij}.$$

To construct all the other additive operations, we take first

$$\mathrm{Aut}(G,\circ) \cong (\mathbb{Z}/p^2\mathbb{Z})^*,$$

a cyclic group of order $p(p-1)$. Let us take a generic $\phi_d \in \mathrm{Aut}(G,\circ)$, with $d \in (\mathbb{Z}/p^2\mathbb{Z})^*$ and

$$\phi_d(\sigma^i) = \sigma^{id}.$$

We can compute

$$\phi_d(\sigma^i + \sigma^j) = \phi_d(\sigma^{i+j+pij}) = \sigma^{d(i+j+pij)}$$

and

$$\phi_d(\sigma^i) + \phi_d(\sigma^j) = \sigma^{id} + \sigma^{jd} = \sigma^{d(i+j+dpij)}$$

We deduce that $\phi_d \in \mathrm{Aut}(G, +, \circ)$ if and only if $d \equiv 1 \pmod{p}$. As expected, we deduce that the number of Hopf–Galois structures on L/K whose associated skew brace is isomorphic to $(G, +, \circ)$ is

$$\frac{|\operatorname{Aut}(G, \circ)|}{|\operatorname{Aut}(G, +, \circ)|} = p - 1.$$

We see now how to explicitly find these structures. Consider again a map $\phi_d \in \mathrm{Aut}(G, \circ)$, write $\phi_f = \phi_d^{-1}$, and define

$$\sigma^i +_d \sigma^j = \phi_d(\phi_f(\sigma^i) + \phi_f(\sigma^j)) = \sigma^{i+j+fpij}.$$

In this way, we obtain for all $k = 1, \ldots, p-1$ a skew brace $(G, +_k, \circ)$, with

$$\sigma^i +_k \sigma^j = \sigma^{i+j+kpij}.$$

To define explicitly the corresponding Hopf–Galois structure, we need the gamma function of this skew brace: as

$$-\sigma = \sigma^{kp-1},$$

we find

$$^{\gamma(\sigma)}(\sigma^i) = -\sigma + (\sigma \circ \sigma^i) = \sigma^{kp-1} + \sigma^{1+i} = \sigma^{kp+i+kp(kp-1)(1+i)} = \sigma^{i(1-kp)}.$$

We conclude that

$$H = \left\{ \sum_{i=0}^{p^2-1} \ell_i \sigma^i \in L[G, +] \mid \sigma(\ell_i) = \ell_{i(1-kp)} \text{ for all } i \right\}.$$

3.4 The description of the Hopf algebras and their actions

In this section, we explore how we can employ Theorem 3.2.3 to describe explicitly properties of the Hopf–Galois structures in terms of skew braces. First, we just describe the abstract structure of the Hopf algebras appearing; afterwards, we take in consideration their actions and relation with the classical Galois structure.

We fix, for the rest of the section, a finite Galois extension L/K with Galois group $(G, \circ)$, and we consider a Hopf–Galois structure $(H, \cdot)$ on L/K, corresponding by Theorem 3.2.3 to an operation $+$ such that $(G, +, \circ)$ is a skew brace, which we denote by G. In particular, we can assume that

$$H = L[G_+]^{G_\circ} = \left\{ \sum_{\tau \in G} \ell_\tau \tau \in L[G_+] \mid \sigma(\ell_\tau) = \ell_{(^{\gamma(\sigma)}\tau)} \text{ for all } \sigma, \tau \in G \right\}$$

and that the action of H on L is the given as follows:

$$\left(\sum_{\tau\in G}\ell_\tau\tau\right)\cdot x=\sum_{\tau\in G}\ell_\tau\tau(x).$$

3.4.1 The Hopf algebras

We begin by aligning the basic substructures of the skew brace and the Hopf algebra.

Theorem 3.4.1. *There exists a bijective correspondence between*

- *the (strong) left ideals of G;*
- *the (normal) Hopf subalgebras of H.*

Specifically, a (strong) left ideal I of G corresponds to the (normal) Hopf subalgebra $L[I_+]^{(G,\circ)}$ of H.

Proof. By Corollary 1.3.10, the (normal) Hopf subalgebras of $H = L[G_+]^{G_\circ}$ correspond bijectively to the (normal) subgroups of $(G,+)$ invariant under the action of $(G,\circ)$. As this action is given by the gamma function of the skew brace $(G,+,\circ)$, we immediately derive the assertion. □

If in addition I is a strong left ideal of G, then I is a normal $(G,\circ)$-invariant subgroup of $(G,+)$, so $(G,\circ)$ acts on $(G,+)/(I,+)$ via automorphisms. This yields a K-Hopf algebra that we denote by $L[G/I_+]^{G_\circ}$.

Proposition 3.4.2. *Let I be a strong left ideal of G, corresponding to a normal Hopf subalgebra J of H. Then the map*

$$H/J\to L[G/I_+]^{G_\circ},\quad \overline{\sum_{\tau\in G}\ell_\tau\tau}\mapsto\sum_{\tau\in G}\ell_\tau\overline{\tau}$$

is a K-Hopf algebra isomorphism.

Proof. This follows by Corollary 1.3.11. □

A consequence of Theorem 3.2.3 is that we can easily describe the grouplike elements of the Hopf algebras appearing.

Proposition 3.4.3. *The grouplike elements of H are the elements of* $\mathrm{Fix}(G)$.

Proof. By Corollary 1.3.12, the grouplike elements of $L[G_+]^{G_\circ}$ are the elements of $(G,+)$ fixed by the action of $(G,\circ)$. As the action is given by the gamma function of the skew brace $(G,+,\circ)$, the assertion follows. □

Inspired by this result, we can characterise the (strong) left ideals corresponding Hopf subalgebras J such that J or H/J are group algebras.

Proposition 3.4.4. *Let I be a left ideal of G, corresponding to the Hopf subalgebra J of H.*

- *I is contained in $\mathrm{Fix}(G)$ if and only if J is a group algebra.*
- *I has abelian type and is contained in $\mathrm{Fix}(G)$ if and only if J is a commutative group algebra.*

Proof. By Corollary 1.3.12, the Hopf subalgebra $L[I,+]^{(G,\circ)}$ is a group algebra if and only if $(G,\circ)$ acts trivially on $(I,+)$, that is, $(I,+)$ is contained in $\mathrm{Fix}(G)$. In this case, $J = K[I,+]$ is commutative if and only if $(I,+)$ is abelian. □

Proposition 3.4.5. *Let I be a strong left ideal of G, corresponding to the normal Hopf subalgebra J of H.*

- *I contains G^2 if and only if H/J is a group algebra.*
- *I contains $[G,G]$ if and only if H/J is a commutative group algebra.*

Proof. Recall that $H/J \cong L[G/I_+]^{G_\circ}$ as K-Hopf algebras. In particular, by Corollary 1.3.12, the Hopf algebra $L[G/I_+]^{G_\circ}$ is a group algebra if and only if $(G,\circ)$ acts trivially on $(G/I,+)$, that is, if for all $\sigma,\tau \in G$,

$$\sigma * \tau = {}^{\gamma(\sigma)}\tau - \tau \in I,$$

which means that $G^2 \subseteq I$. In this case, $H/J \cong K[G/I_+]$ is abelian if and only if $[G,G]_+ \subseteq I$. As $[G,G] = \langle [G,G]_+,\ G^2\rangle_+$, the assertion follows. □

Proposition 3.4.6. *Suppose that there exist left ideals I and I' of G such that $(G,+)$ is the direct product of $(I,+)$ and $(I',+)$. Then*

$$H \cong L[I_+]^{G_\circ} \otimes_K L[I'_+]^{G_\circ}$$

as K-Hopf algebras.

Proof. This follows by Corollary 1.3.14. □

3.4.2 Their actions

So far, the results seen in this section just describe the structure of the Hopf algebra H, without mentioning its action on the field L. Here we consider the Hopf–Galois structure $(H,\cdot)$ in its entirety.

First, by Theorem 3.4.1, a left ideal I of G identifies an intermediate field L^J of L/K via the Hopf–Galois correspondence, where $J = L[I_+]^{G_\circ}$. This in principle could be confusing, because a left ideal is also a subgroup of the Galois group, so it also identifies an intermediate field L^I via Galois theory. The following result removes ambiguity.

Proposition 3.4.7. *Let I be a left ideal of G, corresponding to the Hopf subalgebra J of H. Then*

$$L^J = L^I.$$

Proof. Recall that $J = L[I_+]^{G_\circ}$. It is clear that if $x \in L^I$, then $x \in L^J$. Indeed, for all $\sum_{\tau\in I} \ell_\tau \tau \in J$,

$$\left(\sum_{\tau\in I} \ell_\tau \tau\right) \cdot x = \sum_{\tau\in I} \ell_\tau \tau(x) = \sum_{\tau\in I} \ell_\tau x = \varepsilon\left(\sum_{\tau\in I} \ell_\tau \tau\right) x.$$

The assertion then follows by Corollary 1.2.8, which implies that

$$[L : L^I] = |I| = \dim_K J = [L : L^J]. \qquad \square$$

This means that a left ideal I of G identifies uniquely an intermediate field of L/K, denoted by L^I, whatever method we choose. In particular, the extension L/L^I is Galois with Galois group $(I, \circ)$ via Galois theory. On the other side, the extension is also $L^I \otimes_K J$-Galois via Hopf–Galois theory, and by Theorem 3.2.3 this Hopf–Galois structure corresponds to an additive operation $+'$ such that $(I, +', \circ)$ is a skew brace. We see now that this operation coincides with the operation $+$ of the left ideal I of G.

Proposition 3.4.8. *The Hopf–Galois structure on L/L^I given by $L^I \otimes_K J$ corresponds to the (additive operation of) the skew brace I.*

Proof. Recall that $J = L[I_+]^{G_\circ}$. First, we claim that the obvious L^I-Hopf algebra map

$$\phi\colon L^I \otimes_K L[I, +]^{(G,\circ)} \to L[I, +]^{(I,\circ)}$$

is a bijection. Equivalently, we can show that

$$\mathrm{id}_L \otimes_{L^I} \phi\colon L \otimes_{L^I} (L^I \otimes_K L[I, +]^{(G,\circ)}) \to L \otimes_{L^I} L[I, +]^{(I,\circ)}$$

is a bijection. This follows by considering the commutative diagram

$$\begin{array}{ccc} L \otimes_{L^I} (L^I \otimes_K L[I_+]^{G_\circ}) & \longrightarrow & L \otimes_{L^I} L[I_+]^{I_\circ} \\ \downarrow & & \downarrow \\ L \otimes_K L[I_+]^{G_\circ} & \longrightarrow & L[I_+] \end{array}$$

where we obtain the arrows via associativity of the tensor products and Galois descent applied to L/L^I.

Finally, note that ϕ respects the action of these Hopf algebras on L, as both can be obtained by the action of $L[G_+]^{G_\circ}$. $\square$

In a slight variation of the proof of this result, we can characterise the trivial left ideals of G.

Proposition 3.4.9. *There exists a bijective correspondence between*

- *the trivial left ideals of G;*
- *the Hopf subalgebras J of H such that $L \otimes_K J$ is a group algebra.*

Proof. Note that $L \otimes_K J$ is a group algebra if and only if $L[I_+]^{I_\circ}$ is a group algebra, if and only if $(I, \circ)$ acts trivially on $(I, +)$, if and only if I is trivial. □

We consider now the ideals of the skew brace G.

Proposition 3.4.10. *There exists a bijective correspondence between*

- *the ideals of G;*
- *the normal Hopf subalgebras J of H such that L^J/K is Galois.*

Proof. It is enough to note that given a strong left ideal I of G, corresponding to the normal Hopf subalgebra $J = L[I_+]^{G_\circ}$ of H, then I is an ideal of G if and only if $(I, \circ)$ is a normal subgroup of $(G, \circ)$, that is, if and only if L^I/K is Galois. As $L^I = L^J$ by Proposition 3.4.7, we derive the assertion. □

When I is an ideal of G, also L^I/K is Galois with Galois group (identified with) $(G/I, \circ)$, and by Hopf–Galois theory, we can consider a Hopf–Galois structure on L/K with Hopf algebra $H/J \cong L[G/I_+]^{G_\circ}$. We show again that the operation on G/I we obtain via Theorem 3.2.3 is the natural one.

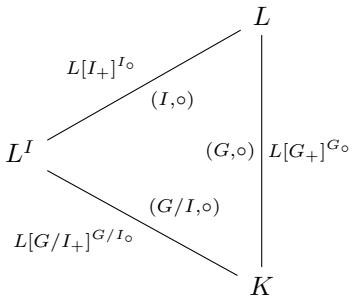
Proposition 3.4.11. *The Hopf–Galois structure on L^I/K with Hopf algebra H/J corresponds to the (additive operation of) the skew brace G/I.*

Proof. First, a simple double inclusion shows that

$$L[G/I_+]^{G_\circ} = L^I[G/I_+]^{G/I_\circ}.$$

As the action of $L^I[G/I_+]^{G/I_\circ}$ on L^I is obtained by the action of $L[G_+]^{G_\circ}$ on L, the assertion follows. □

The following diagram represents the situation described so far:



Remark 3.4.12. If I is a strong left ideal but not an ideal of G, then L^I/K is Hopf–Galois but not Galois; see Proposition 3.4.2 above. On the other side, if I is a strong left ideal of G such that $G^2 \subseteq I$, then reasoning as in the proof of [CSV19, Lemma 1.9], we can deduce that I is also an ideal. In particular, we obtain another proof of the fact that if J is a normal Hopf subalgebra of H such that H/J is a group algebra, then L^J/K is Galois.

We state now three similar results that characterise Hopf–Galois structures corresponding to a skew brace with a suitable property. They can be proved in the same way: the property on the skew brace G identifies an ideal I such that I and G/I have a certain property, and this translates to an normal intermediate field F of L/K in the image of the Hopf–Galois correspondence such that the actions of H on L/F and F/K are controlled by I and G/I, respectively.

Proposition 3.4.13. *The following are equivalent:*

- *G is metatrivial.*
- *There exists an intermediate field F of L/K with the following properties:*
  - *F/K is Galois.*
  - *$F = L^J$, where J is a normal Hopf subalgebra of H.*
  - *The Hopf–Galois structures on L/F and F/K obtained by the action of H on L are the classical structures.*

Proof. The skew brace G is metatrivial if and only there exists an ideal I of G such that I and G/I are trivial, so the result follows translating to information for the Hopf–Galois structure. □

Proposition 3.4.14. *The following are equivalent:*

- *G is left nilpotent of class at most two.*
- *There exists an intermediate field F of L/K with the following properties:*
  - *F/K is Galois.*
  - *$F = L^J$, where J is a normal Hopf subalgebra of H and also a group algebra.*
  - *The Hopf–Galois structures on L/F and F/K obtained by the action of H on L are the classical structures.*

Proof. The skew brace G is left nilpotent of class at most two if and only if $G * G^2 = 0$, and this is equivalent to asking that there exists an ideal I of G such that $I \subseteq \mathrm{Fix}(G)$ and G/I is trivial. Indeed, for one direction one can take $I = G^2$. For the other, if $I \subseteq \mathrm{Fix}(G)$ is an ideal of G such that G/I is trivial, then $G^2 \subseteq I \subseteq \mathrm{Fix}(G)$, that is $G * G^2 = 0$.

The result then follows translating this information to the Hopf–Galois structure. □

Proposition 3.4.15. *The following are equivalent:*

- *G is metabelian.*
- *There exists an intermediate field F of L/K with the following properties:*
  - *F/K is an abelian extension.*

– *$F = L^J$, where J is a normal commutative Hopf subalgebra of H such that H/J is commutative.*

– *The Hopf–Galois structures on L/F and F/K obtained by the action of H on L are the classical structures.*

Proof. The skew brace G is metatrivial if and only there exists an ideal I of G such that I and G/I are abelian, so the result follows translating this information to the Hopf–Galois structure. □

Finally, we describe the behaviour of a Hopf–Galois structure in a particularly nice situation: when the skew brace is a (semi)direct product.

Proposition 3.4.16. *Suppose that G is isomorphic to a semidirect product of skew braces. Then there exist an ideal I and a left strong ideal I' of G such that the following hold:*

- *There exists a K-Hopf algebra isomorphism*

$$L[G_+]^{G_\circ} \cong L[I_+]^{G_\circ} \otimes_K L[I'_+]^{G_\circ}.$$

- *The group $(G, \circ)$ is the semidirect product of $(I, \circ)$ and $(I', \circ)$. In particular, the obvious map $\varphi\colon (I', \circ) \to (G/I, \circ)$ is a group isomorphism.*

- *The Hopf–Galois structure on L^I/K given by the pair (I', φ) corresponds to the additive operation of the skew brace G/I.*

- *There exists an $L^{I'}$-Hopf algebra isomorphism*

$$L^{I'} \otimes_K L^I[G/I_+]^{G/I_\circ} \cong L[I'_+]^{I'_\circ}.$$

If the semidirect product is also direct, then also I' is an ideal, the group $(G, \circ)$ is the direct product of $(I, \circ)$ and $(I', \circ)$, and the previous results also hold switching the roles of I and I'.

Proof. Denote by A and A' the skew braces such that there exists a skew brace isomorphism

$$\phi\colon A \rtimes A' \to G.$$

We take $I = \phi(A \rtimes 0)$ and $I' = \phi(0 \rtimes A')$, which are easily checked to be respectively an ideal and a strong left ideal of G. The first two items then immediately follow.

For the third, we know that the Hopf–Galois structure on L^I/K obtained by the action of H on L corresponds to the (additive operation of) the skew brace G/I. As the group isomorphism

$$\varphi\colon (I', \circ) \to (G/I, \circ)$$

is also a skew brace isomorphism

$$\varphi\colon I' \to G/I$$

the assertion follows.

The $L^{I'}$-Hopf algebra isomorphism

$$L^{I'} \otimes_K L^I[G/I_+]^{G/I_\circ} \cong L[I'_+]^{I'_\circ}$$

can be obtained tensoring with L and reasoning exactly as in the proof of Proposition 3.4.8.

Finally, the last claim on the direct product immediately follows as in this case also $0 \times A'$ is an ideal of $A \times A'$. □

3.5 The Hopf–Galois correspondence

In this section, we employ the description of Theorem 3.2.3 to study the Hopf–Galois correspondence for Hopf–Galois structures on Galois extensions. We follow [ST23b, section 4].

3.5.1 First consequences and examples

Let L/K be a finite Galois extension with Galois group $(G, \circ)$. We begin by showing how a skew brace can be employed to control the image of the Hopf–Galois correspondence. From now on, to lighten the notation, we say that a Hopf–Galois structure on L/K corresponds to a skew brace $(G, +, \circ)$, rather than an operation $+$ such that $(G, +, \circ)$ is a skew brace, via Theorem 3.2.3.

Theorem 3.5.1. *Let $(H, \cdot)$ be a Hopf–Galois structure on L/K, corresponding to the skew brace $(G, +, \circ)$.*

- *An intermediate field F of L/K is in the image of the Hopf–Galois correspondence if and only if the subgroup T of $(G, \circ)$ corresponding to F via Galois theory is a left ideal of $(G, +, \circ)$.*
- *The equality*

$$\mathrm{HGC}(L/K, H) = \frac{|\{\textit{left ideals of } (G, +, \circ)\}|}{|\{\textit{subgroups of } (G, \circ)\}|}$$

  holds.

In particular, the Hopf–Galois correspondence for $(H, \cdot)$ is bijective if and only if every subgroup of $(G, \circ)$ is a left ideal of $(G, +, \circ)$.

Proof. By Theorem 3.4.1, there exists a bijective correspondence between

- the left ideals of $(G, +, \circ)$;
- the intermediate field of L/K in the image of the Hopf–Galois correspondence.

By Proposition 3.4.7, if I is a left ideal of $(G, +, \circ)$, then the corresponding intermediate field is the one that is associated with $(I, \circ)$ by Galois theory, and thus the assertion follows. □

Example 3.5.2. Consider the classical structure on L/K, corresponding to the trivial 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 the classical structure is bijective.

Example 3.5.3. Suppose that $(G, \circ)$ is cyclic of order $2n$, where $n \geq 3$ is odd, and consider the Hopf–Galois structure as in Example 3.2.9. In this case, if σ is a generator of $(G, \circ)$ and $\tau \in G$, then the gamma function of the skew brace $(G, +, \circ)$ satisfies

$$\gamma(\sigma)_\tau = \tau^{-1}.$$

In particular, every subgroup of $(G, \circ)$ is a left ideal of $(G, +, \circ)$. We deduce that the Hopf–Galois structure found in this way has a bijective Hopf–Galois correspondence.

Note that this example can be generalised to every Galois extension with Galois group G isomorphic to a direct product of an abelian group and a cyclic group of order 2; see [ST23b, Example 4.8].

As an application of Theorem 3.5.1, we can see that the behaviour of the canonical nonclassical structure (Theorem 1.4.9) can be assumed also by other Hopf–Galois structures.

Proposition 3.5.4. *Consider a Hopf–Galois structure $(H, \cdot)$ on L/K such that the gamma function of the corresponding skew brace $(G, +, \circ)$ satisfies $\gamma(G) \subseteq \mathrm{Inn}(G, \circ)$. Then every normal intermediate field K of L/K is in the image of the Hopf–Galois correspondence for $(H, \cdot)$. If in addition $\gamma(G) = \mathrm{Inn}(G, \circ)$, then the image of the Hopf–Galois correspondence for $(H, \cdot)$ consists precisely of the normal intermediate fields of L/K.*

Proof. If $\gamma(G) \subseteq \mathrm{Inn}(G, \circ)$, then every normal subgroup of $(G, \circ)$ is a left ideal of $(G, +, \circ)$, that is, every normal intermediate field is in the image of the Hopf–Galois correspondence.

Clearly, if $\gamma(G) = \mathrm{Inn}(G, \circ)$, then the left ideals of $(G, +, \circ)$ are exactly the normal subgroups of $(G, \circ)$, that is, the image of the Hopf–Galois correspondence for $(H, \cdot)$ consists precisely of the normal intermediate fields of L/K. □

Remark 3.5.5. By [CCDC20, table at page 1175], one can show that a skew brace A is a bi-skew brace if and only if $\gamma(A) \subseteq \mathrm{Aut}(A, \circ)$. In particular, a skew brace $(G, +, \circ)$ satisfies the first assumption of Proposition 3.5.4 if and only if $(G, +, \circ)$ is a bi-skew brace and $(G, \circ, +)$ is inner.

Example 3.5.6. Consider the canonical nonclassical structure on L/K, corresponding to the almost trivial skew brace $(G, \circ_{\mathrm{op}}, \circ)$. Here $\gamma(\sigma) = \iota_\circ(\sigma)$ for all $\sigma \in G$. Applying Proposition 3.5.4, we recover the fact that that the image of the Hopf–Galois correspondence for this structure consists precisely of the normal intermediate fields of L/K.

Example 3.5.7. Suppose that $(G, \circ)$ is nilpotent of class two, consider a group homomorphism $\psi\colon (G, \circ) \to (G, \circ)$, and define

$$\sigma + \tau = \sigma \circ {}^{\iota_\circ(\psi(\sigma))}\tau = \sigma \circ \psi(\sigma) \circ \tau \circ \psi(\sigma)^{-1}.$$

As showed in Corollary 2.5.11, we obtain a skew brace $(G, +, \circ)$ with gamma function given by $\gamma(\sigma) = \iota_\circ(\psi(\sigma))^{-1} = \iota_\circ(\psi(\sigma)^{-1})$. By Proposition 3.5.4, we obtain a Hopf–Galois structure on L/K such that the normal intermediate fields of L/K are in the image of the Hopf–Galois correspondence.

If in addition ψ is surjective (for example, $\psi = \mathrm{id}$), then the image of the Hopf–Galois correspondence consists precisely of the normal intermediate fields of L/K.

Finally, take $\psi = \mathrm{id}$; 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 examples, for the Heisenberg group of order p^3, with p an odd prime.

We conclude this subsection with two easy observations.

Remark 3.5.8. Let L/K be a finite Galois extension with Galois group G, and let $(H, \cdot)$ be a Hopf–Galois structure on L/K of type N. As immediate consequence of Theorem 3.5.1, if N has less subgroups than G, then the Hopf–Galois correspondence for $(H, \cdot)$ is not bijective.

Remark 3.5.9. Let L/K be a finite Galois extension with Galois group $(G, \circ)$, and let $(G, +, \circ)$ be a skew brace, corresponding to the Hopf–Galois structure $(H, \cdot)$ on L/K. If the skew brace $(G, +, \circ)$ is isomorphic a direct product of skew braces A_i of coprime order and for all i, every subgroup of $(A_i, \circ)$ is a left ideal of A_i, then every subgroup of $(G, \circ)$ is a left ideal of $(G, +, \circ)$. In particular, $(H, \cdot)$ has a bijective Hopf–Galois correspondence by Theorem 3.5.1.

3.5.2 An explicit construction

We can propose a concrete recipe to obtain Hopf–Galois structures with a bijective Hopf–Galois correspondence. Let L/K be a finite Galois extension with Galois group $(G, \circ)$, and denote by $Z(G)$ its centre and by $N(G)$ its *norm*, which is the intersection of the normalisers of the subgroup of $(G, \circ)$. The quotient $N(G)/Z(G)$ is abelian; this follows, for example, by [Sch60, Theorem], where it was stated that $N(G)$ is contained in the second centre of $(G, \circ)$. This means that we can apply Corollary 2.5.6 to deduce that every group homomorphism

$$\phi\colon (G, \circ) \to N(G)/Z(G)$$

can be used to construct a bi-skew brace $(G, \circ, +)$, where

$$\sigma + \tau = \sigma \circ \psi(\sigma) \circ \tau \circ \psi(\sigma)^{-1}.$$

Here $\psi\colon G \to G$ is any map that satisfies

$$\psi(\sigma) \circ Z(G) = \phi(\sigma).$$

As the gamma function of this skew brace is given by $\gamma(\sigma) = \iota_\circ(\psi(\sigma))$, we find that the gamma function of $(G, +, \circ)$ is given by

$$\sigma \mapsto \iota_\circ(\psi(\sigma))^{-1} = \iota_\circ(\psi(\sigma)^{-1}).$$

In particular, every subgroup T of $(G, \circ)$ is a left ideal of $(G, +, \circ)$, as $\psi(\sigma)^{-1}$ belongs to the normaliser of T by definition of $N(G)$. We obtain in this way a Hopf–Galois structure $(H, \cdot)$ on L/K with a bijective Hopf–Galois correspondence; explicitly,

$$H = \left\{ \sum_{\tau \in G} \ell_\tau \tau \in L[G_+] \mid \sigma(\ell_\tau) = \ell_{\psi(\sigma)^{-1} \circ \tau \circ \psi(\sigma)} \text{ for all } \sigma, \tau \in G \right\}.$$

Finally, different group homomorphisms ϕ yield different operations $+$, again by Corollary 2.5.6, and therefore this discussion implies the following result.

Theorem 3.5.10. *Let L/K be a finite Galois extension with Galois group G. Then there exists an injective correspondence from the group homomorphisms $\psi\colon G \to N(G)/Z(G)$ to the Hopf–Galois structures on L/K with a bijective Hopf–Galois correspondence.*

Remark 3.5.11. In [ST23b, section 4], it was underlined how this construction may be seen as an application of the behaviour of the power automorphisms of a group.

Example 3.5.12. Let L/K be a finite Galois extension with Galois group G isomorphic Q_8, the quaternion group of order 8. There are 22 Hopf–Galois structures on L/K, and 6 of them are of cyclic type; see [SV18, Table 2]. As G 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 with a bijective Hopf–Galois correspondence. We find indeed all the Hopf–Galois structures on L/K except for the 6 of cyclic type, for which the Hopf–Galois correspondence is not bijective by Remark 3.5.8.

Example 3.5.13. Let L/K be a finite Galois extension with Galois group G isomorphic to the nonabelian group of order p^3 and exponent p^2, where p is an odd prime. One can check that $N(G)$ is the elementary abelian subgroup of G of order p^2, while the centre is the cyclic of order p. As there are p^2 distinct group homomorphisms

$$G \to C_p,$$

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

3.5.3 Bi-skew braces

We deal now with some results related to bi-skew braces, again following [ST23b, section 4]. First, we can give a peculiar characterisation of cyclic groups. We need a technical lemma.

Lemma 3.5.14. *Let L/K be a Galois extension with Galois group G isomorphic to a direct product of groups $T \times T'$. Suppose that there exists a skew brace A such that $(A, \circ) \cong T$ and not every subgroup of $(A, \circ)$ is a left ideal of A. Then there exists a Hopf–Galois structure on L/K with a nonbijective Hopf–Galois correspondence.*

Proof. Consider the direct product of skew braces $B = A \times \mathrm{Triv}(T')$. By assumption, not every subgroup of $(B, \circ)$ is a left ideal of B. As $(B, \circ) \cong G$, we obtain a Hopf–Galois structure on L/K by Theorem 3.2.11, and by Theorem 3.5.1, this Hopf–Galois structure has a nonbijective Hopf–Galois correspondence. □

The following result is contained in the proof of [ST23b, Theorem 4.24].

Theorem 3.5.15. *Let L/K be a finite Galois extension with Galois group $(G, \circ)$. Then the following are equivalent:*

- *The group $(G, \circ)$ is cyclic.*
- *Every Hopf–Galois structure on L/K whose corresponding skew brace $(G, +, \circ)$ is a bi-skew brace has a bijective Hopf–Galois correspondence.*

Proof. Suppose first that $(G, \circ)$ is cyclic. If $(G, +, \circ)$ is a bi-skew brace, then every subgroup of $(G, \circ)$ is a left ideal, as every subgroup of a cyclic group is characteristic and the gamma function of $(G, +, \circ)$ take values in $\mathrm{Aut}(G, \circ)$. This immediately yields one direction by Theorem 3.5.1.

We assume now that every Hopf–Galois structure on L/K whose corresponding skew brace $(G, +, \circ)$ is a bi-skew brace has a bijective Hopf–Galois correspondence. As the canonical nonclassical structure corresponds to an almost trivial skew brace, which is a bi-skew brace, we can derive by Example 3.5.6 that $(G, \circ)$ has to be abelian or Hamiltonian. We proceed by exclusion. If $(G, \circ)$ is Hamiltonian, then there exists an abelian group T such that $(G, \circ)$ is isomorphic to the direct product of the quaternion group Q_8 and T, as stated in [Hal59, Theorem 12.5.4]. By Example 2.5.4 and Remark 3.5.8, we obtain a skew brace A with $(A, \circ) \cong Q_8$ such that not every subgroup of $(A, \circ)$ is a left ideal. By Lemma 3.5.14, we derive a contradiction.

This means that $(G, \circ)$ is abelian. Suppose that $(G, \circ)$ is not cyclic. Then there exist a prime p and an abelian group T such that $(G, \circ)$ is isomorphic to a direct product of the form $\mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/p^s\mathbb{Z} \times T$, where $1 \leq s \leq r$. As in Example 2.5.18, there exists a skew brace $(\mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/p^s\mathbb{Z}, \circ, +)$, where $+$ is the usual operation on the direct product of cyclic groups and

$$(i, j) \circ (a, b) = (i + a, j + b + ia).$$

Note that the subgroup $\{(i,0) \mid i = 0,\dots,p^r-1\}$ of $(\mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/p^s\mathbb{Z}, +)$ is not a subgroup of $(\mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/p^s\mathbb{Z}, \circ)$, so in particular it is not a left ideal of $(\mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/p^s\mathbb{Z}, \circ, +)$. Again by Lemma 3.5.14, we find a contradiction. □

We discuss now a question posed in [Chi21]. Let L/K and L'/K' be finite Galois extensions with Galois group G and G', respectively. Suppose that A is a bi-skew brace such that there exist group isomorphisms $\varphi\colon (A,\circ) \to G$ and $\varphi'\colon (A,+) \to G'$. Then, by Theorem 3.2.11, the pair (A,φ) yields a Hopf–Galois structure $(H,\cdot)$ on L/K, and the pair $(A_{\leftrightarrow},\varphi)$ yields a Hopf–Galois structure $(H',\cdot)$ on L'/K'. In [Chi21], it was inquired whether these two Hopf–Galois structures are related in some way. In principle, it may seem difficult to give a positive answers, as the Hopf algebras are defined over different fields. However, the relation between the two underlying skew braces of a bi-skew brace has the following implication.

Theorem 3.5.16. *There exists a bijective correspondence between*

- *the Hopf subalgebras of H;*
- *the Hopf subalgebras of H'.*

There is the same number of intermediate fields in the images of the Hopf–Galois correspondence for $(H,\cdot)$ and $(H',\cdot)$ on L/K and L'/K', respectively, and the following equality holds:

$$\frac{\mathrm{HGC}(L/K,H)}{\mathrm{HGC}(L'/K',H')} = \frac{|\{\textit{subgroups of } G'\}|}{|\{\textit{subgroups of } G\}|}.$$

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

Proof. Denote by $\circ$ the group operation of G and by $\circ'$ the group operation of G'. The pair (A,φ) yields a Hopf–Galois structure on L'/K' via Theorem 3.2.11, and this corresponds to a skew brace $(G,+,\circ)$. Similarly, the pair $(A_{\leftrightarrow},\varphi)$ yields a Hopf–Galois structure on L/K via Theorem 3.2.11, and this corresponds to a skew brace $(G,+',\circ')$. In particular, there exists a bijective correspondence between the left ideals of A and $(G,+,\circ)$, and the same for those of $A_{\leftrightarrow}$ and $(G',+',\circ')$. By Lemma 2.2.24, we know that the left ideals of A and $A_{\leftrightarrow}$ coincide. The result then follows by Theorem 3.5.1. □

Example 3.5.17. Take an odd prime p, let L/K be a Galois extension with dihedral Galois group G of order $2p$, and let L'/K' be a Galois extension with cyclic Galois group G' of order $2p$.

Consider the bi-skew brace $A = \mathrm{Triv}(C_p) \rtimes \mathrm{Triv}(C_2)$ of Example 2.2.23, where C_2 acts on C_p via inversion. Then $(A,+)$ is cyclic of order $2p$ and $(A,\circ)$ is dihedral of order $2p$. Once we fix group isomorphisms $\varphi\colon (A,\circ) \to G$ and $\varphi'\colon (A,+) \to G'$, we obtain a Hopf–Galois structure $(H,\cdot)$ on L/K and a Hopf–Galois structure $(H',\cdot)$ on L'/K' by Theorem 3.2.11. Exactly as shown in Example 3.5.3, every subgroup of $(A,+)$ is a left ideal of A. As there are $p+3$

subgroups of G and 4 subgroups of G', and as every subgroup of $(A, \circ)$ is a left ideal of A, we derive the following equalities:

$$\begin{aligned} \mathrm{HGC}(L/K, H) &= \frac{4}{p+3}, \\ \mathrm{HGC}(L'/K', H') &= 1, \\ \frac{\mathrm{HGC}(L/K, H)}{\mathrm{HGC}(L'/K', H')} &= \frac{4}{p+3}. \end{aligned}$$

3.5.4 Childs's property

We fix a finite Galois extension L/K with Galois group G. Motivated by the behaviour of cyclic extensions of odd prime power degree, we give the following definition.

Definition 3.5.18. The extension L/K satisfies *Childs's property* if every Hopf–Galois structure on L/K has a bijective Hopf–Galois correspondence.

The goal of this part is to classify entirely extensions with Childs's property, by stating and proving [ST23b, Theorem 4.24]. We begin with an easy proposition.

Proposition 3.5.19. *Consider a Hopf–Galois structure $(H, \cdot)$ on L/K of type N. Suppose that the number of characteristic subgroups of N is greater than or equal to the number of subgroups of G. Then these numbers coincide and $(H, \cdot)$ has a bijective Hopf–Galois correspondence.*

Proof. Denote by $\circ$ the group operation of G. The Hopf–Galois structure $(H, \cdot)$ corresponds by Theorem 3.2.3 to a skew brace $(G, +, \circ)$, where $N \cong (G, +)$. As every characteristic subgroup of $(G, +)$ is a left ideal of $(G, +, \circ)$ and thus also a subgroup of $(G, \circ)$, we deduce by assumption that the numbers of characteristic subgroups of N and of subgroups of G coincide, and that every subgroup of $(G, \circ)$ is a left ideal of $(G, +, \circ)$, and therefore $(H, \cdot)$ has a bijective Hopf–Galois correspondence by Theorem 3.5.1. □

As a consequence, we can first recover [Chi17, Proposition 4.3], (see Proposition 3.1.7 above), and then complete it considering also groups with even order; see [ST23b, Example 4.21].

Corollary 3.5.20 (Childs)**.** *Suppose that G is cyclic of odd prime power order. Then L/K satisfies Childs's property.*

Proof. Let $(H, \cdot)$ be a Hopf–Galois structure of type N on L/K. As stated in [Koh98, Theorem 4.5], also N is cyclic, so by Proposition 3.5.19, we conclude that $(H, \cdot)$ has a bijective Hopf–Galois correspondence. □

Proposition 3.5.21. *Suppose that G is cyclic of order 2^m, where $m \geq 1$. Then L/K satisfies Childs's property.*

Proof. Denote by $\circ$ the group operation of G. Let $(H, \cdot)$ be a Hopf–Galois structure of type N on L/K, corresponding to a skew brace $(G, +, \circ)$ by Theorem 3.2.3 (in particular, $(G, +) \cong N$).

If $m = 1, 2$, then both operations of $(G, +, \circ)$ are abelian, so $(G, +, \circ)$ arises from a radical ring. By Example 2.2.12, we get that $(G, +, \circ)$ is a bi-skew brace, so the result follows by Theorem 3.5.15.

Suppose now that $m \geq 3$. As proved in [Byo07, Theorem 6.1], the type N of the extension is cyclic, dihedral, or (generalised) quaternion.

- If N is cyclic, then the numbers of characteristic subgroups of N and subgroups of G coincide, so we conclude by Proposition 3.5.19.

- If N is dihedral with presentation

$$\langle r, s \mid r^{2^m-1} = 1,\ s^2 = 1,\ srs^{-1} = r^{-1} \rangle,$$

  then the subgroup generated by r is a characteristic cyclic subgroup of order 2^{m-1} (for example because every element outside of it has order 2), and also its subgroups are characteristic in N. We find in this way $m+1$ characteristic subgroups of N (counting also N), and as this number equals the number of subgroups of G, we conclude by Proposition 3.5.19.

- If N is a generalised quaternion group with presentation

$$\langle x, y \mid x^{2^m-1} = 1,\ x^{2^{m-2}} = y^2,\ yxy^{-1} = x^{-1} \rangle,$$

  then, with the only exception $m = 3$, the subgroup generated by x is a characteristic cyclic subgroup of order 2^{m-1} (as it can be checked to be the centraliser of the commutator subgroup $\langle x^2 \rangle$ of N), and also its subgroups are characteristic in N. We find in this way $m+1$ characteristic subgroups of N (counting also N), and as this number equals the number of subgroups of G, we conclude by Proposition 3.5.19.

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

Remark 3.5.22. With the classification given in [Bac15] one can construct a skew brace A with $(A, \circ)$ cyclic of order p^3, where p is a prime, such that A is not a bi-skew brace. Thus Corollary 3.5.20 and Proposition 3.5.21 do not follow by Theorem 3.5.15.

We finally arrive at the main result.

Theorem 3.5.23. *Let L/K be a finite Galois extension with Galois group G. Then the following are equivalent:*

- *The extension L/K satisfies Childs's property.*

- *The group G is cyclic, and if p and q are prime divisors of the order of G, then p does not divide $q-1$.*

Proof. Suppose first that G is cyclic, of order n and if p and q are prime divisors of the order of G, then p does not divide $q-1$. If n in even, then n needs to be a power of 2; therefore the result follows by Proposition 3.5.21.

Suppose instead that n is odd, and take a Hopf–Galois structure $(H,\cdot)$ of type N, corresponding to a skew brace $(G,+,\circ)$. By [Tsa22, Corollary 1.6], $N \cong (G,+)$ is isomorphic to a semidirect product of cyclic groups $\mathbb{Z}/a\mathbb{Z} \rtimes \mathbb{Z}/b\mathbb{Z}$, where a and b are coprime and $ab = n$. By the assumption on the divisors of the order of G, this semidirect product is necessarily a direct product. In particular, we find that $(G,+)$ is cyclic, and we can apply [CSV19, Corollary 4.3] (which is [Byo13, Theorem 1] in the context of skew braces) to deduce that $(G,+,\circ)$ is isomorphic to a direct product of skew braces A_i of coprime odd prime power order. Since every subgroup of $(A_i,\circ)$ is a left ideal of A_i, as shown in the proof of Corollary 3.5.20, we conclude by Remark 3.5.9 that every subgroup of $(G,\circ)$ is a left ideal of $(G,+,\circ)$, deriving the assertion.

Conversely, suppose that L/K satisfies Childs's property. By Theorem 3.5.15, G needs to be cyclic. Suppose that there exist primes p and q dividing the order of G such that p divides $q-1$. Consider the Sylow q-subgroup Q and the Sylow p-subgroup P of G. By assumption on p and q, we can construct a nontrivial semidirect product $(A,+)$ of Q and P. So we consider the skew brace A, where instead $(A,\circ)$ is the direct product of Q and P (see Example 2.2.23). Note that G is the direct product of all its Sylow subgroups. If the subgroup $1 \times P$ of $(A,\circ)$ is not a left ideal of A, then we can apply Lemma 3.5.14 to derive a contradiction. If instead $1 \times P$ is a left ideal of A, then $1 \times P$ is not a left ideal of A_{op}, because otherwise $1 \times P$ would be a normal subgroup of $(A,+)$. Again, we find a contradiction by Lemma 3.5.14. □

3.6 A take-home theorem

In the previous sections, we have started from a finite Galois extension L/K with Galois group $(G,\circ)$ and a Hopf–Galois structure $(H,\cdot)$ on L/K, obtained a skew brace $(G,+,\circ)$ by Theorem 3.2.3, and we have obtained various results regarding the properties of H and the Hopf–Galois correspondence of $(H,\cdot)$. However, as already mentioned, one can also start from a totally abstract skew brace A and obtain a Hopf–Galois structure on every finite Galois extension L/K with Galois group $G \cong (A,\circ)$, once a group isomorphism is chosen, by Theorem 3.2.11.

We conclude this chapter with a final result, which summarises many of the ones developed so far, in a way that captures both the aforementioned approaches. Its proof follows by Theorem 3.2.11, together with the appropriate results given in the context of Theorem 3.2.3.

Theorem 3.6.1. *If A is a skew brace, then we can associate with A, on every Galois extension L/K with Galois group $G \cong (A,\circ)$, a Hopf–Galois structure*

$(H, \cdot)$.

Conversely, if $(H, \cdot)$ is a Hopf–Galois structure on a finite Galois extension L/K with Galois group G, then we can associate with $(H, \cdot)$ a skew brace A with $(A, \circ) \cong G$.

The data associated in either of these ways satisfy the following properties.

1. *The type of $(H, \cdot)$ is $(A, +)$. In particular, $L \otimes_K H \cong L[A, +]$ as L-Hopf algebras.*
2. *A is (almost) trivial if and only if $(H, \cdot)$ is the (canonical non)classical structure.*
3. *There exists a bijective correspondence between*
   - *the (strong) left ideals of A;*
   - *the (normal) Hopf subalgebras of H.*
4. *There exists a bijective correspondence between*
   - *the elements of $\mathrm{Fix}(A)$;*
   - *the grouplike elements of H.*
5. *There exists a bijective correspondence between*
   - *the trivial left ideals of A;*
   - *the Hopf subalgebras J of H such that $L \otimes_K J$ is a group algebra.*
6. *There exists a bijective correspondence between*
   - *the left ideals of A contained in $\mathrm{Fix}(A)$;*
   - *the Hopf subalgebras of H that are group algebras.*
7. *There exists a bijective correspondence between*
   - *the abelian left ideals of A;*
   - *the commutative Hopf subalgebras J of H such that $L \otimes_K J$ is a group algebra.*
8. *There exists a bijective correspondence between*
   - *the abelian left ideals of A contained in $\mathrm{Fix}(A)$;*
   - *the commutative Hopf subalgebras of H that are group algebras.*
9. *There exists a bijective correspondence between*
   - *the strong left ideals A that contain A^2;*
   - *the normal Hopf subalgebras J of H such that H/J is a group algebra*
10. *There exists a bijective correspondence between*

- *the strong left ideals A that contain $[A, A]$;*
- *the normal Hopf subalgebras J of H such that H/J is a commutative group algebra.*

11. *There exists a bijective correspondence between*
    - *the ideals of A;*
    - *the normal Hopf subalgebras J of H such that L/L^J is Galois.*
12. *If A is a (semi)direct product of skew braces, then H is a tensor product of Hopf algebras and G is a (semi)direct product of groups.*
13. *The Hopf–Galois correspondence for $(H, \cdot)$ is bijective if and only if every subgroup of $(A, \circ)$ is a left ideal of A.*
14. *Every normal intermediate field of L/K is in the image of the Hopf–Galois correspondence for $(H, \cdot)$ if and only if every normal subgroup of $(A, \circ)$ is a left ideal of A. In particular, this is the case when A is a bi-skew brace and $A_{\leftrightarrow}$ is inner.*

Bibliography

[AB20] E. Acri and M. Bonatto, *Skew braces of size pq*, Comm. Algebra **48** (2020), no. 5, 1872–1881. MR 4085764

[AB21] Ali A. Alabdali and Nigel P. Byott, *Skew braces of squarefree order*, J. Algebra Appl. **20** (2021), no. 7, Paper No. 2150128, 21. MR 4269712

[AD95a] Bernhard Amberg and Oliver Dickenschied, *On the adjoint group of a radical ring*, Canad. Math. Bull. **38** (1995), no. 3, 262–270. MR 1347297

[AD95b] N. Andruskiewitsch and J. Devoto, *Extensions of Hopf algebras*, Algebra i Analiz **7** (1995), no. 1, 22–61. MR 1334152

[Bac15] David Bachiller, *Classification of braces of order p^3*, J. Pure Appl. Algebra **219** (2015), no. 8, 3568–3603. MR 3320237

[Bac16] ———, *Counterexample to a conjecture about braces*, J. Algebra **453** (2016), 160–176. MR 3465351

[Bac18] ———, *Solutions of the Yang–Baxter equation associated to skew left braces, with applications to racks*, J. Knot Theory Ramifications **27** (2018), no. 8, 1850055, 36. MR 3835326

[BBERJSPC23] Adolfo Ballester-Bolinches, Ramón Esteban-Romero, Paz Jiménez-Seral, and Vicent Pérez-Calabuig, *On solubility of skew left braces and solutions of the Yang-Baxter equation*, arXiv:2304.13475, 2023.

[BC12] Nigel P. Byott and Lindsay N. Childs, *Fixed-point free pairs of homomorphisms and nonabelian Hopf–Galois structures*, New York J. Math. **18** (2012), 707–731. MR 2991421

[BFP23] Dominique Bourn, Alberto Facchini, and Mara Pompili, *Aspects of the category SKB of skew braces*, Comm. Algebra **51** (2023), no. 5, 2129–2143. MR 4561474

[BG22] Valeriy G. Bardakov and Vsevolod Gubarev, *Rota—Baxter groups, skew left braces, and the Yang—Baxter equation*, J. Algebra **596** (2022), 328–351. MR 4370524

[BJ23] Marco Bonatto and Přemysl Jedlička, *Central nilpotency of skew braces*, J. Algebra Appl. **22** (2023), no. 12, Paper No. 2350255. MR 4663905

[BML22] Nigel P. Byott and Isabel Martin-Lyons, *Hopf-Galois structures on non-normal extensions of degree related to Sophie Germain primes*, J. Pure Appl. Algebra **226** (2022), no. 3, Paper No. 106869, 20. MR 4295182

[BNY22] Valeriy G. Bardakov, Mikhail V. Neshchadim, and Manoj K. Yadav, *On λ-homomorphic skew braces*, J. Pure Appl. Algebra **226** (2022), no. 6, Paper No. 106961, 37. MR 4346001

[Byo96] N. P. Byott, *Uniqueness of Hopf Galois structure for separable field extensions*, Comm. Algebra **24** (1996), no. 10, 3217–3228. MR 1402555

[Byo97] Nigel 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

[Byo02] ———, *Integral Hopf–Galois structures on degree p^2 extensions of p-adic fields*, J. Algebra **248** (2002), no. 1, 334–365. MR 1879021

[Byo04] ———, *Hopf-Galois structures on Galois field extensions of degree pq*, J. Pure Appl. Algebra **188** (2004), no. 1-3, 45–57. MR 2030805

[Byo07] ———, *Hopf–Galois structures on almost cyclic field extensions of 2-power degree*, J. Algebra **318** (2007), no. 1, 351–371. MR 2363137

[Byo13] ———, *Nilpotent and abelian Hopf–Galois structures on field extensions*, J. Algebra **381** (2013), 131–139. MR 3030514

[Byo15] ———, *Solubility criteria for Hopf–Galois structures*, New York J. Math. **21** (2015), 883–903. MR 3425626

[Car20] A. Caranti, *Bi-skew braces and regular subgroups of the holomorph*, J. Algebra **562** (2020), 647–665. MR 4130907

[CCDC20] 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

[CCDC24] ———, *Hopf-Galois structures on extensions of degree p^2q and skew braces of order p^2q: the elementary abelian Sylow p-subgroup case*, New York J. Math. **30** (2024), 93–186. MR 4709044

[CCS19] Francesco Catino, Ilaria Colazzo, and Paola Stefanelli, *Skew left braces with non-trivial annihilator*, J. Algebra Appl. **18** (2019), no. 2, 1950033, 23. MR 3917122

[Ced18] Ferran Cedó, *Left braces: solutions of the Yang-Baxter equation*, Adv. Group Theory Appl. **5** (2018), 33–90. MR 3824447

[CGK+21] Lindsay N. Childs, Cornelius Greither, Kevin P. Keating, Alan Koch, Timothy Kohl, Paul J. Truman, and Robert G. Underwood, *Hopf Algebras and Galois Module Theory*, Mathematical Surveys and Monographs, vol. 260, American Mathematical Society, Providence, RI, [2021] ©2021. MR 4390798

[Chi89] Lindsay N. Childs, *On the Hopf Galois theory for separable field extensions*, Comm. Algebra **17** (1989), no. 4, 809–825. MR 990979

[Chi96] ———, *Hopf Galois structures on degree p^2 cyclic extensions of local fields*, New York J. Math. **2** (1996), 86–102. MR 1420597

[Chi00] ———, *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory*, Mathematical Surveys and Monographs, vol. 80, American Mathematical Society, Providence, RI, 2000. MR 1767499

[Chi17] ———, *On the Galois correspondence for Hopf Galois structures*, New York J. Math. **23** (2017), 1–10. MR 3611070

[Chi18] ———, *Skew braces and the Galois correspondence for Hopf Galois structures*, J. Algebra **511** (2018), 270–291. MR 3834774

[Chi19] ———, *Bi-skew braces and Hopf Galois structures*, New York J. Math. **25** (2019), 574–588. MR 3982254

[Chi21] ———, *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

[CJO14] Ferran Cedó, Eric Jespers, and Jan Okniński, *Braces and the Yang–Baxter equation*, Comm. Math. Phys. **327** (2014), no. 1, 101–116. MR 3177933

[CR81] Charles W. Curtis and Irving Reiner, *Methods of Representation Theory. Vol. I*, Pure and Applied Mathematics, John Wiley & Sons, Inc., New York, 1981, With applications to finite groups and orders. MR 632548

[CRV16a] Teresa Crespo, Anna Rio, and Montserrat Vela, *Induced Hopf Galois structures*, J. Algebra **457** (2016), 312–322. MR 3490084

[CRV16b] ———, *On the Galois correspondence theorem in separable Hopf Galois theory*, Publ. Mat. **60** (2016), no. 1, 221–234. MR 3447739

[CS69] Stephen U. Chase and Moss E. Sweedler, *Hopf Algebras and Galois Theory*, Lecture Notes in Mathematics, Vol. 97, Springer-Verlag, Berlin-New York, 1969. MR 0260724

[CS21] 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

[CS22] ———, *Brace blocks from bilinear maps and liftings of endomorphisms*, J. Algebra **610** (2022), 831–851. MR 4473766

[CS23] ———, *Skew braces from Rota–Baxter operators: a cohomological characterisation and some examples*, Ann. Mat. Pura Appl. (4) **202** (2023), no. 1, 1–13. MR 4531710

[CSV19] Ferran Cedó, Agata Smoktunowicz, and Leandro Vendramin, *Skew left braces of nilpotent type*, Proc. Lond. Math. Soc. (3) **118** (2019), no. 6, 1367–1392. MR 3957824

[DC23] Ilaria Del Corso, *Module braces: relations between the additive and the multiplicative groups*, Annali di Matematica Pura ed Applicata (1923 -) (2023).

[Dri92] V. G. Drinfel'd, *On some unsolved problems in quantum group theory*, Quantum groups (Leningrad, 1990), Lecture Notes in Math., vol. 1510, Springer, Berlin, 1992, pp. 1–8. MR 1183474

[ESS99] Pavel Etingof, Travis Schedler, and Alexandre Soloviev, *Set-theoretical solutions to the quantum Yang-Baxter equation*, Duke Math. J. **100** (1999), no. 2, 169–209. MR 1722951

[GLS21] Li Guo, Honglei Lang, and Yunhe Sheng, *Integration and geometrization of Rota-Baxter Lie algebras*, Adv. Math. **387** (2021), Paper No. 107834, 34. MR 4271483

[GP87] Cornelius Greither and Bodo Pareigis, *Hopf Galois theory for separable field extensions*, J. Algebra **106** (1987), no. 1, 239–258. MR 878476

[Gre92] C. Greither, *Extensions of finite group schemes, and Hopf Galois theory over a complete discrete valuation ring*, Math. Z. **210** (1992), no. 1, 37–67. MR 1161169

[GSV19] Marino Gran, Florence Sterck, and Joost Vercruysse, *A semi-abelian extension of a theorem by Takeuchi*, J. Pure Appl. Algebra **223** (2019), no. 10, 4171–4190. MR 3958087

[GV17] L. Guarnieri and L. Vendramin, *Skew braces and the Yang–Baxter equation*, Math. Comp. **86** (2017), no. 307, 2519–2534. MR 3647970

[Hal59] Marshall Hall, Jr., *The Theory of Groups*, The Macmillan Company, New York, 1959. MR 103215

[Hun80] Thomas W. Hungerford, *Algebra*, Graduate Texts in Mathematics, vol. 73, Springer-Verlag, New York-Berlin, 1980, Reprint of the 1974 original. MR 600654

[JKVAV19] E. Jespers, Ł . Kubat, A. Van Antwerpen, and L. Vendramin, *Factorizations of skew braces*, Math. Ann. **375** (2019), no. 3-4, 1649–1663. MR 4023387

[JKVAV21] ———, *Radical and weight of skew braces and their applications to structure groups of solutions of the Yang-Baxter equation*, Adv. Math. **385** (2021), Paper No. 107767, 20. MR 4256133

[JVAV23] E. Jespers, A. Van Antwerpen, and L. Vendramin, *Nilpotency of skew braces and multipermutation solutions of the Yang–Baxter equation*, Commun. Contemp. Math. **25** (2023), no. 09, Paper No. 2250064. MR 4627847

[KKTU19] Alan Koch, Timothy Kohl, Paul J. Truman, and Robert Underwood, *Normality and short exact sequences of Hopf-Galois structures*, Comm. Algebra **47** (2019), no. 5, 2086–2101. MR 3977722

[Koc21] Alan 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

[Koh98] Timothy Kohl, *Classification of the Hopf Galois structures on prime power radical extensions*, J. Algebra **207** (1998), no. 2, 525–546. MR 1644203

[Koh19] ———, *Characteristic subgroup lattices and Hopf-Galois structures*, Internat. J. Algebra Comput. **29** (2019), no. 2, 391–405. MR 3934792

[KSV21] Alexander Konovalov, Agata Smoktunowicz, and Leandro Vendramin, *On skew braces and their ideals*, Exp. Math. **30** (2021), no. 1, 95–104. MR 4223285

[KT20] Alan Koch and Paul J. Truman, *Opposite skew left braces and applications*, J. Algebra **546** (2020), 218–235. MR 4033084

[KT23] _____, *Skew left braces and isomorphism problems for Hopf–Galois structures on Galois extensions*, J. Algebra Appl. **22** (2023), no. 5, Paper No. 2350118, 22. MR 4556334

[LV19] Victoria Lebed and Leandro Vendramin, *On structure groups of set-theoretic solutions to the Yang–Baxter equation*, Proc. Edinb. Math. Soc. (2) **62** (2019), no. 3, 683–717. MR 3974961

[Mon93] Susan 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; by the American Mathematical Society, Providence, RI, 1993. MR 1243637

[Nas19] Timur Nasybullov, *Connections between properties of the additive and the multiplicative groups of a two-sided skew brace*, J. Algebra **540** (2019), 156–167. MR 4003478

[NZ19] Kayvan Nejabati Zenouz, *Skew braces and Hopf–Galois structures of Heisenberg type*, J. Algebra **524** (2019), 187–225. MR 3905210

[Rum07a] Wolfgang Rump, *Braces, radical rings, and the quantum Yang–Baxter equation*, J. Algebra **307** (2007), no. 1, 153–170. MR 2278047

[Rum07b] _____, *Classification of cyclic braces*, J. Pure Appl. Algebra **209** (2007), no. 3, 671–685. MR 2298848

[Rum14] _____, *The brace of a classical group*, Note Mat. **34** (2014), no. 1, 115–144. MR 3291816

[Rum19] _____, *Classification of cyclic braces, II*, Trans. Amer. Math. Soc. **372** (2019), no. 1, 305–328. MR 3968770

[Sch60] Eugene Schenkman, *On the norm of a group*, Illinois J. Math. **4** (1960), 150–152. MR 113928

[Smo22] Agata Smoktunowicz, *Algebraic approach to Rump's results on relations between braces and pre-Lie algebras*, J. Algebra Appl. **21** (2022), no. 3, Paper No. 2250054, 13. MR 4391819

[ST23a] L. Stefanello and S. Trappeniers, *On bi-skew braces and brace blocks*, J. Pure Appl. Algebra **227** (2023), no. 5, Paper No. 107295. MR 4521746

[ST23b] Lorenzo Stefanello and Senne Trappeniers, *On the connection between Hopf–Galois structures and skew braces*, Bull. Lond. Math. Soc. **55** (2023), no. 4, 1726–1748. MR 4623681

[SV18] Agata Smoktunowicz and Leandro Vendramin, *On skew braces (with an appendix by N. Byott and L. Vendramin)*, J. Comb. Algebra **2** (2018), no. 1, 47–86. MR 3763907

[Swe69] Moss E. Sweedler, *Hopf Algebras*, Mathematics Lecture Note Series, W. A. Benjamin, Inc., New York, 1969. MR 252485

[Tsa22] Cindy 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

[Ven19] Leandro Vendramin, *Problems on skew left braces*, Adv. Group Theory Appl. **7** (2019), 15–37. MR 3974481

[Ven23] Leandro Vendramin, *Skew braces: a brief survey*, arXiv: 2311.07112, 2023.

[Wat68] J. F. Watters, *On the adjoint group of a radical ring*, J. London Math. Soc. **43** (1968), 725–729. MR 229677

[Wei69] Edwin Weiss, *Cohomology of Groups*, Pure and Applied Mathematics, Vol. 34, Academic Press, New York-London, 1969. MR 263900

[Win74] David Winter, *The Structure of Fields*, Graduate Texts in Mathematics, No. 16, Springer-Verlag, New York-Heidelberg, 1974. MR 389873