VRIJE
UNIVERSITEIT
BRUSSEL

Thesis submitted in fulfilment of the requirements for the award of the degree of Doctor of Sciences

# SKEW BRACES AND THEIR CONNECTION TO THE YANG–BAXTER EQUATION, HOPF–GALOIS STRUCTURES AND POST-LIE RINGS

**Senne Trappeniers**

2025-2026

| | |
|---|---|
| Promotor: | Prof. Dr. Leandro Vendramin |
| Co-promotor: | Dr. Arne Van Antwerpen |
| Chairperson: | Prof. Dr. Mark Sioen |
| Jury: | Prof. Dr. Kenny De Commer |
| | Prof. Dr. Dominique Maes |
| | Prof. Dr. Karel Dekimpe |
| | Prof. Dr. Anna Zamojska-Dzienio |

**Faculty of Sciences and Bio-Engineering Sciences**
**Department of Mathematics and Data Science**

# Abstract

The Yang–Baxter equation initially appeared in both quantum and statistical mechanics. Drinfeld proposed studying a special class of its solutions, the so-called set-theoretical solutions. Although more restrictive, these solutions remain too general to be classified completely. Nevertheless, studying them leads to a better understanding of the Yang–Baxter equation. Braces, algebraic structures introduced by Rump, turn out to provide the right algebraic framework to study involutive non-degenerate solutions. Later, skew braces were introduced by Guarnieri and Vendramin as a generalization to study also the non-involutive ones. These algebraic structures form the main focus of this thesis.

We start by studying two classes of skew braces. The first is the class of two-sided skew braces. We show that they can be described as extensions of weakly trivial skew braces by two-sided braces, which leads to novel structural results. The second class comprises bi-skew braces, which are more generally related to brace blocks. We provide a technical characterization of brace blocks as well as more feasible constructions.

In the next three chapters, we treat the connection between skew braces and non-degenerate set-theoretical solutions of the Yang–Baxter equation. After exploring how certain properties of solutions relate to those of their associated skew braces, we classify finite indecomposable involutive non-degenerate solutions with an abelian permutation group and indecomposable involutive non-degenerate solutions of size $p^2$ with $p$ a prime.

Subsequently, we discuss the existing connection between skew braces and Hopf–Galois structures on finite Galois field extensions and propose a refined version. This enables an explicit classification of all such extensions where the Hopf–Galois correspondence is surjective, a behavior closely resembling that of the classical Galois correspondence.

In the final part of the thesis, we develop a Lazard correspondence between $L$-nilpotent post-Lie rings and $L$-nilpotent skew braces. By means of illustration, we then use this correspondence to obtain in a more explicit form Zenouz's classification of skew braces of order $p^3$, $p > 3$ a prime, through a classification of $L$-nilpotent Lie rings of the same order.

Collectively, these results deepen the structural understanding of skew braces and emphasize their pivotal role, both in algebra and in relation to the Yang–Baxter equation.

# Samenvatting

De Yang–Baxter vergelijking verscheen oorspronkelijk zowel in de kwantummechanica als in de statistische mechanica. Drinfeld stelde voor om een bijzondere klasse van oplossingen te bestuderen: de verzamelingtheoretische oplossingen. Hoewel restrictiever, blijven deze oplossingen te algemeen om volledig te classificeren. Toch leidt het onderzoek ervan tot een beter begrip van de Yang–Baxter vergelijking. Braces, algebraïsche structuren geïntroduceerd door Rump, blijken het juiste algebraïsche kader te bieden om involutieve niet-gedegenereerde oplossingen te bestuderen. Later werden skew braces geïntroduceerd door Guarnieri en Vendramin als een veralgemening hiervan om ook niet-involutieve oplossingen te bestuderen. Deze algebraïsche structuren vormen de kern van deze thesis.

We beginnen met het bestuderen van twee klassen van skew braces. De eerste is de klasse van tweezijdige skew braces. We tonen aan dat deze steeds bekomen kunnen worden als extensies van een zwak triviale skew brace met een tweezijdige brace, wat leidt tot nieuwe structurele resultaten. De tweede klasse omvat biskew braces, die sterk gerelateerd zijn aan braceblokken. We geven voor braceblokken zowel een technische karakterisering als makkelijker hanteerbare constructies.

Vervolgens behandelen we de connectie tussen skew braces en niet-gedegenereerde verzamelingtheoretische oplossingen van de Yang–Baxter vergelijking. Na te onderzoeken hoe bepaalde eigenschappen van oplossingen gerelateerd zijn aan die van hun geassocieerde skew braces, classificeren we onontbindbare eindige involutieve niet-gedegenereerde oplossingen onder de voorwaarde dat hun permutatiegroep abels is of ze van grootte $p^2$ zijn, met $p$ priem.

Daarna bespreken we de bestaande connectie tussen skew braces en Hopf–Galois structuren op eindige Galois velduitbreidingen en geven we een verfijndere correspondentie tussen deze twee structuren. Deze maakt een expliciete classificatie mogelijk van alle Galoisuitbreidingen waarbij de Hopf–Galoiscorrespondentie surjectief is, hetgeen overeenkomt met het gedrag van de klassieke Galoiscorrespondentie.

In het laatste deel ontwikkelen we een Lazardcorrespondentie tussen $L$-nilpotente post-Lie-ringen en $L$-nilpotente skew braces. Ter illustratie gebruiken we vervolgens deze correspondentie om Zenouz's classificatie van skew braces van orde $p^3$, met $p > 3$ priem, in een meer expliciete vorm te verkrijgen via een classificatie van $L$-nilpotente post-Lie-ringen van dezelfde orde.

De bekomen resultaten dragen bij aan een beter begrip van skew braces en benadrukken hun essentiële rol in zowel pure algebra als in onderzoek naar de Yang–Baxter vergelijking.

# Acknowledgements

First and foremost, I would like to express my gratitude to my supervisors, Prof. Dr. Leandro Vendramin and Dr. Arne Van Antwerpen, for their support over the past four years. I would especially like to thank Arne, who, in addition, not only supervised my master's thesis but also witnessed my growth as a mathematician over the last nine years and has significantly contributed to this growth. I am grateful to the members of the jury for taking the time to read my thesis and for giving valuable feedback. My thanks further go to Dr. Lorenzo Stefanello and Dr. Marco Castelli, who played an important role in my academic journey through the many stimulating discussions we shared during our collaborations.

Moreover, a special mention is due to Prof. Dr. Eric Jespers; when I was in search of a topic for my master's thesis, it only took him a few minutes to convince me that these weird algebraic structures called skew braces could be of interest. Also taking into account his ever-interesting classes, he is definitely one of the main reasons I decided to pursue research in algebra. Additionally, I would also like to thank Dr. Ilaria Colazzo for always being there to provide me with solid advice, whether it concerned mathematical or less mathematical matters.

More broadly, I would like to thank all of my VUB colleagues. In particular, those colleagues with whom I had the pleasure of sharing an office—and who therefore had to witness my fluctuating caffeine addiction over the last years: Charlotte Verwimp, Silvia Properzi, Thomas Letourmy, Carsten Dietzel, Davide Ferri, Charlotte Roelants, and Yufei Qin. Continuing along the same line of thought, the WK vending machine deserves a special mention for sustaining said addiction.

I am equally indebted to many people outside of mathematics. Of course, I owe thanks to my family for their continuous and unconditional support. A very special mention also goes to Emi and Orane; the many lunch breaks we shared were just a small part of a much deeper friendship, but nonetheless a driving force behind my thesis. The many weekends away with Carlijn, Chiqui, Emi, Manon, Matthias, Nand, Beire, Stijn, Tuur, and Tazze (or any subset thereof) have been invaluable in providing me with both well-timed breaks and plenty of laughter.

Finally, I am eternally grateful to the many other friends and roommates (turned friends) who have accompanied me on this journey. Whether they witnessed me in my most stressful and overworked moments, patiently endured my repeated attempts to explain my research, or simply reminded me that there is more to life than mathematics, their presence has truly made all the difference.

Senne Trappeniers,
19 September 2025

# Contents

# Introduction

Many, if not most, fields of mathematics revolve around the study of a class of objects of interest. The nature of said object can range from purely algebraic (groups, fields, algebras, ...) to geometric (topological spaces, manifolds, ...) to something in between (Lie groups, algebraic varieties, ...) or to something else entirely. The beauty of it all lies in the fact that none of these research fields really stand on their own. There are, of course, the obvious inclusions where one simply forgets some structure of an object to end up with a weaker notion. Any Lie group is, in particular, a group, any manifold is, in particular, a topological space, and so forth, but there are also more intriguing cases where objects of a different nature are obtained. Whenever a notion of symmetry is present, one may consider the group formed by these symmetries, thus ending up in the realm of group theory. A group, in turn, gives rise to a group algebra, the modules of that group algebra form a monoidal category, etc. Often, when applying such constructions, we lose some of the information encoded in the original object. One can generally not expect that the symmetry group of an object retains all information about said object, although that certainly does not mean that no insight into the starting object is to be recovered from it. On the other hand, sometimes surprising results are obtained that state that, in fact, all information about the starting object can be recovered. Think, for example, of the Tannaka–Krein duality, where objects are reconstructed from their representations.

Although uncovering such connections in mathematics is rewarding in its own right, their true strength often lies in the fact that the objects involved are of fundamentally different natures. A classical example is Galois theory: starting from a field extension $L/K$, one may consider its group $G$ of field automorphisms; the symmetries in this setting. As one might expect, transitioning from a field extension to its group of automorphisms results in a loss of specific information about $L$ and $K$. Nonetheless, when the extension satisfies suitable conditions, it becomes possible to recover key structural features. For instance, the lattice of intermediate field extensions is then dual to the lattice of subgroups of $G$.

Another example, and one of central importance to this thesis, is found in the study of set-theoretical solutions of the Yang–Baxter equation. We will present a more detailed account in Chapter 1; here we limit ourselves to a brief overview. A *set-theoretical solution of the Yang–Baxter equation* consists of a non-empty set $X$ and a map $r : X^2 \to X^2$ such that the equation

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

is satisfied. Set-theoretical solutions are a special case of the more general Yang–Baxter equation, which involves a linear map on the tensor square of a vector space, which appeared in the works of Yang [169] and Baxter [20]. This equation can be visualized as the third Reidemeister move, which explains why it is also known as the *braid equation*, see Fig. 1.

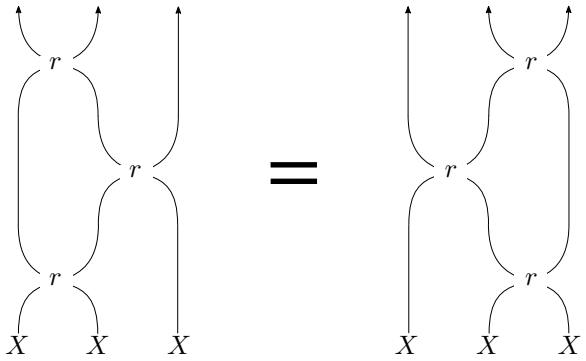



Figure 1: A visualisation of the Yang–Baxter equation. On the bottom, the beginning of the three strands each signifies a copy of $X$ in $X^3$, and every crossing of two strands symbolizes an application of the map $r$.

Set-theoretical solutions of the Yang–Baxter equation are at first sight far removed from algebra. However, we could interpret the map $r$ as giving certain quadratic relations. Such interpretation gives rise to its *structure monoid* $M = M(X, r)$. This monoid is constructed by starting from the free monoid on $X$ and imposing the relation $xy = ab$ whenever $r(x, y) = (a, b)$, where $x, y, a, b \in X$. Note that this construction solely relies on $r$ being a map from $X^2$ to itself, not on it satisfying the Yang–Baxter equation. A good indication that this structure monoid is of interest, is that this monoid has a natural left action on $X$ where a generator $x$ maps $y$ to the first component of $r(x, y)$. Similarly, there is a right action defined where the generator $x$ maps $y$ to the second component of $r(y, x)$ The obtained monoid naturally gives rise to its monoid algebra $K[M]$ over a given field $K$. Natural questions now arise: is $K[M]$ interesting from a ring-theoretic perspective? Are there properties of $K[M]$ that can be directly related to those of $(X, r)$, and vice versa? It turns out that the answer to these is positive, see [52, 92]. Going back to the structure monoid $M$ of $(X, r)$, one can instead head into a different direction and construct its group of fractions $G = G(X, r)$. We call $G$ the structure group of $(X, r)$. If one wants to make the monoid actions of $M$ on $X$ into actions of the group $G$ on $X$, then a non-degeneracy condition on $(X, r)$ appears naturally. Together with bijectivity of $r$, which we will henceforth always assume to be the case, this allows for the construction of a secondary group structure on the set $G$. Let $\circ$ denote the original group operation on $G$ and let $\cdot$ denote the secondary one. Remarkably, these operations satisfy the identity

$$a \circ (b \cdot c) = (a \circ b) \cdot a^{-1} \cdot (a \circ c),$$

for all $a, b, c \in G$, where $a^{-1}$ is the inverse of $a$ in the group $(G, \cdot)$. This fact is highly non-trivial and constitutes the main result of [73, 117, 152]. A triple $(G, \cdot, \circ)$ for which the above condition is satisfied, is called a *skew brace*. If the canonical map $\iota : X \to G$ is injective then the data $(G, \cdot, \circ)$ and $\iota$ determine the solution $(X, r)$ completely. When $r^2 = \mathrm{id}_{X^2}$, this injectivity condition is always satisfied; in this case, we say that the solution is *involutive*. More than just being a surprising construction, this opens the door to applying group theoretic techniques in the study of set-theoretical solutions. As far as classification purposes go, attempting to instead classify structure skew braces will, in general, not facilitate the task: even when $X$ is finite, the structure group $G$ is infinite. To address this, one considers the permutation skew brace $\mathcal{G}(X, r)$, a natural quotient of the structure skew brace that retains finiteness when $X$ is finite. An answer to how much of the information of $(X, r)$ is lost in the process of passing to $\mathcal{G}(X, r)$ is provided in [11, 12]:

the solution $(X, r)$ can be recovered from $\mathcal{G}(X, r)$ provided we are also given the image of the canonical map $X \to \mathcal{G}(X, r)$ and the stabilizers of a natural action of $\mathcal{G}(X, r)$ on $X$.

We can summarize the driving force behind this thesis as follows: to deepen our understanding of how skew braces relate to other mathematical structures, and how these connections can be exploited to transfer problems from one setting to another. Ideally, of course, the latter then leads to a problem that is more easily solved. To clarify this perspective, we now provide an overview of the thesis, highlighting some of the novel contributions that we present.

In an attempt to make this thesis as self-contained as possible, Chapter 1 contains many preliminary results and examples regarding all of the different objects of interest in this thesis. For most results, we simply give the statement without proof and provide a reference to where its proof can be found. However, we include proofs in cases where they offer additional insight or when the statements presented extend slightly beyond what is found in the literature.

Unlike the later chapters, Chapters 2 and 3 focus exclusively on skew braces. We study two different classes of skew braces. The first is the class of bi-skew braces; skew braces that remain a skew brace when the two group operations are interchanged. This property is not merely a curiosity; it follows by a result of Caranti [41] that the property of being a bi-skew brace can be interpreted as satisfying a certain nilpotency condition. When $(A, \cdot)$ is abelian, in this case $(A, \cdot, \circ)$ is simply called a *brace*, this is equivalent to having multipermutation level 2. Braces and involutive solutions of multipermutation level 2 are heavily featured in Chapters 4 to 6. Moreover, using the theory of bi-skew braces, we prove in Theorem 2.3.6 that there are precisely three isomorphism classes of skew braces whose multiplicative group is infinite cyclic, thereby solving [164, Problem 27]. Going beyond bi-skew braces, one can study families $(A, \circ_i)_{i\in I}$ of group structures on the same set $A$ such that, for any $i, j \in I$, the triple $(A, \circ_i, \circ_j)$ is a skew brace. Such a family is called a *brace block*. Our two main results concerning brace blocks are Theorems 2.4.1 and 2.4.5. Theorem 2.4.1 provides a precise but technical characterization of when a family $(A, \circ_i)_{i\in I}$ forms a brace block. Theorem 2.4.5 gives sufficient conditions for when a family $(A, \circ_i)_{i\in I}$ is a brace block, which are more manageable when one's interest is in constructing explicit examples. It turns out that all known constructions of brace blocks in the literature can be obtained through the latter construction. We also use it to construct new examples exhibiting curious behaviors, where we draw inspiration from ring theory.

The second class that we consider is that of two-sided skew braces. Historically, (left) braces occurred as generalizations of Jacobson radical rings, where the latter correspond precisely to two-sided braces. Instead of removing the two-sidedness condition of a Jacobson radical ring and thus ending up with a brace, we can also relax the abelianity of the additive group to obtain the notion of a two-sided skew brace. Our main result, Theorem 3.2.3, shows that such a skew brace contains a canonical ideal that is a two-sided brace and such that the quotient with this ideal is very close to being just a group. We coin the term *weakly trivial* skew braces for such quotients, which we characterize in Theorem 3.1.12 by pairs of groups with isomorphic abelianizations. Finally, we discuss consequences of Theorem 3.2.3 on the nilpotency and solvability of the groups of two-sided skew braces, thereby extending some of the results by Nasybullov obtained in [123].

We subsequently focus on the earlier-mentioned connection between skew braces and non-degenerate set-theoretical solutions of the Yang–Baxter equation. In Chapter 4 we explore four of its different aspects. First, we revisit the well-established notion of the multipermutation level of a set-theoretical solution $(X, r)$, denoted $\mathrm{mpl}(X, r)$, which can be interpreted as a nilpotency condition. There is also the notion of multipermutation level for skew braces, where this interpretation as a nilpotency condition is very precise. For $(X, r)$ a non-degenerate set-theoretical solution with $|X| > 1$, results from [49, 79] establish the inequalities

$$\mathrm{mpl}(G(X, r)) - 1 \leq \mathrm{mpl}(\mathcal{G}(X, r)) \leq \mathrm{mpl}(X, r) \leq \mathrm{mpl}(G(X, r)).$$

For injective solutions, one has $\mathrm{mpl}(G(X, r)) = \mathrm{mpl}(\mathcal{G}(X, r)) + 1$, but even then no strict relation exists

between $\mathrm{mpl}(X,r)$ and $\mathrm{mpl}(\mathcal{G}(X,r))$ without additional assumptions on $(X,r)$. To address this, we propose a slight modification of the multipermutation level of a solution, which we denote by $\mathrm{mpl}'(X,r)$. The underlying idea here is that while $\mathrm{mpl}(X,r)$ measures how far away a solution is from being the trivial one-element solution, $\mathrm{mpl}'(X,r)$ instead quantifies the distance to a trivial solution of the form $(x,y)\mapsto(y,x)$ on a set of cardinality possibly greater than 1. Our main result on this, Theorem 4.1.10, shows that the equality $\mathrm{mpl}'(X,r)=\mathrm{mpl}(\mathcal{G}(X,r))$ holds without any additional assumptions. Though the difference between $\mathrm{mpl}(X,r)$ and $\mathrm{mpl}'(X,r)$ is minor in the sense that $\mathrm{mpl}(X,r)-1\leq\mathrm{mpl}'(X,r)\leq\mathrm{mpl}(X,r)$, this refinement is significant given that classification problems become considerably more complex when moving from multipermutation level $n$ to $n+1$ (cf. Chapter 6). The second aspect concerns the relation between the indecomposability of non-degenerate set-theoretical solutions of the Yang–Baxter equation and generators of the associated skew braces $G(X,r)$ and $\mathcal{G}(X,r)$. Indecomposable solutions, by definition, cannot be decomposed into two subsolutions. Results from [136, 150] show that if $(X,r)$ is indecomposable, involutive and has a finite multipermutation level, then the braces $G(X,r)$ and $\mathcal{G}(X,r)$ are one-generated; that is, there exists an element such that the smallest subbrace containing this element is the whole brace. Rump also provided an example to show that this does not necessarily hold without the finite multipermutation level assumption. In Proposition 4.2.3 and Corollary 4.2.6 we extend the results by instead relating indecomposability of a solution to $G(X,r)$ and $\mathcal{G}(X,r)$ being one-generated as strong left ideals, and proving that these two different notions of being one-generated coincide in the multipermutation case. More generally, we relate the minimal number of orbits in a cycle base of a skew brace to its minimal number of generators, where indecomposability corresponds to the existence of a unique orbit. We use this then as a stepping stone to explore different notions of generating sets and how these coincide under certain nilpotency conditions. Next, motivated by Chapter 2, we describe how the property of being a bi-skew brace interacts with solutions of the Yang–Baxter equation. We provide a precise characterization of when the structure or permutation skew brace of a solution is bi-skew. Additionally, we negatively answer the question of whether solutions associated with $(A,\cdot,\circ)$ and $(A,\circ,\cdot)$ are directly related when $(A,\cdot,\circ)$ is a bi-skew brace. In the last part of the chapter, we treat automorphisms of both solutions and skew braces. We prove that a non-degenerate indecomposable multipermutation solution has no trivial subsolutions, which then implies that all homomorphisms of such solutions are surjective. In the finite case, this further implies that all endomorphisms of such a solution are in fact automorphisms. Similar results were previously known in the case of multipermutation level 2 [88, 90]. Any automorphism of a non-degenerate indecomposable involutive solution $(X,r)$ yields an automorphism of the braces $G(X,r)$ and $\mathcal{G}(X,r)$. Conversely, it is described by Cedó, Jespers and Bachiller how certain automorphisms of $\mathcal{G}(X,r)$ lift to automorphisms of $(X,r)$. We build upon this result to define a subbrace $H$ of $\mathcal{G}(X,r)$ which we can use to construct a subgroup of automorphisms of $(X,r)$. Moreover, we have control over the structure of this subgroup of automorphisms since we prove that it is isomorphic to a quotient of $(H,\cdot)$. Although possibly $|H|=1$, the other extreme case $H=\mathcal{G}(X,r)$ occurs precisely when $\mathrm{mpl}(X,r)=2$. Under this assumption, Theorem 4.4.14 expresses the whole automorphism group $\mathrm{Aut}(X,r)$ as a quotient of $(\mathcal{G}(X,r),\cdot)$, thereby extending a result by Jedlička and Pilitowska [88, Proposition 5.16].

In Chapter 5 our main result is the classification of non-degenerate, indecomposable, involutive set-theoretical solutions of size $p^2$, for $p$ a prime.

**Theorem.** *Let $p$ be a prime, let $\Phi:\mathbb{Z}/p\to\mathbb{Z}/p$ be a non-constant map with $\Phi(x)=\Phi(-x)$ and let $\alpha\in(\mathbb{Z}/p)^\times$ be such that $\Phi(\alpha x)=\alpha\Phi(x)$, where $(\mathbb{Z}/p)^\times$ denotes the group of invertible elements of $\mathbb{Z}/p$. If we set $X=\mathbb{Z}/p\times\mathbb{Z}/p$ and*

$$r\begin{pmatrix}(a,x)\\(b,y)\end{pmatrix}=\begin{pmatrix}(\alpha^{-1}b-x,\alpha^{-1}y-\Phi(\alpha^{-1}b-x-a))\\(\alpha a+y-\Phi(b-\alpha x-\alpha a),\alpha x+\Phi(\alpha a-\alpha x-b))\end{pmatrix},$$

*then $(X, r)$ is a non-degenerate, irretractable, indecomposable, involutive set-theoretical solution of the Yang–Baxter equation of size $p^2$. Up to isomorphism, every such solution is of this form. The parameters $\alpha, \Phi$ and $\alpha', \Phi'$ define isomorphic solutions if and only if $\alpha = \alpha'$ and there is a $\beta \in (\mathbb{Z}/p)^\times$ such that $\beta^{-1}\Phi(\beta x) = \Phi'(x)$ for all $x \in \mathbb{Z}/p$.*

We use this result to give an explicit formula for the number of isomorphism classes of such solutions for any prime $p$. The strategy used to prove this classification theorem begins by first considering such solutions $(X, r)$ as transitive cycle bases of their permutation brace. In the case where $\mathcal{G}(X, r)$ is a $p$-group, then the left nilpotency of the brace yields a subbrace $F$ of fixed points of $\mathcal{G}(X, r)$. We prove that $X$ is a double coset of $F$ in $(\mathcal{G}(X, r), \circ)$, from which the explicit form of $r$ can then be deduced. In the remaining case, where $|\mathcal{G}(X, r)|$ contains prime divisors different from $p$, we prove that $(X, r)$ is a deformation by an automorphism of one of the solutions obtained in the $p$-group case.

Another classification is addressed in Chapter 6, namely that of the class of finite non-degenerate, indecomposable, involutive set-theoretical solutions with abelian permutation group. Such solutions necessarily have a finite multipermutation level. The classification is first reduced to that of one-generated finite braces whose multiplicative group is abelian. The generating relations of such braces are then encoded via matrices, allowing us to reduce the classification problem to analyzing orbits of a group action on these matrices. If we restrict to those solutions of multipermutation level at most 2, we recover in an alternative way the classification obtained by Jedlićka, Pilitowska and Zamosjka-Dzienio in [90]. For multipermutation level 3, we obtain in Theorem 6.3.4 an explicit formula for the number of isomorphism classes of such solutions of a given size. We conclude the chapter with a brief discussion of infinite solutions satisfying the same conditions.

In Chapter 7, we investigate the connection between skew braces and Hopf–Galois structures. The latter generalizes the classical notion of the Galois group associated with a Galois field extension by replacing groups with Hopf algebras acting on (not necessarily Galois) field extensions. When we restrict to Hopf–Galois structures on a Galois field extension $L/K$ with Galois group $(G, \circ)$, results by Greither and Pareigis [82] and Childs [57] reduce the classification of Hopf–Galois structures on $L/K$ to finding regular affine actions of $G$ on another group $N$. Such actions yield regular subgroups of the holomorph of $N$, which are fundamentally linked to the theory of skew braces. We first summarize the known connection and then refine it in Theorem 7.2.1, where we prove a bijective correspondence between Hopf–Galois structures on $L/K$ and operations $\cdot$ such that $(G, \cdot, \circ)$ is a skew brace. This correspondence allows for an explicit construction of the Hopf–Galois structure corresponding to a given skew brace $(G, \cdot, \circ)$. We further explore this correspondence by examining how substructures of $(G, \cdot, \circ)$ relate to those of the corresponding Hopf algebra and to intermediate fields of $L/K$. The overarching theme is that skew braces play the same role in Hopf–Galois theory over Galois fields that groups play in classical Galois theory. The Hopf–Galois correspondence, analogous to the classical Galois correspondence, is a central object of study. However, in contrast to the classical case, this correspondence is not always surjective; that is, not every intermediate field of $L/K$ necessarily is reached through this correspondence. Examples of extensions where surjectivity holds for all possible Hopf–Galois structures on a given extension are scarce in the literature. Through Theorem 7.2.1, we reduce the problem of finding such extensions to a concrete question about skew braces. We then provide a complete answer for this problem in Theorem 7.3.23.

Chapter 8 is entirely devoted to developing a Lazard-type correspondence between skew braces and post-Lie algebras in a setting that is as general as possible. A *post-Lie algebra* over a commutative ring $R$ is a Lie algebra $\mathfrak{a}$ with Lie bracket $[-, -]$ over $R$, together with an $R$-bilinear operation $\triangleright$ satisfying

$$x \triangleright [y, z] = [x \triangleright y, z] + [y, x \triangleright z],$$
$$[x, y] \triangleright z = (x, y, z)_\triangleright - (y, x, z)_\triangleright,$$

for all $x, y, z \in \mathfrak{a}$, with $(x, y, z)_\triangleright$ defined as the associator $x \triangleright (y \triangleright z) - (x \triangleright y) \triangleright z$. If the bracket on $\mathfrak{a}$ is trivial, then $(\mathfrak{a}, \triangleright)$ is a *pre-Lie algebra*. When $R = \mathbb{Z}$, we call such structures *post-Lie rings* or *pre-Lie rings* respectively. Multiple constructions relating post-Lie algebras and skew braces are known in the literature. For instance, in [15, 27, 98] the differentiation of a skew Lie brace produces a post-Lie algebra, where a *skew Lie brace* is a skew brace $(A, \cdot, \circ)$ with $A$ a differential manifold and $(A, \cdot)$ and $(A, \circ)$ Lie groups. We remark that skew braces appeared here under equivalent formulations like regular affine actions of Lie groups or post-Lie groups. A similar construction in a purely algebraic context was developed by Smoktunowicz in [147], under a strong nilpotency condition. Also, methods for constructing pre-Lie rings from braces are given in [87, 143]. Conversely, methods to construct skew braces from post-Lie algebras are also known: in [27, 98] this is done via Lie theory, while in [2, 15, 147] algebraic approaches are used. If we restrict our attention to the finite setting and to constructions where no information is inevitably lost (as is for example the case in [87, 143]) then all known results are due to Smoktunowicz: mimicking the construction of the group of formal flows by Agrashev and Gamkredlidze [2], she proved how starting from a left nilpotent pre-Lie algebra $(\mathfrak{a}, \triangleright)$ of size $p^n$ with $n < p - 1$ one obtains a brace $(\mathfrak{a}, +, \circ)$. She also gives a partial inverse to this construction, but this requires the starting brace to be strongly nilpotent of class strictly smaller than $p$. Since then, it has remained an open problem whether Smoktunowicz's construction can be inverted without imposing the strong nilpotency assumption, see [147, Question 1] and [97, Problem 20.92 b)]. A result that relates to the construction of the group of flows is the Lazard correspondence [112]. This is a correspondence between filtered Lie rings and filtered groups satisfying a divisibility condition; we refer to these as *Lazard Lie rings* and *Lazard groups* respectively. In the finite setting, the Lazard correspondence restricts to a correspondence between Lie rings of size a power of $p$ and nilpotency class strictly less than $p$, and groups of the same size and nilpotency class, where $p$ is a prime. Our main tool in extending Smoktunowicz's result lies in a careful analysis of the behavior of the Lazard correspondence on semidirect sums of Lazard Lie rings and semidirect products of Lazard groups, and in explicitly relating automorphisms and derivations of Lazard Lie rings. This leads to a natural notion of filtered post-Lie rings and filtered skew braces, and subsequently to that of *Lazard post-Lie rings* and *Lazard skew braces*. We then establish a correspondence between these structures in Theorem 8.4.14. Through the theory of filtered skew braces, we also obtain in Theorem 8.6.6 a statement that was shown to hold for finite skew braces by Cédo, Smoktunowicz and Vendramin [55, Theorem 4.8].

**Theorem.** *Let $(A, \cdot, \circ)$ be a left nilpotent skew brace such that the group $(A, \cdot)$ is nilpotent. Then also the group $(A, \circ)$ is nilpotent.*

The Lazard property, for post-Lie rings and skew braces, gives rise to $L$-nilpotency. We show that $L$-nilpotency is equivalent to left nilpotency and nilpotency of the additive group. In Theorem 8.7.1 we then restrict our general correspondence to finite structures, where it very closely resembles the classical Lazard correspondence in its best-known form:

**Theorem.** *Let $p^n$ be a prime power. Then there exists a correspondence between post-Lie rings of size $p^n$ and $L$-nilpotency class less than $p$, and skew braces of size $p^n$ and $L$-nilpotency class less than $p$. This correspondence respects isomorphisms.*

We emphasize that our constructions extend those by Smoktunowicz. However, the construction from skew braces to post-Lie rings is not generally given by the same formula used by Smoktunowicz. We discuss why both formulas coincide when strong nilpotency of the appropriate class is satisfied and extend this formula to skew braces in Proposition 8.7.9. Also, since the Lazard correspondence overlaps with Lie theory, the correspondence given by Burde, Dekimpe and Deschamps [27] can be deduced as a special case of Theorem 8.4.14. We also extend our correspondence to post-Lie rings and skew braces that appear as the

inverse limit of Lazard post-Lie rings and Lazard skew braces respectively. This extension bypasses both that of the group of formal flows [2] and the formal integration of post-Lie algebras by Bai, Guo, Sheng and Tang [15].

In Chapter 9, we classify all skew braces $(A, \cdot, \circ)$ of size $p^3$ with $(A, \cdot)$ non-abelian, for $p > 3$ a prime. The classification in the case that $(A, \cdot)$ is abelian was done by Bachiller in [9], and also the general classification has already been achieved by Zenouz in his PhD-thesis [124, 125]. Zenouz achieved this through a careful study of subgroups of the holomorph of groups and classified the regular subgroups in terms of generating sets. Our approach, however, is entirely different. It is based on the following special case of the correspondence established in the preceding chapter:

**Theorem.** *Let $p$ be a prime and $n < p$. Then there exists a bijective correspondence between $L$-nilpotent post-Lie rings of size $p^n$ and skew braces of size $p^n$. This correspondence respects isomorphisms.*

We thus proceed by first classifying $L$-nilpotent post-Lie rings of size $p^3$ and then explicitly applying this correspondence. In this way, we get the desired classifications in an explicit form, with the operations given as polynomial functions on $(\mathbb{Z}/p)^3$ or $\mathbb{Z}/p \times \mathbb{Z}/p^2$. Our main goal here is to show the machinery from the previous chapter in action, to show its potential for classification purposes, and also to provide an explicit form of the obtained skew braces since we hope that they will be of use to others.

In this way, the thesis aligns with the broader mathematical vision introduced at the outset: how structures of fundamentally different natures complement the study of one another when their connection is well understood. This guiding philosophy is reflected through concrete results, which contribute to a more cohesive understanding of the rich mathematical landscape surrounding skew braces and their many interconnections.

# Chapter 1

# Preliminaries

## 1.1 Skew braces

A *skew (left) brace* is a triple $(A, \cdot, \circ)$ where $A$ is a set, $(A, \cdot)$ and $(A, \circ)$ are groups, called the *additive* and *multiplicative* group respectively, and

$$a \circ (b \cdot c) = (a \circ b) \cdot a^{-1} \cdot (a \circ c), \tag{B}$$

is satisfied for all $a, b, c \in A$. Here, $a^{-1}$ denotes the inverse of $a \in A$ in the group $(A, \cdot)$. The inverse of $a$ in the group $(A, \circ)$ is denoted by $\overline{a}$. A map

$$f : (A, \cdot, \circ) \to (B, \cdot, \circ),$$

between skew braces is a *homomorphism* if it respects both group operations. The $n$-th power of an element $a \in A$ with respect to the groups $(A, \cdot)$ and $(A, \circ)$ is denoted by $a^n$ and $a^{\circ n}$ respectively. When $(A, \cdot)$ is an abelian group, then we say that $(A, \cdot, \circ)$ is a *brace* and we usually use the notation $(A, +, \circ)$ instead. The latter were introduced by Rump in [132] in connection with non-degenerate involutive solutions of the Yang–Baxter equation, and were subsequently generalized to skew braces by Guarnieri and Vendramin in [83]. Let $0$ denote the neutral element in $(A, \cdot)$, then

$$0 \circ 0 = 0 \circ (0 \cdot 0) = (0 \circ 0) \cdot 0 \cdot (0 \circ 0),$$

hence $0 = 0 \circ 0$, from which it follows that $0$ is also the neutral element of $(A, \circ)$. From now on, when working in a skew brace $A$, by $0$ we will always mean the common neutral element of $(A, \cdot)$ and $(A, \circ)$. In general, when we do not specify the operations on a skew brace $A$, one can always assume that they are $(A, \cdot, \circ)$. Similarly, for a brace, one can always assume them to be $(A, +, \circ)$ in that case.

**Example 1.1.1.** Let $(A, \circ)$ be a group, then $(A, \circ, \circ)$ is a skew brace. We call this the *trivial* skew brace on $(A, \circ)$ and use the notation $\mathrm{Triv}(A, \circ) = (A, \circ, \circ)$.

**Example 1.1.2.** Let $(A, \circ)$ be a group, then $(A, \circ_{\mathrm{op}}, \circ)$ is a skew brace, where $\circ_{\mathrm{op}}$ denotes the opposite operation, meaning $a \circ_{\mathrm{op}} b = b \circ a$. We call this the *almost trivial* skew brace on $(A, \circ)$ and use the notation $\mathrm{opTriv}(A, \circ) = (A, \circ_{\mathrm{op}}, \circ)$.

For a skew brace $A$ and $a, b \in A$, we define

$$\lambda_a(b) = a^{-1} \cdot (a \circ b).$$

If one applies $a^{-1}\cdot$ on both sides of (B), we find precisely $\lambda_a(b \cdot c) = \lambda_a(b) \cdot \lambda_a(c)$. Also, $\lambda_a$ is bijective since its inverse is given by $b \mapsto \overline{a} \circ (a \cdot b)$. We thus obtain a map

$$\lambda : A \to \mathrm{Aut}(A, \cdot) : a \mapsto \lambda_a,$$

called the $\lambda$-*map* of the skew brace $A$. For $a, b, c \in A$, we find

$$\lambda_a\lambda_b(c) = \lambda_a(b^{-1} \cdot (b \circ c)) = a^{-1} \cdot (a \circ (b^{-1} \cdot (b \circ c))) = a^{-1} \cdot (a \circ b^{-1}) \cdot a^{-1} \cdot (a \circ b \circ c),$$

which combined with

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

yields the equality

$$\lambda_a\lambda_b(c) = (a \circ b)^{-1} \cdot (a \circ b \circ c) = \lambda_{a\circ b}(c).$$

We find that the $\lambda$-map induces an action of $(A, \circ)$ on $(A, \cdot)$, which we refer to as the $\lambda$-*action* of $A$.

**Definition 1.1.3.** Let $A$ be a skew brace and $L \subseteq A$. Then $L$ is a

1. *skew subbrace* of $A$ if $L$ is a subgroup of $(A, \cdot)$ and $(A, \circ)$.
2. *left ideal* of $A$ if $L$ is a subgroup of $(A, \cdot)$ such that $\lambda_a(L) \subseteq L$ for all $a \in A$.
3. *strong left ideal* of $A$ if $L$ is a normal subgroup of $(A, \cdot)$ such that $\lambda_a(L) \subseteq L$ for all $a \in A$.
4. *ideal* of $A$ if $L$ is a normal subgroup of $(A, \cdot)$ and $(A, \circ)$ such that $\lambda_a(L) \subseteq L$ for all $a \in A$.

Note that a subset $L$ of $A$ which is invariant under the $\lambda$-action is a subgroup of $(A, \cdot)$ if and only if it is a subgroup of $(A, \circ)$, since $a \circ b = a \cdot \lambda_a(b)$ and $\overline{a} = \lambda_a^{-1}(a^{-1})$. In particular, this implies that left ideals are also skew subbraces.

**Example 1.1.4.** Let $A$ be a skew brace. The *fix* of $A$ is defined as

$$\mathrm{Fix}(A) = \{a \in A \mid \lambda_b(a) = a \text{ for all } b \in A\},$$

and is a left ideal of $A$.

**Example 1.1.5.** Let $A$ be a skew brace. The *socle* of $A$ is defined as

$$\mathrm{Soc}(A) = \{a \in A \mid a \circ b = a \cdot b = b \cdot a \text{ for all } b \in A\} = (\ker \lambda) \cap Z(A, \cdot),$$

and is an ideal of $A$. Here, $Z(A, \cdot)$ denotes the center of the group $(A, \cdot)$. It is interesting to remark that for $a \in \mathrm{Soc}(A)$ we find

$$\lambda_b(a) = b^{-1} \cdot (b \circ a) = (b \circ a) \cdot b^{-1} = b \circ (a \cdot \overline{b}) = b \circ a \circ \overline{b}.$$

**Example 1.1.6.** Let $A$ be a skew brace, then $\ker \lambda$ is a skew subbrace of $A$. Indeed, it is a normal subgroup of $(A, \circ)$ and since $a \cdot b = a \circ b$ for all $a, b \in \ker \lambda$, it is also a subgroup of $(A, \cdot)$. Note that if $A$ is a brace, then $\ker \lambda = \mathrm{Soc}(A)$ and thus it is an ideal, but in general this is not the case.

**Example 1.1.7.** Let $A$ be a skew brace. The *annihilator* of $A$ is defined as

$$\mathrm{Ann}(A) = \{a \in A \mid a \circ b = b \circ a = a \cdot b = b \cdot a \text{ for all } b \in A\},$$

and is an ideal of $A$. Note that we can characterize the annihilator in multiple ways:

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

If $L$ is an ideal of $A$, then $L \cdot a = a \cdot L = a \circ L = L \circ a$ for any $a \in A$, and thus left and right cosets of $L$ with respect to both groups coincide. Therefore, we can consider the *quotient skew brace* $A/L$ with underlying set the cosets of $L$ and with operations

$$(a \cdot L) \cdot (b \cdot L) = a \cdot b \cdot L, \quad (a \cdot L) \circ (b \cdot L) = (a \circ b) \cdot L.$$

Let $A$ be a skew brace and let us denote by $\mathrm{Aut}(A, \cdot, \circ)$ the skew brace *automorphisms* of $A$, by which we mean the invertible skew brace homomorphisms. Let $B$ be a skew brace with a group homomorphism $\alpha : (B, \circ) \to \mathrm{Aut}(A, \cdot, \circ)$, we say in this case that the skew brace $B$ *acts* on $A$. The *semidirect product* of $A$ and $B$, in the sense of Vendramin and Smoktunowicz [151], is the skew brace $A \rtimes_\alpha B$ with underlying set $A \times B$ and group operations

$$\begin{aligned}(a_1, b_1) \cdot (a_2, b_2) &= (a_1 \cdot a_2, b_1 \cdot b_2),\\ (a_1, b_1) \circ (a_2, b_2) &= (a_1 \circ \alpha_{b_1}(a_2), b_1 \circ b_2).\end{aligned}$$

In other words, the additive group of $A \rtimes_\alpha B$ is the direct product of the additive groups of $A$ and $B$, and the multiplicative group is the semidirect product of the multiplicative groups of $A$ and $B$ by the action $\alpha$. Note that the $\lambda$-action in this case is given by

$$\lambda_{(a_1,b_1)}(a_2, b_2) = (\lambda_{a_1}(\alpha_{b_1}(a_2)), \lambda_{b_1}(b_2)).$$

Usually, the action $\alpha$ is suppressed in the notation and we write simply $A \rtimes B$. If we let $B$ act trivially on $A$, we obtain the *direct product* $A \times B$ where both operations are defined component-wise.

Another useful construction is that of the opposite skew brace. Given a skew brace $(A, \cdot, \circ)$, its *opposite* is the skew brace $(A, \cdot_{\mathrm{op}}, \circ)$, so we replace the additive group of $A$ by its opposite. We see that this is indeed a skew brace since for all $a, b, c \in A$ we have that

$$a \circ (b \cdot_{\mathrm{op}} c) = a \circ (c \cdot b) = (a \circ c) \cdot a^{-1} \cdot (b \circ c) = (a \circ b) \cdot_{\mathrm{op}} a^{-1} \cdot_{\mathrm{op}} (a \circ c).$$

We denote the opposite of $A$ by $A_{\mathrm{op}}$. Note in particular that this explains the notation $\mathrm{opTriv}(G)$ for the almost trivial skew brace on a given group $G$, since it is precisely the opposite of the trivial skew brace $\mathrm{Triv}(G)$. The $\lambda$-map of $A_{\mathrm{op}}$ is

$$\lambda^{\mathrm{op}}_a(b) = (a \circ b) \cdot a^{-1} = a \cdot \lambda_a(b) \cdot a^{-1},$$

so we see that a $L \subseteq A$ is a left ideal of both $A$ and $A_{\mathrm{op}}$ if and only if it is a strong left ideal of $A$. In particular, strong left ideals and ideals of $A$ and $A_{\mathrm{op}}$ coincide.

When given a skew brace $(A, \cdot, \circ)$, it is natural to ask how much information on the structure of $(A, \circ)$ can be deduced from $(A, \cdot)$ and vice versa. In the infinite case, this answer seems difficult to answer without assuming any additional structure. See the introduction of Section 1.1.5 and Chapter 9 for some results when in addition $(A, \cdot)$ and $(A, \circ)$ are Lie groups. Let us, for this discussion, assume that $A$ is finite. It is a consequence of Hall's theorem on Sylow systems that if $(A, \cdot)$ is nilpotent, then $(A, \circ)$ is solvable, see [151, Corollary 2.2]. In general, it is an open problem whether the same holds when $(A, \cdot)$ is solvable. Since Byott asked this question in the context of Hopf–Galois structures in [37], this is also known as Byott's conjecture.

**Conjecture 1.1.8** (Byott's Conjecture)**.** *Let $A$ be a finite skew brace. If $(A,\cdot)$ is solvable, then $(A,\circ)$ is solvable.*

There is strong evidence that shows that this conjecture holds, see [38, 80, 162]. Conversely, if $(A,\circ)$ is nilpotent, then $(A,\cdot)$ is solvable, as proved by Tsang and Qin in [162, Theorem 1.3] as a consequence of the Kegel–Wielandt theorem. Examples contained in [161] show that solvability of $(A,\circ)$ does not imply solvability of $(A,\cdot)$. Moreover, results of Ito and Huppert imply that if $(A,\circ)$ is cyclic, then $(A,\cdot)$ is supersolvable, and if $(A,\circ)$ is abelian, then $(A,\cdot)$ is metabelian, as proved in [162, Theorem 1.3].

### 1.1.1 Regular subgroups of the holomorph

The crux of this thesis is that skew braces are inherently related to many other (algebraic) structures. Some well-known connections are those with regular subgroups of the holomorph, bijective 1-cocycles of groups, groups with compatible actions, braiding operators, see [83, 117]. The connection with regular subgroups of the holomorph will play a crucial role, so we give a full account of this correspondence.

Given a group $G$, its *holomorph* is the semidirect product $G \rtimes \mathrm{Aut}(G)$. We denote this group by $\mathrm{Hol}(G)$. There is a natural faithful action of $\mathrm{Hol}(G)$ on $G$, given by

$$(g,\lambda)\star h = g\lambda(h),$$

where $g,h \in G$, $\lambda \in \mathrm{Aut}(G)$. A subgroup $H \subseteq \mathrm{Hol}(G)$ is *regular* if it acts regularly (meaning freely and transitively) on $G$ through this action. Note that this means that for every $g \in G$ there exists a unique $h \in H$ such that $h \star 0 = g$, or equivalently that $H$ is regular if and only if for every $g \in G$ there exists a unique $\lambda \in \mathrm{Aut}(G)$ such that $(g,\lambda) \in H$.

**Proposition 1.1.9** ([83, Theorem 4.2])**.** *Let $(A,\cdot)$ be a group, there exists a bijective correspondence between operations $\circ$ such that $(A,\cdot,\circ)$ is a skew brace and regular subgroups of* $\mathrm{Hol}(A,\cdot)$.

*Proof.* Let $(A,\cdot,\circ)$ be a skew brace and consider the set

$$G = \{(a,\lambda_a) \mid a \in A\} \subseteq \mathrm{Hol}(A,\cdot).$$

We claim that $G$ is a subgroup of $\mathrm{Hol}(A,\cdot)$. Indeed, for $a,b \in A$ we find

$$(a,\lambda_a)(b,\lambda_b) = (a\cdot\lambda_a(b),\lambda_a\lambda_b) = (a\circ b,\lambda_{a\circ b}) \in G,$$

which shows that the map

$$(A,\circ) \to H : a \mapsto (a,\lambda_a),$$

is a group isomorphism. Since every element of $A$ appears as the first coordinate of precisely one element of $G$, the latter is regular.

Conversely, assume that $G$ is a regular subgroup of $\mathrm{Hol}(A,\cdot)$ and consider the map

$$\phi : G \to A : h \mapsto h\star 0.$$

Since $G$ acts regularly, $\phi$ is a bijection. We now define $(A,\circ)$ by transferring the group structure of $G$ to $A$, explicitly:

$$a\circ b = \phi(\phi^{-1}(a)\phi^{-1}(b)) = \phi^{-1}(a)\star b.$$

In order to see that these two groups satisfy (B), note that the map

$$\lambda_a : A \to A : b \mapsto a^{-1}\cdot(a\circ b),$$

which corresponds to the element $(a^{-1},0)\phi^{-1}(a)$, is contained in $\mathrm{Stab}_{\mathrm{Hol}(A,\cdot)}(0) = \{0\} \rtimes \mathrm{Aut}(A,\cdot)$. For $a,b,c \in A$ we find

$$\begin{aligned} a^{-1}\cdot(a\circ(b\cdot c)) &= ((a^{-1},0)\phi^{-1}(a)) \star (b\cdot c) \\ &= (((a^{-1},0)\phi^{-1}(a)) \star b)\cdot(((a^{-1},0)\phi^{-1}(a)) \star c) \\ &= a^{-1}\cdot(a\circ b)\cdot a^{-1}\cdot(a\circ c), \end{aligned}$$

from which (B) follows. □

**Lemma 1.1.10** ([39, Theorem 2.2])**.** *Let $(A,\cdot)$ be a group and $\lambda : A \to \mathrm{Aut}(A,\cdot)$ a map. Then $(A,\cdot,\circ)$ with $a\circ b := a\cdot\lambda_a(b)$ is a skew brace if and only if*

$$\lambda_{a\cdot\lambda_a(b)} = \lambda_a\lambda_b, \tag{1.1}$$

*for all $a,b \in A$.*

*Proof.* One implication is trivial since we know that the $\lambda$-map yields an action of $(A,\circ)$ on $(A,\cdot)$. Let $\lambda : A \to \mathrm{Aut}(A,\cdot)$ satisfying (1.1). By Proposition 1.1.9 it suffices to prove that, the set

$$G = \{(a,\lambda_a) \mid a \in A\},$$

is a regular subgroup of $\mathrm{Hol}(A,\cdot)$. Note that as soon as $H$ is a subgroup, it is automatically regular, so we really only need to prove that $G$ is a subgroup. From (1.1) we find

$$(a,\lambda_a)(b,\lambda_b) = (a\cdot\lambda_a(b),\lambda_a\lambda_b) = (a\cdot\lambda_a(b),\lambda_{a\cdot\lambda_a(b)}) \in G,$$

so $G$ is a subsemigroup of $\mathrm{Hol}(A,\cdot)$. Moreover, $(0,\lambda_0)(0,\lambda_0) = (0,\lambda_0^2) \in H$, which forces $\lambda_0 = \mathrm{id}$ and thus $G$ is a submonoid of $\mathrm{Hol}(A,\cdot)$. At last, note that for all $a \in A$ we find

$$(a,\lambda_a)(\lambda^{-1}(a^{-1}),\lambda_{\lambda_a^{-1}(a^{-1})}) = (0,\lambda_a\lambda_{\lambda_a^{-1}(a^{-1})}) = (0,\lambda_0) = (0,\mathrm{id}),$$

from which we conclude that $G$ is a subgroup. □

*Remark* 1.1.11. A map $\lambda : A \to \mathrm{Aut}(A,\cdot)$ satisfying (1.1) is by some authors called a *gamma function* on $(A,\cdot)$, see [39, 41].

## 1.1.2 Two-sided skew braces

**Definition 1.1.12.** A ring $A$ is *Jacobson radical* if for all $a \in A$ there exists an element $b \in A$ such that $a + b + ab = 0$. Equivalently, this happens precisely when $A$ coincides with its Jacobson radical, see for example [110] for more on this topic.

One easily verifies that for any given ring $A$, the operation $a\circ b := a + b + ab$ yields a monoid with neutral element 0, such that moreover (B) is satisfied. We find that $A$ is Jacobson radical if and only if $(A,+,\circ)$ is a brace. The braces that can be obtained in this way can be characterized in a precise way.

**Definition 1.1.13.** A skew brace $A$ is *two-sided* if also

$$(a\cdot b)\circ c = (a\circ c)\cdot c^{-1}\cdot(b\circ c), \tag{B'}$$

is satisfied for all $a,b,c \in A$.

**Proposition 1.1.14** ([132]). *The following data are equivalent on an abelian group $(A, +)$:*

1. *An operation $\circ$ such that $(A, +, \circ)$ is a two-sided brace.*

2. *An operation $*$ such that $(A, +, *)$ is a Jacobson radical ring.*

One direction of the correspondence in Proposition 1.1.14 is precisely as described earlier. Conversely, if $(A, +, \circ)$ is a two-sided skew brace, then, in order to obtain an inverse construction, we define the operation $*$ as

$$a * b = -a + a \circ b - b.$$

The following result is proved for left braces in [51, Remark 5.2] and one implication is proved for skew left braces in [123, Lemma 4.1]. The proof of the other implication is the same as for left braces.

**Proposition 1.1.15.** *A skew brace $A$ is two-sided if and only if all inner automorphisms of $(A, \circ)$ are skew brace automorphisms of $A$.*

**Corollary 1.1.16** ([123]). *Let $A$ be a two-sided skew brace and $I$ a characteristic subgroup of $(A, \cdot)$. Then $I$ is an ideal of $A$.*

Following the construction for braces given in Proposition 1.1.14, for an arbitrary skew brace $(A, \cdot, \circ)$ and $a, b \in A$ we define

$$a * b = a^{-1} \cdot (a \circ b) \cdot b^{-1}.$$

Surprisingly, a result by Lau states that, among braces, two-sided braces can be characterized completely in terms of the associativity of $*$, without explicitly requiring it to be right distributive.

**Proposition 1.1.17** ([111]). *A brace $A$ is two-sided if and only if $a * (b * c) = (a * b) * c$ for all $a, b, c \in A$.*

We note that Proposition 1.1.17 can not be extended to skew braces, see [107, Section 1]. Also, for braces, $*$ is left distributive with respect to the additive operation. This follows from the following lemma, which can be derived directly from (B).

**Lemma 1.1.18.** *Let $A$ be a skew left brace. Then for all $a, b, c \in A$, the following equalities hold:*

$$a * (b \cdot c) = (a * b) \cdot b \cdot (a * c) \cdot b^{-1},$$
$$(a \circ b) * c = (a * (b * c)) \cdot (b * c) \cdot (a * c).$$

Even though $*$ is usually not associative nor distributive, this operation is indispensable in the study of skew braces. For example, we can define left ideals, strong left ideals and ideals using $*$ instead. This highlights the similarity with the corresponding notions in ring theory.

**Lemma 1.1.19.** *Let $A$ be a skew brace and $L$ a subgroup of $(A, \cdot)$. Then $L$ is*

1. *a left ideal if and only if $a * x \in L$ for all $a \in A$, $x \in L$.*

2. *an ideal if and only if $L$ is normal in $(A, \cdot)$ and also $a * x, x * a \in L$ for all $a \in A$, $x \in L$.*

**Example 1.1.20.** Let $A$ be a skew brace. Then $A^2$, the subgroup of $(A, \cdot)$ generated by all elements of the form $a * b$, is an ideal of $A$. It is easily seen that for $I$ an ideal of $A$, $A/I$ is trivial if and only if $A^2 \subseteq I$.

**Example 1.1.21.** Let $A$ be a skew brace. Then $A^2_{\mathrm{op}}$, the subgroup of $(A,\cdot)$ generated by all elements of the form $a *_{\mathrm{op}} b$, is an ideal of $A$. By $*_{\mathrm{op}}$ we mean the $*$-operation in the opposite skew brace $A_{\mathrm{op}}$, thus $a *_{\mathrm{op}} b = b^{-1}\cdot(a\circ b)\cdot a^{-1}$. Clearly, for any ideal $I$ of $A$, the quotient $A/I$ is an almost trivial skew brace if and only if $A^2_{\mathrm{op}} \subseteq I$.

**Example 1.1.22.** Let $A$ be a skew brace, then $A' = A^2 \cdot A^2_{\mathrm{op}}$ is an ideal of $A$ see [116, Proposition 2.2], called the *commutator* of $A$. It is the smallest ideal of $A$ such that the quotient is a trivial brace. Alternatively, we can define $A'$ as the ideal generated by $A^2$ and the commutator subgroup of $(A,\cdot)$.

### 1.1.3 Nilpotency

Since in any skew brace $A$ we have $a * b = 0$ if and only if $a\cdot b = a\circ b$, the operation $*$ should be seen as a measure of how similar both group operations are, or equivalently, how close $A$ is to being a trivial skew brace. If $A$ is an almost trivial skew brace, then we find $a*b = \overline{b}\circ a\circ b\circ\overline{a}$, which is precisely the commutator of $\overline{b}$ and $a$ in the group $(A,\circ)$. Also, within the context of two-sided braces, the operation $*$ is precisely the ring operation of the associated Jacobson radical ring. With this in mind, it is natural to use this operation to define nilpotency of a skew brace. However, $*$ is not associative, so there are multiple variations to be distinguished.

For $X, Y \subseteq A$ we define $X * Y$ as the additive subgroup of $A$ generated by the set

$$\{x * y \mid x \in X, y \in Y\}.$$

**Definition 1.1.23.** For a skew brace $A$ we define $A^1 = A$ and $A^{n+1} = A * A^n$ for $n \geq 1$. The descending series of strong left ideals

$$A^1 \supseteq A^2 \supseteq A^3 \supseteq \dots$$

is called the *left series* of $A$. If there exists some $n \geq 1$ such that $A^n = \{0\}$, we say that $A$ is *left nilpotent*. In this case, the smallest $n \geq 0$ such that $A^{n+1} = \{0\}$ is called the *left nilpotency class* of $A$.

Left nilpotency has direct implications on the structure of the additive and multiplicative group of a skew brace, see [55, Theorem 4.6], and under some extra conditions it coincides with nilpotency of the multiplicative group.

**Theorem 1.1.24** ([55, Theorem 4.8, Corollary 4.9])**.** *Let $A$ be a finite skew brace with $(A,\cdot)$ a nilpotent group. Then $A$ is left nilpotent if and only if $(A,\circ)$ is nilpotent. In particular, skew braces of prime power size are left nilpotent.*

In the finite setting, skew braces of prime power size are the archetypal example of left nilpotent skew braces with nilpotent additive group, as the following result shows.

**Proposition 1.1.25** ([55, Corollary 4.3])**.** *Let $A$ be a finite left nilpotent skew brace such that $(A,\cdot)$ is nilpotent. Then $A$ is isomorphic to a direct product of skew braces of prime power size.*

**Definition 1.1.26.** For a skew brace $A$ we define $A^{(1)} = A$ and $A^{(n+1)} = A^{(n)} * A$ for $n \geq 1$. The descending series of ideals

$$A = A^{(1)} \supseteq A^{(2)} \supseteq A^{(3)} \supseteq \dots$$

is called the *right series* of $A$. We say that $A$ is *right nilpotent* if the right series reaches the zero skew brace. In this case, the smallest $n \geq 0$ such that $A^{(n+1)} = \{0\}$ is called its *right nilpotency class*.

**Definition 1.1.27** ([55, 132])**.** Let $A$ be a skew brace. We set $\mathrm{Soc}_0(A) = \{0\}$ and we inductively define $\mathrm{Soc}_{n+1}(A)$ as the ideal of $A$ corresponding to $\mathrm{Soc}(A/\mathrm{Soc}_n(A))$. The resulting ascending series of ideals

$$\{0\} = \mathrm{Soc}_0(A) \subseteq \mathrm{Soc}_1(A) = \mathrm{Soc}(A) \subseteq \mathrm{Soc}_2(A) \subseteq \dots$$

is called the *socle series* of $A$. The skew brace $A$ has *finite multipermutation level* (or simply, $A$ is *multipermutation*) if there exists $n$ such that $\mathrm{Soc}_n(A) = A$. In this case, the smallest such $n \geq 0$ is called the *multipermutation level* of $A$, which we denote by $\mathrm{mpl}(A)$.

A brace $A$ is right nilpotent if and only if it has finite multipermutation level, and moreover, the right nilpotency class and multipermutation level coincide. In the more general setting, this is not true.

**Proposition 1.1.28** ([55, Theorem 2.20])**.** *A skew brace $A$ has finite multipermutation level if and only if it is right nilpotent and the group $(A, \cdot)$ is nilpotent.*

**Definition 1.1.29** ([55, 145])**.** For a skew brace $A$ we define $A^{[1]} = A$ and, for $n \geq 1$, $A^{[n+1]}$ is the additive subgroup generated by $\bigcup_{i=1}^{n} A^{[i]} * A^{[n+1-i]}$. We say that $A$ is *strongly nilpotent* if there exists some $n \geq 1$ such that $A^{[n]} = \{0\}$. In this case, the smallest $n \geq 0$ such that $A^{[n+1]} = \{0\}$ is called its *strong nilpotency class*.

**Theorem 1.1.30** ([55, Theorem 2.30])**.** *A skew brace is strongly nilpotent if and only if it is both left and right nilpotent.*

For two-sided braces, the notions of left, right and strong nilpotency coincide with nilpotency of the associated Jacobson radical ring. Similarly, for almost trivial skew braces, left, right and strong nilpotency coincide with nilpotency of the underlying group.

For completeness sake, we also mention that a skew brace $A$ is *annihilator nilpotent* or *centrally nilpotent* if there exists some $n$ such that $\mathrm{Ann}_n(A) = A$, where the annihilator series $\mathrm{Ann}_n(A)$ is defined in a similar way as the socle series. A skew brace $A$ is annihilator nilpotent precisely when it is strongly nilpotent and $(A, \cdot)$ is a nilpotent group. Within the setting of universal algebra, this is the correct notion of nilpotency, see [21, 93].

**Definition 1.1.31.** For a skew brace $A$ we define $A_{(1)} = A$ and $A_{(n+1)} = A_{(n)} * A_{(n)}$ for $n \geq 0$. We say that $A$ is *solvable* if there exists some $n \geq 1$ such that $A_{(n)} = \{0\}$ and the smallest $n$ such that $A_{n+1} = \{0\}$ is called its *derived length*.

*Remark* 1.1.32. We follow here the convention of [13] in order to define solvable skew braces. There also exist different notions of solvability of skew braces, see for example [16].

### 1.1.4 Bi-skew braces

A skew brace $(A, \cdot, \circ)$ is a *bi-skew brace* if also $(A, \circ, \cdot)$ is a skew brace. In this case, when no confusion is possible, we will refer to the starting skew brace $(A, \cdot, \circ)$ as $A$ and to the skew brace with exchanged operations $(A, \circ, \cdot)$ as $A_{\leftrightarrow}$. When $A$ is a bi-skew brace, the $\lambda$-map of $A_{\leftrightarrow}$, denoted by $\lambda^{\leftrightarrow}$, is directly related to that of $A$ since

$$\lambda_a^{\leftrightarrow}(b) = \overline{a} \circ (a \cdot b) = \lambda_a^{-1}(b).$$

In particular, this implies that $\lambda_a$ is an automorphism $(A, \circ)$, and thus of $(A, \cdot, \circ)$, since it is the additive group of $A_{\leftrightarrow}$. The following lemma completely characterizes when $\lambda_a$ is a skew brace automorphism of $A$.

**Lemma 1.1.33.** *Let $A$ be a skew brace and $a \in A$. Then $\lambda_a \in \mathrm{Aut}(A, \cdot, \circ)$ if and only if $\lambda_{a\cdot b} = \lambda_{b\circ a}$ for all $b \in A$.*

*Proof.* Let $a \in A$. Since $\lambda_a$ is always an automorphism of the group $(A, \cdot)$, it suffices to characterize when it is an automorphism of $(A, \circ)$. For $b, c \in A$ we find

$$\lambda_a(b \circ c) = \lambda_a(b \cdot \lambda_b(c)) = \lambda_a(b) \cdot \lambda_a\lambda_b(c) = \lambda_a(b) \circ \lambda^{-1}_{\lambda_a(b)}\lambda_a\lambda_b(c),$$

so this expression equals $\lambda_a(b) \circ \lambda_a(c)$ whenever $\lambda_a = \lambda^{-1}_{\lambda_a(b)}\lambda_a\lambda_b$. After bringing $\lambda^{-1}_{\lambda_a(b)}$ over to the left an substituting $b$ by $\lambda_a^{-1}(b)$ we find the equation $\lambda_{b\circ a} = \lambda_{a\circ\lambda_a^{-1}(b)} = \lambda_{a\cdot b}$. □

The following characterization of bi-skew braces using the $\lambda$-function is an extended version of a result by Caranti [41, Theorem 3.1].

**Theorem 1.1.34.** *Let $A$ be a skew brace. Then the following are equivalent:*

1. *$A$ is a bi-skew brace.*
2. *$\lambda_a$ is a skew brace automorphism for all $a \in A$.*
3. *$\lambda : (A, \cdot) \to \mathrm{Aut}(A, \cdot)$ is a group antihomomorphism.*
4. *$A^2_{\mathrm{op}}$ is contained in $\ker\lambda$.*
5. *$A^2_{\mathrm{op}} * A = \{0\}$.*

*Proof.* The implication from 1 to 2 is contained in the discussion preceding Lemma 1.1.33. Conversely, note that if $\lambda_a$ is a skew brace automorphism for all $a \in A$, then we can use Lemma 1.1.33 to find

$$\lambda^{-1}_{a\circ\lambda_a^{-1}(b)} = \lambda^{-1}_{a\cdot b} = \lambda^{-1}_{b\circ a} = \lambda_a^{-1}\lambda_b^{-1}.$$

This implies that the map

$$A \to (A, \circ) : a \mapsto \lambda_a^{-1},$$

satisfies the condition of Lemma 1.1.10 and thus $(A, \circ, \cdot)$ is a skew brace since $a \cdot b = a \circ \lambda_a^{-1}(b)$.

The equivalence of 2 and 3 follows directly from Lemma 1.1.33.

To see that 3 implies 4, note that from 3 it follows that $\lambda : (A, \cdot, \circ) \to \mathrm{opTriv}(\mathrm{Aut}(A, \cdot))$ is a skew brace homomorphism. Since the image $\lambda(A) \cong A/\ker\lambda$ is almost trivial, this implies that $A^2_{\mathrm{op}} \subseteq \ker\lambda$. Conversely, if $A^2_{\mathrm{op}}$ is contained in $\ker\lambda$ then $\ker\lambda$ is an ideal of $A$, since ideals of $A/A^2_{\mathrm{op}}$ correspond to normal subgroups of its multiplicative group. Since $\ker\lambda$ is an ideal and $a *_{\mathrm{op}} b \in \ker\lambda$, we find $b \cdot a \cdot \ker\lambda = (a \circ b) \cdot \ker\lambda$ and thus $\lambda_{b\cdot a} = \lambda_{a\circ b}$.

The equivalence of 4 and 5 is clear since an element $a \in A$ is contained in $\ker\lambda$ if and only if $a * b = 0$ for all $b \in A$. □

Let $(A, \cdot, \circ)$ be a skew brace. Then $(A, \cdot, \circ)$ is *$\lambda$-homomorphic* if $\lambda_{a\cdot b} = \lambda_a\lambda_b$ for all $a, b \in A$. The class of $\lambda$-homomorphic skew braces was first defined and studied by Bardakov, Neshchadim and Yadav in [18]. Combined with Theorem 1.1.34 we recover the following result.

**Lemma 1.1.35** ([41, Lemma 3.7])**.** *Let $A$ be a skew brace. Then any two of the following statements imply the third:*

1. *$A$ is $\lambda$-homomorphic.*
2. *$A$ is a bi-skew brace.*
3. *$\lambda(A)$ is abelian.*

If one pushes the idea of a bi-skew brace further in order to allow more than two group structures, the definition of a brace block arises naturally. In particular, every non-trivial bi-skew brace gives rise to a brace block with two distinct operations.

**Definition 1.1.36.** Let $A$ be a set. A *brace block*, denoted by $(A, \circ_i)_{i\in I}$, consists of a family of group operations $(\circ_i)_{i\in I}$ on $A$ such that $(A, \circ_i, \circ_j)$ is a bi-skew brace for all $i, j \in I$.

### 1.1.5 Skew braces on Lie groups

In [15], Bai, Guo, Sheng and Tang introduce the notion of a post-group and prove that this coincides with that of a skew brace.

**Definition 1.1.37.** A *post-group* is a group $(A, \cdot)$ equipped with a map $\lambda : A \to \mathrm{Aut}(A, \cdot)$ satisfying $\lambda_{a\cdot\lambda_a(b)} = \lambda_a\lambda_b$ for all $a, b \in A$.

*Remark* 1.1.38. Note that the original definition of post groups is defined in terms of the binary operation $(a, b) \mapsto \lambda_a(b)$, but we freely use the fact that binary operations on $A$ are equivalent to maps $A \to \mathrm{Fun}(A, A)$ where $\mathrm{Fun}(A, A)$ denotes the set of maps $A \to A$.

It is an immediate consequence of Lemma 1.1.10 that post-groups on $(A, \cdot)$ are equivalent to skew brace structures $(A, \cdot, \circ)$, where the relation is given by the usual expression $a \circ b = a \cdot \lambda_a(b)$. In the same paper, the authors also introduce post-Lie groups.

**Definition 1.1.39.** A *post-Lie group* is a Lie group $(A, \cdot)$ equipped with a map $\lambda : A \to \mathrm{Aut}(A, \cdot)$ satisfying $\lambda_{a\cdot\lambda_a(b)} = \lambda_a\lambda_b$ for all $a, b \in A$ and such that $A \times A \to A : (a, b) \mapsto \lambda_a(b)$ is a smooth map.

**Proposition 1.1.40.** *Let $A$ be a differentiable manifold and let $(A, \cdot, \circ)$ be a skew brace structure on $A$ such that $(A, \cdot)$ is a Lie group. Then $(A, \circ)$ is a Lie group if and only if its associated post-group is a post-Lie group.*

*Proof.* Let $A$ be a differentiable manifold and let $(A, \cdot, \circ)$ be a skew brace structure on $A$ such that $(A, \cdot)$ is a Lie group. Then the map

$$A \times A \to A : (a, b) \mapsto \lambda_a(b) = a^{-1} \cdot (a \circ b) \tag{1.2}$$

is smooth. Conversely, if (1.2) is smooth, then multiplication in $(A, \circ)$ is also smooth since $a \circ b = a \cdot \lambda_a(b)$. Also, note that the assumption implies that $\lambda_a$ is smooth for all $a$, so also $\lambda_{\overline{a}} = \lambda_a^{-1}$ is smooth and thus $\lambda_a$ is an automorphism of the Lie group $(A, \cdot)$. Since the automorphism group of a Lie group is itself a Lie group, we find that $a \mapsto \lambda_a^{-1}$ is smooth. Combined with the fact that inversion is smooth in $(A, \cdot)$, we conclude that the inversion map of $(A, \circ)$ is smooth since $\overline{a} = \lambda_a^{-1}(a^{-1})$. □

The following definition is now natural. When $(A, \cdot)$ is a Lie group, we denote its group of Lie group automorphisms by $\mathrm{Aut}^\infty(A, \cdot)$ and $\mathrm{Hol}^\infty(A, \cdot) := (A, \cdot) \rtimes \mathrm{Aut}^\infty(A, \cdot)$. Note that both are Lie groups.

**Definition 1.1.41.** A *skew Lie brace* is a skew brace $(A, \cdot, \circ)$ with $A$ a differentiable manifold and $(A, \cdot)$ and $(A, \circ)$ Lie groups.

**Proposition 1.1.42.** *Let $A$ be a differentiable manifold and let $(A, \cdot)$ be a Lie group. Then the following data are equivalent:*

1. *An operation $(A, \circ)$ such that $(A, \cdot, \circ)$ is a skew Lie brace.*
2. *A map $\lambda : A \to \mathrm{Aut}(A, \cdot)$ such that $(A, \cdot, \lambda)$ is a post-Lie group.*
3. *A regular Lie subgroup of $\mathrm{Hol}^\infty(A, \cdot)$.*

*Proof.* The equivalence between 1 and 2 is precisely the content of Proposition 1.1.40. We now prove the equivalence of 1 and 3. We claim that the correspondence described in Proposition 1.1.9 restricts to this specific case. Indeed, assume that $(A, \cdot, \circ)$ is a skew Lie brace, then we know from Proposition 1.1.40 that $\lambda : A \to \mathrm{Aut}^\infty(A, \cdot)$ is smooth, hence

$$(A, \circ) \to \mathrm{Hol}^\infty(A, \cdot) : a \mapsto (a, \lambda_a),$$

is an injective homomorphism of Lie groups, with image precisely the associated regular subgroup.

Conversely, let $G$ be a regular Lie subgroup of $\mathrm{Hol}^\infty(A, \cdot)$. Then we know that there exists a Lie group $H$ and an injective homomorphism of Lie groups $f : H \to \mathrm{Hol}^\infty(A, \cdot)$ such that $f(H) = G$, thus we obtain a regular smooth action of $G$ on $A$. The smooth map

$$\phi : H \to G : h \mapsto f_h(1_G),$$

then has constant rank. Indeed, if we let $\mathcal{L}_h : H \to H$ denote left multiplication by $h \in H$, then $\phi\mathcal{L}_h = f_h\phi$ and thus

$$d\phi|_h \circ d\mathcal{L}_h|_{1_H} = df_h|_{1_G} \circ d\phi|_{1_H}.$$

Since both $\mathcal{L}_h$ and $f_h$ are diffeomorphisms, we find that $\phi$ has constant rank. Since it is moreover a smooth bijection, it follows that it is a diffeomorphism. Recall that the operation $\circ$ associated to $G$ is given by

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

so we conclude that $(A, \circ)$ is a Lie group. We remark that the precise choice of $H$ and $f$ does not affect the construction. Indeed, the group $(A, \circ)$ is determined by $G$, we only needed $H$ and $f$ to conclude that multiplication and inversion in $(A, \circ)$ are smooth. □

## 1.2 Set-theoretical solutions of the Yang–Baxter equation

Braces and skew braces were originally introduced as algebraic tools to study set-theoretical solutions of the Yang–Baxter equation. Although their utility and importance are by now much broader than this original motivation, the majority of research on skew braces so far has focused on (or was motivated by) this connection. We cannot do full justice to the full history and importance of the Yang–Baxter equation, so we content ourselves with a short motivation coming from representations of braid groups, which we also hope gives some additional insight into notions like non-degeneracy or the derived solution. For the interested reader, we refer to Chapter 1 of the PhD thesis of Verwimp [166], which touches upon multiple topics where the Yang–Baxter equation appears.

A pair $(V, R)$, with $V$ a vector space and $R : V \otimes V \to V \otimes V$ a linear map, is a *solution of the Yang–Baxter equation* if it satisfies

$$R_{12}R_{23}R_{12} = R_{23}R_{12}R_{23}, \tag{YBE}$$

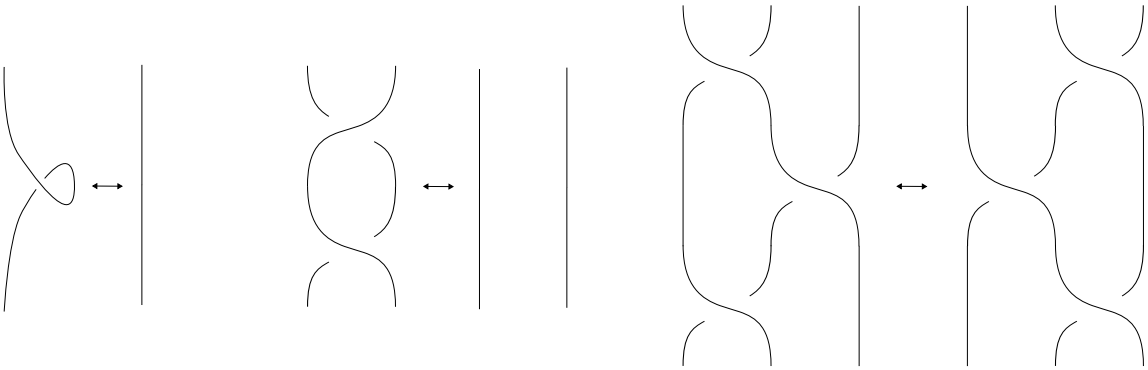


Figure 1.1: From left to right: the first, second and third Reidemeister move.

on $V^{\otimes 3}$, where $R_{ij}$ denotes the map $V^{\otimes 3} \to V^{\otimes 3}$ acting as $R$ on the $(i, j)$ tensor factor and as the identity of the remaining factor. This equation can be understood as the third Reidemeister move, one of the three local moves that suffice to relate any two knot diagrams belonging to the same knot, as independently demonstrated by Reidemeister [129] and Alexander and Garland [3], see Fig. 1.1.

An algebraic interpretation of $n$-braids, for $n \geq 2$, is given by the braid group

$$B_n = \langle b_i, 1 \leq i < n \mid b_i b_j = b_j b_i \text{ for } |i-j| > 1, b_i b_{i+1} b_i = b_{i+1} b_i b_{i+1} \text{ for } 1 \leq i < n \rangle.$$

Here, the generator $b_i$ corresponds to swapping the strand at position $i+1$ over that at position $i$. The second relation in the definition corresponds to the third Reidemeister move; the other relation relates to the fact that if two disjoint pairs of strands are swapped, then these operations do not affect each other and thus they commute. Note that, if we further impose the relations that $b_i^2 = 1$ for all $1 \leq i \leq n$, then the obtained group is isomorphic to the symmetric group $\mathbb{S}_n$, where $b_i$ corresponds to the transposition $(i\ i+1)$. The following proposition follows directly from the relations on $B_n$.

**Proposition 1.2.1.** *Let $V$ be a vector space and $R : V \otimes V \to V \otimes V$ a bijective linear map. For $n \geq 3$, the assignment $b_i \mapsto R_{i,i+1}$, extends to an action of $B_n$ on $V^{\otimes n}$ if and only if $R$ is a solution of the YBE. In the same manner it extends to an action of $\mathbb{S}_n$ on $V^{\otimes n}$ if and only if moreover $R^2 = \mathrm{id}_{V^{\otimes 2}}$.*

If one fixes a basis $X$ of $V$ and imposes the restriction that $r$ should map the associated basis

$$\{x \otimes y \mid x, y \in X\},$$

into itself then we find that $r$, interpreted as a map $r : X^2 \to X^2$, satisfies

$$r_{12} r_{23} r_{12} = r_{23} r_{12} r_{23}, \tag{SYBE}$$

where similar as before $r_{ij} : X^3 \to X^3$ acts as $r$ on coordinates $(i, j)$ and as the identity on the remaining coordinate. A pair $(X, r)$ where $X$ is a non-empty set and $r : X^2 \to X^2$ is a map satisfying (SYBE) is a *set-theoretical solution of the Yang–Baxter equation*. A solution $(X, r)$ is *bijective* if $r$ is bijective, *finite* if $X$ is a finite set and *involutive* if $r^2 = \mathrm{id}_{X^2}$. Given two set-theoretical solutions of the Yang–Baxter equation $(X, r)$ and $(Y, s)$, a map $f : X \to Y$ is a *homomorphism* if $s(f \times f) = (f \times f)r$. Moreover, $f$ is an *isomorphism of solutions* if it is also bijective. We obtain the following obvious variation of Proposition 1.2.1.

**Proposition 1.2.2** ([73, Proposition 1.1]). *Let $X$ be a non-empty set and $r : X^2 \to X^2$ a map. For $n \geq 3$, the assignment $b_i \mapsto r_{i,i+1}$ extends to an action of $B_n$ on $X^n$ if and only if $(X, r)$ is a bijective solution of the YBE. In the same manner, it extends to an action of $\mathbb{S}_n$ on $X^n$ if and only if moreover $(X, r)$ is involutive.*

In the proceedings of a workshop on quantum groups held at the Euler International Mathematical Institute in 1990, while discussing some open problems in quantum group theory [72], Drinfeld wrote: "Maybe it would be interesting to study set-theoretical solutions of the Yang–Baxter equation." He also included the following two examples and stated that they are the only thing he knows about set-theoretical solutions of the YBE, accrediting them to Lyubashenko and Venkov respectively. In this way, he arguably, single-handedly and with only a single paragraph, initiated a completely new field of mathematics.

**Example 1.2.3** (Lyubashenko). Let $X$ be a non-empty set and $\sigma, \tau : X \to X$ maps. Then $r(x, y) = (\sigma(y), \tau(x))$ satisfies (SYBE) if and only if $\sigma\tau = \tau\sigma$. It is involutive if and only if $\sigma = \tau^{-1}$.

**Example 1.2.4** (Venkov). Let $X$ be a non-empty set and $\triangleright$ a binary operation on $X$. Then $r(x, y) = (y, y \triangleright x)$ satisfies (SYBE) if and only if

$$x \triangleright (y \triangleright z) = (x \triangleright y) \triangleright (x \triangleright z),$$

for all $x, y, z \in X$. Moreover, $r$ is involutive only if $x \triangleright y = y$ for all $x, y \in X$.

For $(X, r)$ a set-theoretical solution of the Yang–Baxter equation, we introduce the notation

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

where $x, y \in X$. Hence, we obtain maps $\sigma_x, \tau_x : X \to X$ for all $x \in X$ and we say that $(X, r)$ is *non-degenerate* if all the maps $\sigma_x, \tau_x$ are bijective for all $x \in X$. We can express (SYBE) in terms of the maps $\sigma_x, \tau_x$.

**Lemma 1.2.5** ([73, Proposition 2.1]). *Let $X$ be a set and $\{\sigma_x, \tau_x : X \to X \mid x \in X\}$ a collection of maps. Then $(X, r)$ with $r$ given by*

$$r : X^2 \to X^2 : (x, y) \mapsto (\sigma_x(y), \tau_y(x)),$$

*is a set-theoretical solution of the Yang–Baxter equation if and only if the equations*

$$\sigma_x\sigma_y(z) = \sigma_{\sigma_x(y)}\sigma_{\tau_y(x)}(z), \tag{1.3}$$

$$\tau_x\tau_y(z) = \tau_{\tau_x(y)}\tau_{\sigma_y(x)}(z), \tag{1.4}$$

$$\tau_{\sigma_{\tau_y(x)}(z)}\sigma_x(y) = \sigma_{\tau_{\sigma_y(z)}(x)}\tau_z(y), \tag{1.5}$$

*hold for all $x, y, z \in X$. Moreover, $(X, r)$ is involutive if and only if also*

$$\tau_y(x) = \sigma^{-1}_{\sigma_x(y)}(x) \tag{1.6}$$

*holds for all $x, y \in X$.*

**Example 1.2.6.** Let $X$ be a non-empty set, then $(X, \mathrm{id}_{X^2})$ is an involutive set-theoretical solution of the Yang–Baxter equation which is degenerate since $\sigma_x(y) = x$ and $\tau_x(y) = x$ for all $x, y \in X$.

**Example 1.2.7.** Let $X$ be a non-empty set and define $r(x, y) = (y, x)$, for all $x, y \in X$. Then $(X, r)$ is an involutive non-degenerate solution since $\sigma_x = \tau_x = \mathrm{id}_X$ for all $x \in X$. This is a particular case of Example 1.2.3. We call this the *trivial solution* on $X$. Note that some authors use the term trivial solution only if additionally $|X| = 1$.

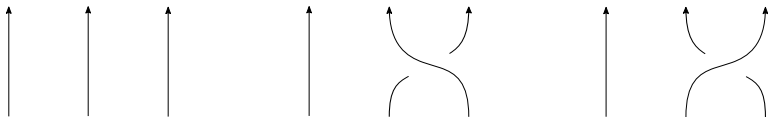


Figure 1.2: From left to right: the braid diagrams corresponding to 1, $b_2$ and $b_2^{-1}$ in $B_3$.

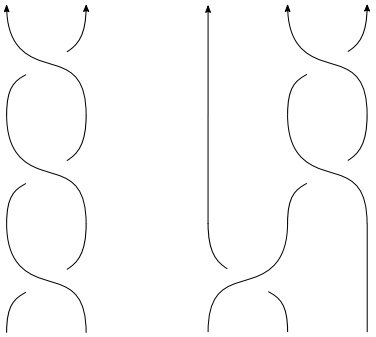


Figure 1.3: The braid diagrams corresponding to the elements $b_1^3 \in B_2 \cong \mathbb{Z}$ (left) and $b_2^2 b_1^{-1} \in B_3$ (right).

**Example 1.2.8.** For set-theoretical solutions as described in Example 1.2.3, an easy verification shows that both bijectivity and non-degeneracy coincide with the maps $\sigma$ and $\tau$ being invertible. In this case, we call $(X, r)$ a *permutation solution*.

**Example 1.2.9.** For set-theoretical solutions coming from a self-distributive operation $(X, \triangleright)$ as described in Example 1.2.4, bijectivity and non-degeneracy also coincide. Moreover, these properties are satisfied if and only for each $x \in X$, the left multiplication map $X \to X : y \mapsto x \triangleright y$ is bijective. In that case, $(X, \triangleright)$ is a *rack*.

### 1.2.1 Braid diagrams

Let us discuss a graphical way of interpreting the non-degeneracy condition. We solely provide this in order to gain some intuition; this discussion is not essential for the continuation of the thesis. We first define the braid diagram associated with an element of $B_n$. For the identity $1 \in B_n$, its associated braid diagram is the *trivial braid diagram* which consists of $n$ upwards oriented strands. For a generator $b_i \in B_n$, its associated braid diagram consists of $n$ upwards pointing strands where the $i+1$-th strand moves over the $i$-th strand, as illustrated in Fig. 1.2. The braid diagram associated with $b_i^{-1}$ is the same, except that the $i+1$-th strand passes under the $i$-th one. Now let $g$ be any element of $B_n$, fix some word $w$ in the generators $b_1, \ldots, b_{n-1}$ which represents the element $g$. Then, we obtain the braid diagram of $g$ by composing the braid diagram of the generators appearing in $w$. Here we read $w$ from right to left, and the composition of braid diagrams is performed upwards. Note that this construction is dependent on the choice of $w$. We say that two braid diagrams are *equivalent* if they can be obtained from words $w, w'$ both representing the same element $g \in B_n$. From the defining relations of $B_n$, it follows that braid diagrams are equivalent if and only if they can be transformed one into another using only the second and third Reidemeister move.

Let $(X, r)$ be a bijective set-theoretical solution of the YBE and let $\mathcal{D}$ be a braid diagram. A *segment* of $\mathcal{D}$ is a connected piece of a strand whose delimiting points are either a crossing or the start or end of a strand. We denote the set of all segments of $\mathcal{D}$ by $\mathrm{Segm}(\mathcal{D})$. An $(X, r)$-coloring of $\mathcal{D}$ is a map $C : \mathrm{Segm}(\mathcal{D}) \to X$,

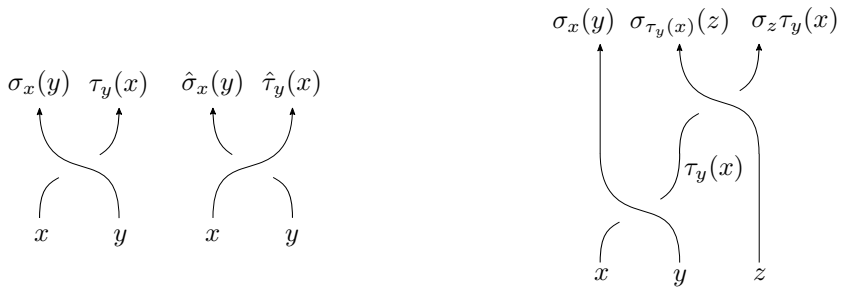



Figure 1.4: Left: the required conditions for a $(X, r)$-coloring of a braid diagram. Right: an example of a coloring, which can also be interpreted as graphical way of calculating of $b_2b_1 \in B_3$ acting on a triple $(x, y, z) \in X^3$, the result is then recovered from the top segments as $(\sigma_x(y), \sigma_{\tau_y(x)}(z), \sigma_z\tau_y(x))$.

assigning to each segment $s$ its *color* $C(s)$, such that each crossing looks like illustrated in Fig. 1.4. Hereby, we mean that when we have a crossing where the right hand strand passes over the left hand one, and the bottom left segment has color $x$ and the bottom right segment has color $y$, then the upper left segment has color $\sigma_x(y)$ and the upper right segment has color $\tau_y(x)$. Conversely, if we have a crossing where the left-hand strand passes over the right-hand one, and the bottom left and right segments have colors $x$ and $y$ respectively, then the upper left and right segments have colors $\hat{\sigma}_x(y)$ and $\hat{\tau}_y(x)$ respectively. Here the maps $\hat{\sigma}_x, \hat{\tau}_x : X \to X$ are defined by

$$r^{-1}(x, y) = (\hat{\sigma}_x(y), \hat{\tau}_y(x)).$$

It follows directly from the defining conditions that an $(X, r)$-coloring of a braid diagram is determined completely by the colors of the bottom segments, or more generally by the colors of all segments intersected by a horizontal line. If $\mathcal{D}$ and $\mathcal{D}'$ are equivalent braid diagrams, then any coloring on $\mathcal{D}$ uniquely determines a coloring on $\mathcal{D}'$ since $r$ satisfies the braid equation. The following lemma now gives an interpretation of the non-degeneracy condition in terms of colorings.

**Lemma 1.2.10.** *Let $(X, r)$ be a bijective set-theoretical solution of the Yang–Baxter equation and let $\mathcal{D}$ be a non-trivial braid diagram on $n$ strands. Then $r$ is non-degenerate if and only if for any $(X, r)$-coloring of a braid diagram, the colors of any two adjacent segments of a crossing determine the colors of the remaining segments.*

## 1.2.2 The structure skew brace

For the rest of this section, let $(X, r)$ be a non-degenerate bijective set-theoretical solution of the Yang–Baxter equation. From now on, we will refer to a non-degenerate bijective set-theoretical solution of the Yang–Baxter equation as a *solution of the YBE*, or simply as a *solution*. This subsection is dedicated to the construction of a universal skew brace associated to $(X, r)$, the structure skew brace. See [115] for a more extensive discussion of this topic.

The *structure group* of $(X, r)$ is defined as

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

It is a direct consequence of (1.3) that the map sending a generator $x \in G(X, r)$ to $\sigma_x$ defines a group homomorphism

$$\sigma : (G(X, r), \circ) \to \mathbb{S}_X,$$

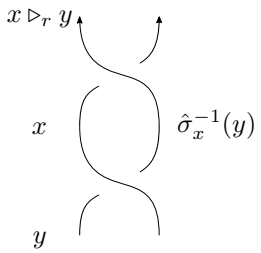



Figure 1.5: The definition of the operation $\triangleright_r$ in terms of coloring of a braid diagram.

and thus $\sigma$ defines an action of $(G(X,r),\circ)$ on $X$. We also associate to $(X,r)$ its *(left) derived solution* $(X,r')$ with $r'(x,y) = (y, y \triangleright_r x)$ with $y \triangleright_r x = \sigma_y \hat{\sigma}_y^{-1}(x)$. In terms of colorings of a diagram, this says that if we have two consecutive crossings and we look at the three consecutive segments on the left then reading from the bottom up, if the first two segments have colors $y$ and $x$, the third segment has color $x \triangleright_r y$. See also Fig. 1.5. The following statement follows trivially.

**Lemma 1.2.11.** *Let $(X,r)$ be a solution. Then its derived solution $(X,r')$ is trivial if and only if $(X,r)$ is involutive.*

For any $x \in X$, the permutation $\sigma_x$ is an automorphism of the rack $(X, \triangleright_r)$, meaning that

$$\sigma_x(y \triangleright_r z) = \sigma_x(y) \triangleright_r \sigma_x(z),$$

for all $y, z \in X$. The *(left) derived structure group* of $(X,r)$ is defined as

$$(A(X,r),\cdot) = \langle x \in X \mid x \cdot y = y \cdot (y \triangleright_r x) \text{ for all } x, y \in X \rangle.$$

Equivalently, $A(X,r)$ is the structure group of the derived solution $(X,r')$. Since the permutations $\sigma_x$ are automorphisms of $(X, \triangleright_r)$, we find that the earlier constructed action $\sigma$ in fact yields an action of $(G(X,r),\circ)$ on the rack $(X, \triangleright_r)$. In particular, we obtain a corresponding action of $(G(X,r),\circ)$ on $(A(X,r),\cdot)$.

**Example 1.2.12.** Consider the trivial solution $(X,r)$ on a non-empty set $X$. Then $(G(X,r),\circ)$ is the free abelian group on the set $X$.

**Example 1.2.13.** Let $n, a \in \mathbb{Z}$ and set $X = \mathbb{Z}/n$. We consider the permutation solution $(X,r)$ with

$$r(i,j) = (j, i+a).$$

Then in $G(X,r)$ we find, where we for readability represent the generator corresponding to $i \in \mathbb{Z}/n$ by $x_i$:

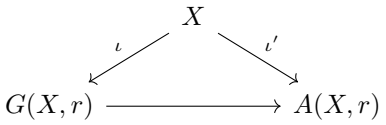
$$x_i \circ x_j = x_j \circ x_{i+a}.$$

In particular, from $i = j$, we find $x_i = x_{i+a}$ which also implies $x_i \circ x_j = x_j \circ x_{i+a} = x_j \circ x_i$. We find that $(G(X,r),\circ)$ is isomorphic to the free abelian group on the set $\mathbb{Z}/(n\mathbb{Z} + a\mathbb{Z})$. In particular, the canonical map $X \to G(X,r)$ is injective only if $(X,r)$ is trivial. Note also that the derived solution coincides with $(X,r)$ since $r^{-1}(i,j) = (j-a, i)$ and thus $i \triangleright_r j = \sigma_i \hat{\sigma}_i^{-1}(j) = \sigma_i(j+a) = j + a$. This holds more generally for all solutions coming from a rack, as in Example 1.2.4.

We are now ready to formulate the first half of [152, Theorem 2.6] and [117, Theorem 4], which were independently proved and state the same result in terms of bijective 1-cocycles and braiding operators respectively.

**Theorem 1.2.14.** *Let $(X,r)$ be a solution. Then there exists a group structure $(G(X,r),\cdot)$, completely determined by the property $x\cdot y = x\circ\sigma_x^{-1}(y)$, such that $(G(X,r),\cdot,\circ)$ is a skew brace. Moreover, $(G(X,r),\cdot)$ is isomorphic to $(A(X,r),\cdot)$, where the isomorphism maps a generator $x\in G(X,r)$ to the corresponding generator of $A(X,r)$.*

*Remark* 1.2.15. As seen in Example 1.2.13, the canonical map $\iota : X \to G(X,r)$, mapping an element $x\in X$ to its corresponding generator of $(G(X,r),\circ)$, is not always injective. Solutions for which $\iota$ is injective are called *injective* solutions. Note that the group isomorphism $(G(X,r),\cdot)\to(A(X,r),\cdot)$ in Theorem 1.2.14 is the unique one such that




commutes. Here, $\iota'$ is the canonical map from $X$ to $A(X,r)$. If we remark that $A(X,r)$ is isomorphic to the structure group of the derived solution, then we immediately find that $(X,r)$ is injective if and only if $(X,r')$ is injective. In particular, we get from Lemma 1.2.11 that involutive solutions are always involutive since $A(X,r)$ is the free abelian group on $X$.

We call the obtained skew brace $(G(X,r),\cdot,\circ)$ the *structure skew brace* of $(X,r)$.

**Example 1.2.16.** Let $(X,r)$ be a solution coming from a rack $(X,\triangleright)$. Then since $(X,r)$ coincides with its derived solution, and also the action $\sigma : (G(X,r),\circ)\to\mathbb{S}_X$ is trivial, we find that $g\cdot h = g\circ h$ for all $g,h\in G(X,r)$. We conclude that $(G(X,r),\cdot,\circ)$ is a trivial skew brace.

The second part of the main results of [117, 152] concerns a universal property satisfied by the structure skew brace. Before we can formulate this we need to introduce another construction, this time starting from a skew brace and yielding a solution.

**Proposition 1.2.17** ([83, Theorem 3.1])**.** *Let $A$ be a skew brace and define*

$$r : A^2\to A^2 : (a,b)\mapsto(\lambda_a(b),\overline{\lambda_a(b)}\circ a\circ b), \tag{1.7}$$

*then $(A,r_A)$ is a solution of the YBE.*

*Proof.* We only show that (1.3) holds. Note that this happens precisely if

$$\lambda_a\lambda_b = \lambda_{\lambda_a(b)}\circ\lambda_{\overline{\lambda_a(b)}\circ a\circ b},$$

for all $a,b\in A$, which is satisfied since the right hand side equals

$$\lambda_{\lambda_a(b)\circ\overline{\lambda_a(b)}\circ a\circ b} = \lambda_{a\circ b}.$$ □

**Example 1.2.18.** Let $G$ be a group and let $A$ be the trivial skew brace $\mathrm{Triv}(G)$, then $r_A(g,h) = (h,h^{-1}gh)$. Note that these are of the same form as the ones in Example 1.2.4. If conversely, $A$ is the almost trivial skew brace $\mathrm{opTriv}(G)$, then we find $r_A(g,h) = (ghg^{-1},g)$.

**Example 1.2.19.** Let $(X,r)$ be a solution and let $x,y\in X$. Then, working in the skew brace $G(X,r)$, we find that $\lambda_x(y) = \sigma_x(y)$ and thus $\overline{\lambda_x(y)}\circ x\circ y = \tau_y(x)$ since

$$\lambda_x(y)\circ(\overline{\lambda_x(y)}\circ x\circ y) = x\circ y = \sigma_x(y)\circ\tau_y(x).$$

We deduce that the canonical map $\iota : (X,r)\to(G(X,r),r_{G(X,r)})$ is a homomorphism of solutions.

**Example 1.2.20.** Let $A$ be a skew brace, let $(A, r_A)$ be the solution on $A$ and let $(A, r_{A_{\mathrm{op}}})$ be the solution on its opposite skew brace. Then we find that the first component of $r_{A_{\mathrm{op}}} r_A(a, b)$ is

$$\begin{aligned}\lambda^{\mathrm{op}}_{\lambda_a(b)}(\overline{\lambda_a(b)} \circ a \circ b) &= (\lambda_a(b) \circ \overline{\lambda_a(b)} \circ a \circ b) \cdot \lambda_a(b^{-1}) \\ &= (a \circ b) \cdot a^{-1} \cdot (a \circ b^{-1}) \\ &= a \circ (b \cdot b^{-1}) \\ &= a.\end{aligned}$$

Since applying $r_A$ or $r_{A_{\mathrm{op}}}$ on $(a, b)$ leaves the $\circ$-product of the pair invariant, we conclude that $r_{A_{\mathrm{op}}} r_A = \mathrm{id}_{A^2}$ and thus $r_{A_{\mathrm{op}}} = r_A^{-1}$. In particular, $(A, r_A)$ is involutive if and only if $A$ is a brace.

**Theorem 1.2.21.** *Let $(X, r)$ be a solution, let $A$ be a skew brace and let $f : (X, r) \to (A, r_A)$ be a homomorphism of solutions. Then there exists a unique skew brace homomorphism*

$$\tilde{f} : (G(X, r), \cdot, \circ) \to (A, \cdot, \circ)$$

*such that $f = \tilde{f}\iota$.*

*Remark* 1.2.22. It is easily seen that in fact the construction $(X, r) \mapsto (G(X, r), \cdot, \circ)$ is functorial, and so is the construction $A \mapsto (A, r_A)$. Therefore, Theorem 1.2.21 states precisely that the first functor is left adjoint to the second one. The analogy with Lie algebras should not go unnoticed. The structure skew brace $G(X, r)$ is, in a sense, the best skew brace we can hope to embed $(X, r)$ into, its "universal enveloping skew brace". Just like in the case of Lie algebras, this injectivity sometimes fails, but this doesn't imply that this enveloping algebraic structure loses its utility, as for example the representations of a Lie algebra correspond to those of its universal enveloping algebra.

### 1.2.3 The permutation skew brace

The structure skew brace of a solution $(X, r)$ exhibits a somewhat rigid structure, especially in the case where $(X, r)$ is involutive and thus the additive group is free abelian. From a practical viewpoint, however, one can argue that these are deemed too big since they are infinite even when $|X| < \infty$. We will now introduce a quotient of the skew brace $\mathcal{G}(X, r)$, which is often more practical to work with.

Let us consider, using the notation from Section 1.2.2, the action

$$\sigma : (G(X, r), \circ) \to \mathbb{S}_X : x \mapsto \sigma_x,$$

and let $K$ denote its kernel. Since $\sigma$ induces an action of $(G(X, r), \circ)$ on $(G(X, r), \cdot)$ which, under the isomorphism described in Theorem 1.2.14, is precisely the $\lambda$-action of the skew brace $(G(X, r), \cdot, \circ)$, we find that $K \subseteq \ker \lambda$. We can apply a similar procedure to the derived solution $(X, r')$. By (1.4) we find a right action of $(G(X, r'), \circ) \cong (A(X, r), \cdot)$ on $X$, where a generator $x \in X$ acts by the permutation $y \mapsto x \triangleright_r y$. Let us denote the kernel of this action by $L$, which we easily see to be contained in the center of the group $(G(X, r), \cdot)$. We claim that $K \cap L$ is an ideal of $(G(X, r), \cdot, \circ)$. For this, we first note that $L$ is a strong left ideal. Indeed, the normality in the additive group is clear. Let $l \in L$ and write it as a word $l = x_1^{\epsilon_1} \cdot x_2^{\epsilon_2} \cdot \ldots \cdot x_r^{\epsilon_r}$ in the generators $X$, where $\epsilon_i \in \{1, -1\}$. We then find for any $y \in X$

$$y = x_r \triangleright_r^{\epsilon_r} (x_{r-1} \triangleright_r^{\epsilon_{r-1}} (\ldots \triangleright_r^{\epsilon_2} (x_1 \triangleright_r^{\epsilon_1} (y)))),$$

where by abuse of notation $x \triangleright_r^{\epsilon} y$ equals $x \triangleright_r y$ when $\epsilon = 1$ and $y'$, with $y'$ the unique element such that $x \triangleright_r y' = y$, when $\epsilon = -1$. Let $z \in X$, then we know that $\sigma_z$ is an automorphism of $(X, \triangleright_r)$, hence

$$\sigma_z(y) = \sigma_z(x_r) \triangleright_r^{\epsilon_r} (\sigma_z(x_{r-1}) \triangleright_r^{\epsilon_{r-1}} (\ldots \triangleright_r^{\epsilon_2} (\sigma_z(x_1) \triangleright_r^{\epsilon_1} (\sigma_z(y))))),$$

but the latter equality expresses precisely that $\lambda_z(l) = \sigma_z(x_1)^{\epsilon_1} \cdot \sigma_z(x_2)^{\epsilon_2} \cdot \ldots \cdot \sigma_z(x_r)^{\epsilon_r}$ acts trivially on $y$, hence $\lambda_z(l) \in L$. Since $X$ is a generating set of $(G(X,r), \circ)$, we find that $\lambda_g(L) \subseteq L$ for any $g \in G(X,r)$ and thus $L$ is a strong left ideal of $G(X,r)$.

Since $K \subseteq \ker \lambda$ and $L \subseteq Z(G(X,r), \cdot)$, we find that $K \cap L \subseteq \mathrm{Soc}(G(X,r))$. Now recall from the comment in Example 1.1.5 that the $\lambda$-action on any element in the socle coincides with the action by multiplicative conjugation. For any $g \in G(X,r)$ we find

$$\lambda_g(K \cap L) \subseteq \lambda_g(K) \cap \lambda_g(L) = (g \circ K \circ \overline{g}) \cap L = K \cap L.$$

This proves simultaneously that $K \cap L$ is a left ideal and that it is normal in the multiplicative group. Moreover, normality in the additive group is trivial since $K \cap L$ is contained in the additive center. The quotient skew brace

$$\mathcal{G}(X,r) := G(X,r)/(K \cap L),$$

is the *permutation skew brace*. The name is justified by the fact that $K \cap L$ is precisely the kernel of the group homomorphism $(G(X,r), \circ) \to \mathbb{S}_X \times \mathbb{S}_X$ that maps a generator $x$ to $(\sigma_x, \hat{\sigma}_x)$. We can therefore identify $\mathcal{G}(X,r)$ with its image in $\mathbb{S}_X \times \mathbb{S}_X$. If $(X,r)$ is involutive, then $\sigma_x = \hat{\sigma}_x$ so $K \cap L$ is the kernel of the homomorphism $\sigma : (G(X,r), \circ) \to \mathbb{S}_X$ sending $x$ to $\sigma_x$. When working with involutive solutions, we will always identify $\mathcal{G}(X,r)$ with its image in $\mathbb{S}_X$. In particular, by the *permutation group* of $(X,r)$ we mean the subgroup of $\mathbb{S}_X$ generated by all $\sigma_x$, $x \in X$. We remark that if the solution $(X,r)$ is finite, then also its permutation skew brace $\mathcal{G}(X,r)$ is finite.

Conversely, any (finite) skew brace is isomorphic to the permutation skew brace of some (finite) solution $(X,r)$. This subject is treated in full generality in [11, 12], we only give a specific statement which will suffice for our purposes.

**Definition 1.2.23.** Let $(X,r)$ be a solution. A set $Y \subseteq X$ is an *orbit* of $(X,r)$ if it is an orbit of the subgroup $\langle \sigma_x, \tau_x \mid x \in X \rangle \subseteq \mathbb{S}_X$. A solution $(X,r)$ is *decomposable* if $(X,r)$ has more than one orbit. It is *indecomposable* if it has a unique orbit. If $(X,r)$ is involutive, then by (1.6) it is indecomposable if and only if its permutation group $\mathcal{G}(X,r)$ acts transitively on $X$.

**Proposition 1.2.24** ([12])**.** *Let $(A, +, \circ)$ be a brace, let $x \in A$ and let $K$ be a subgroup of $(A, \circ)$ such that*

1. *$\{\lambda_a(x) \mid a \in A\}$ generates $(A, +)$,*
2. *$K$ fixes $x$ under the $\lambda$-action,*
3. *the intersection $\bigcap_{a \in A} a \circ K \circ \overline{a}$ equals $\{0\}$.*

*Then we obtain an indecomposable solution on the left cosets $X = (A, \circ)/K$ given by*

$$r : X^2 \to X^2 : (a \circ K, b \circ K) \mapsto (\lambda_a(x) \circ b \circ K, \overline{\lambda_{\lambda_a(x) \circ b}(x)} \circ a \circ K).$$

*Conversely, any indecomposable involutive solution $(X,r)$ is isomorphic to the solution obtained through the above process starting from the brace $\mathcal{G}(X,r)$ with the element $\sigma_x \in \mathcal{G}(X,r)$ and the subgroup $\mathrm{Stab}_{\mathcal{G}(X,r)}(x)$, for any choice of $x \in X$. Under this isomorphism, a coset $\sigma \circ \mathrm{Stab}_{(\mathcal{G}(X,r), \circ)}(x)$ is mapped to $\sigma(x)$.*

**Proposition 1.2.25** ([12])**.** *Let $A$ be a brace, let $(x, K)$ and $(y, L)$ be pairs satisfying the conditions of Proposition 1.2.24 and let $(X, r)$ and $(Y, s)$ be the associated solutions. If $z \in A$ and $\psi$ is a skew brace automorphism of $A$ such that $\psi(x) = \lambda_z(y)$ and $\psi(K) = z \circ L \circ \overline{z}$, then*

$$\Phi : (X, r) \to (Y, s) : a \circ K \mapsto \psi(a) \circ z \circ L,$$

*is an isomorphism of solutions. Moreover, every isomorphism between $(X, r)$ and $(Y, s)$ is of this form.*

The following example shows that the construction of the permutation skew brace is in general not functorial.

**Example 1.2.26.** Let $(X, r)$ be the trivial solution on $X = \{1\}$. Also, let $(Y, s)$ be the permutation solution $s(x, y) = (\sigma(y), \sigma(x))$ on the set $Y = \{1, 2, 3\}$ with $\sigma = (2\ 3)$. The map

$$f : X \to Y : 1 \mapsto 1,$$

is a homomorphism of solutions. We find that $|\mathcal{G}(Y, s)| = 2$, hence $\mathcal{G}(Y, s) \cong \mathrm{Triv}(\mathbb{Z}/2)$ as there exist no non-trivial skew braces of size 2. Also note that the canonical image $Y \to \mathcal{G}(Y, s)$ sends every element of $Y$ to $\sigma$. As $\mathcal{G}(X, r) = \{\mathrm{id}_X\}$, there is no homomorphism $\tilde{f} : \mathcal{G}(X, r) \to \mathcal{G}(Y, s)$ such that

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \downarrow & & \downarrow \\ \mathcal{G}(X, r) & \xrightarrow[\tilde{f}]{} & \mathcal{G}(Y, s) \end{array}$$

commutes, where the vertical maps are the canonical ones.

Functoriality of the permutation skew brace does hold in certain cases; any surjective homomorphism of solutions $(X, r) \to (Y, s)$ yields a surjective skew brace homomorphism $\mathcal{G}(X, r) \to \mathcal{G}(Y, s)$ in a canonical way. From this, the following result of Cedó and Okniński follows.

**Proposition 1.2.27** ([54, Lemma 3.3])**.** *Let $f : (X, r) \to (Y, s)$ be a surjective homomorphism of finite solutions. If $(X, r)$ is indecomposable, then also $(Y, s)$ is indecomposable and the fibres $f^{-1}(y)$ all have the same cardinality. In particular, $|Y|$ divides $|X|$.*

**Definition 1.2.28.** Let $p : (X, r) \to (Y, s)$ be a surjective homomorphism of indecomposable solutions. If the induced skew brace homomorphism $\mathcal{G}(X, r) \to \mathcal{G}(Y, s)$ is an isomorphism, we say that $p$ is a *covering*. A covering $\tilde{p} : (\tilde{X}, \tilde{r}) \to (X, r)$ is *universal* if it factors through any other covering $(Y, s) \to (X, r)$. A solution $(X, r)$ is *uniconnected* if any covering $(Y, s) \to (X, r)$ is invertible.

Let $A$ be a brace and let $x \in A$ such that $\{\lambda_a(x) \mid a \in A\}$ generates $(A, +)$. If we let $K = \{0\}$, then the second and third conditions of Proposition 1.2.24 are trivially satisfied, and we obtain a solution $(X, r)$ with $\mathcal{G}(X, r) \cong A$ and such that its permutation group acts regularly on $X = A$. Moreover, if $K$ is any subgroup of $(A, \circ)$ satisfying the second and third condition of Proposition 1.2.24 and $(Y, s)$ is the associated solution, then we find a canonical surjective homomorphism of solutions $\tilde{p} : (X, r) \to (Y, s)$ mapping an element $a \in A$ to the coset $a \circ K$. Moreover, the induced homomorphism $\mathcal{G}(X, r) \to \mathcal{G}(Y, s)$ is an isomorphism since both are isomorphic to $A$, so $\tilde{p}$ is a covering.

**Proposition 1.2.29** ([135, Theorem 3.3])**.** *With the notation as above, $\tilde{p} : (X, r) \to (Y, s)$ is a universal covering and $(X, r)$ is uniconnected.*

### 1.2.4 Cycle bases

**Definition 1.2.30.** Let $(X, r)$ be a solution. Then $Y \subseteq X$ is a *subsolution* of $(X, r)$ if $r(Y^2) \subseteq Y^2$ and $(Y, r|_{Y^2})$, where $r|_{Y^2}$ denotes the restriction $r|_{Y^2} : Y^2 \to Y^2$, is a solution.

*Remark* 1.2.31. It is clear that if $(X, r)$ is a solution, then for any $Y \subseteq X$ such that $r(Y^2) \subseteq Y^2$, the pair $(Y, r|_{Y^2})$ is a set-theoretical solution of the YBE, but it is not necessarily bijective and non-degenerate. Therefore, the requirement that $(Y, r|_{Y^2})$ is a non-degenerate bijective solution of the YBE (hence in our terminology, a solution) is equivalent to requiring that $r(Y^2) = Y^2$ and $\sigma_x(Y) = \tau_x(Y) = Y$ for all $x \in Y$. In particular, if $X$ is finite, then these requirements are trivially satisfied and a subsolution of $(X, r)$ is really the same as a subset $Y$ such that $\sigma_x(y), \tau_x(y) \in Y$ for all $x, y \in Y$.

Let $A$ be a skew brace. Although the solution $(A, r_A)$ plays an interesting role in Theorem 1.2.21, its properties are often undesirable. Note for example that $\{0\}$ is always an orbit of $(A, r_A)$ hence $(A, r_A)$ is decomposable if $|A| > 1$. Therefore, it is often interesting to look at subsolutions of $(A, r_A)$ that still retain some information on $A$ itself. The correct such notion turns out to be that of a cycle base, originally defined by Rump for braces in [132]. We extend here Rump's definition to skew braces.

**Lemma 1.2.32.** *Let $A$ be a skew brace. Then*

$$\theta : (A, \cdot) \rtimes_\lambda (A, \circ) \to \mathrm{Aut}(A, \cdot) : (a, b) \mapsto \theta_{(a,b)},$$

*with*

$$\theta_{(a,b)}(c) = a \cdot \lambda_b(c) \cdot a^{-1},$$

*is a group homomorphism.*

*Proof.* Let $a, b, c, d, e \in A$, then clearly $\theta_{(a,b)} \in \mathrm{Aut}(A, \cdot)$. Moreover,

$$\theta_{(a,b)}\theta_{(c,d)}(e) = a \cdot \lambda_b(c \cdot \lambda_d(e) \cdot c^{-1}) \cdot a^{-1} = a \cdot \lambda_b(c) \cdot \lambda_b\lambda_d(e) \cdot \lambda_b(c)^{-1} \cdot a^{-1} = \theta_{(a \cdot \lambda_b(c), b \circ d)}(e),$$

which concludes the proof. □

We call this action of $(A, \cdot) \rtimes_\lambda (A, \circ)$ the *$\theta$-action* of $A$. We remark that the $\lambda$-action of $A_{\mathrm{op}}$ is also hidden in the $\theta$-action since $\theta_{(a,a)} = a \cdot a^{-1} \cdot (a \circ b) \cdot a^{-1} = \lambda_a^{\mathrm{op}}(b)$. More precisely, for the same reason that $(A, \circ)$ embeds as a regular subgroup of $\mathrm{Hol}(A, \cdot)$, we can see that the diagonal

$$\Delta = \{(a, a) \mid a \in A\} \subseteq (A, \cdot) \rtimes_\lambda (A, \circ),$$

is an isomorphic copy of $(A, \circ)$ such that moreover the subgroups $\{0\} \rtimes (A, \circ)$ and $\Delta$ yield an exact factorization of $(A, \cdot) \rtimes_\lambda (A, \circ)$. In fact, we have recovered a matched pair of groups, see [151, Remark 3.15]. This also implies that orbits of the $\theta$-action of $A$ coincide with orbits of the $\theta$-action of $A_{\mathrm{op}}$. Also, if $A$ is a brace, then we find that invariant subsets under the $\theta$-action are the same as invariant subsets under the $\lambda$-action.

**Definition 1.2.33.** A subset $X$ of a skew brace $A$ is a *cycle base* if it is invariant under the $\theta$-action of $A$ and moreover $X$ generates the group $(A, \cdot)$. A cycle base is *transitive* if the $\theta$-action is transitive on $X$.

Note that the first condition of Proposition 1.2.24 states precisely that $\{\lambda_a(x) \mid a \in A\}$ is a transitive cycle base of $A$. Also, in the more general construction [11, Theorem 3.19], the starting point of constructing a solution $(X, r)$ such that $\mathcal{G}(X, r) \cong A$ for a given skew brace $A$ starts from a cycle base of $A$.

**Lemma 1.2.34.** *Let $X$ be a cycle base of a skew brace $A$. Then $X$ is a subsolution of $(A, r_A)$ and orbits of the solution $X$ coincide with the orbits of the $\theta$-action restricted to the set $X$. In particular, $X$ is indecomposable if and only if $X$ is a transitive cycle base of $A$.*

*Proof.* Recall that the solution $(A, r_A)$ is given by $r_A(a, b) = (\lambda_a(b), \tau_b(a))$ with $\tau_b(a) = \overline{\lambda_a(b)} \circ a \circ b$. For any $a, b \in A$ we find

$$\lambda^{\mathrm{op}}_{\overline{\lambda_a(b)}}(a) = \overline{\lambda_a(b)} \circ (a \cdot \lambda_a(b)) = \overline{\lambda_a(b)} \circ a \circ b = \tau_b(a). \tag{1.8}$$

Also,

$$\begin{aligned}
\tau_c\tau_b(a) &= \mu_c(\overline{\lambda_a(b)} \circ a \circ b) \\
&= \overline{\lambda_{\overline{\lambda_a(b)} \circ a \circ b}(c)} \circ \overline{\lambda_a(b)} \circ a \circ b \circ c \\
&= \overline{\lambda_a(b) \circ \lambda^{-1}_{\lambda_a(b)}\lambda_a\lambda_b(c)} \circ a \circ b \circ c \\
&= \overline{\lambda_a(b + \lambda_b(c))} \circ a \circ b \circ c \\
&= \overline{\lambda_a(b \circ c)} \circ a \circ b \circ c \\
&= \tau_{b\circ c}(a).
\end{aligned}$$

which implies in particular that $\tau_b^{-1} = \tau_{\overline{b}}$. Let $X$ be a cycle base of $A$, then it follows from (1.8) and the fact that $\theta_{(0,a)} = \lambda_a$ and $\theta_{(a,a)} = \lambda^{\mathrm{op}}_a$ that $r_A(X^2) \subseteq X^2$. Since $X$ is also a cycle base of $A_{\mathrm{op}}$, we find that $r_A^{-1}(X^2) \subseteq X^2$, see Example 1.2.20. Similarly, we find that $\lambda_x(X), \lambda_x^{-1}(X), \tau_x(X)$ and $\tau_x^{-1}(X)$ are all contained in $X$ for all $x \in X$. We conclude that $X$ is a subsolution of $(A, r_A)$.

By the discussion preceding Definition 1.2.33, we find that the subgroup

$$\theta(A \times A) = \{\theta_{(a,b)} \mid a, b \in A\} \subseteq \mathbb{S}_X,$$

is generated by the set $\{\lambda_a, \lambda^{\mathrm{op}}_a \mid a \in A\}$. Although the definition of a cycle base $X$ of $A$ only requires that $X$ generates $(A, \cdot)$, its invariance under the $\lambda$-action also implies that it generates $(A, \circ)$. Therefore $\theta(A \times A)$ is also generated by the set $\{\lambda_x, \lambda^{\mathrm{op}}_x \mid x \in X\}$. Together with (1.8) this implies that $\theta(A \times A)$ is generated by the set $\{\lambda_a, \tau_a \mid a \in A\}$. The second part of the statement now follows. □

*Remark* 1.2.35. If we say that a solution $(X, r)$ is a cycle base of $A$, we mean that the set $X$ is a cycle base and moreover the restriction of $(A, r_A)$ to $X$ is precisely $(X, r)$.

Let $(X, r)$ be a solution. Since we know that $\iota : (X, r) \to (G(X, r), r_{G(X,r)})$ is a homomorphism of solutions, we know that the image $\iota(X)$ is a subsolution. However, since the $\lambda$-map and additive conjugation in $G(X, r)$ come from the maps $\sigma_x$ and the operation $\triangleright_r$ respectively, we find that $\iota(X)$ is invariant under the $\theta$-map and thus a cycle base of $G(X, r)$. Trivially, surjective skew brace homomorphisms $f : A \to B$ map cycle bases of $A$ to cycle bases of $B$. Therefore, we find that also the canonical image of $X$ in $\mathcal{G}(X, r)$ is a cycle base. For an involutive solution $(X, r)$, this cycle base corresponds precisely to the set $\{\sigma_x \mid x \in X\}$. This cycle base is called the *retract* of $(X, r)$ and is denoted by $\mathrm{Ret}(X, r)$. Concretely, this can be realized as $(X/\!\sim, s)$. Here, $X/\!\sim$ denotes the equivalence classes of $X$ with respect to the relation

$$x \sim y \Leftrightarrow \sigma_x = \sigma_y \text{ and } \tau_x = \tau_y, \tag{1.9}$$

and $s([x], [y]) = ([\sigma_x(y)], [\tau_y(x)])$, where $[x]$ denotes the equivalence class of $x$. It is non-trivial that $s$ is indeed well-defined, but this follows precisely by the discussion.

**Example 1.2.36.** Let $(X, r)$ be a solution such that $|\operatorname{Ret}(X, r)| = 1$. This happens precisely if $x \sim y$ for all $x, y \in Y$, meaning $\sigma_x = \sigma_y$ and $\tau_x = \tau_y$. We conclude that the imposed condition is equivalent to $(X, r)$ being a permutation solution.

We can also iterate this retraction procedure. Set $\operatorname{Ret}^0(X, r) = (X, r)$ and

$$\operatorname{Ret}^{i+1}(X, r) = \operatorname{Ret}(\operatorname{Ret}^i(X, r)).$$

In this way, we obtain a chain of surjective homomorphisms of solutions

$$(X, r) \to \operatorname{Ret}(X, r) \to \operatorname{Ret}^2(X, r) \to \operatorname{Ret}^3(X, r) \to \dots$$

If $X$ is finite, this chain becomes stationary at some point. We distinguish two cases. Either we reach the trivial one-element solution, meaning that there exists some $n \geq 0$ such that $|\operatorname{Ret}^n(X, r)| = 1$. In this case, $(X, r)$ is a *multipermutation solution*, readily motivated by Example 1.2.36, and the smallest such $n$ is the *multipermutation level* of $(X, r)$, denoted $\operatorname{mpl}(X, r)$. The other possibility is that this chain becomes stationary at a solution $(Y, s)$ of size $> 1$ with the property $\operatorname{Ret}(Y, s) = (Y, s)$, we call such a solution *irretractable*. Note that these solutions embed into their permutation skew brace.

**Example 1.2.37.** Let $A$ be a skew brace, then the equivalence relation $\sim$ states that $a \sim b$ if and only if $\lambda_a = \lambda_b$ and $\tau_a = \tau_b$, where $\tau_a(c) = \overline{\lambda_c(a)} \circ c \circ a$. By the observations made in the proof of Lemma 1.2.34, we find that this happens precisely if $\lambda_a = \lambda_b$ and $\lambda_a^{\mathrm{op}} = \lambda_b^{\mathrm{op}}$, which in turn is equivalent to $a \circ \overline{b} \in \operatorname{Soc}(A)$ since $\operatorname{Soc}(A) = \ker \lambda \cap \ker \lambda^{\mathrm{op}}$. In other words, the retract of the solution associated to $A$ is the solution associated to $A/\operatorname{Soc}(A)$. We call $A/\operatorname{Soc}(A)$ the *retract* of $A$, and since the retract of $A/\operatorname{Soc}(A)$ can be identified with $A/\operatorname{Soc}_2(A)$, this justifies the notion of multipermutation skew braces as introduced in Section 1.1.3.

We conclude by discussing cabling for involutive solutions [66, 114]. Let $(X, r)$ be an involutive solution. We know that the canonical map $\iota : X \to G(X, r)$ is injective and $\iota(X)$ is a cycle base of $(G(X, r), +, \circ)$. Let $k \in \mathbb{Z}$ and consider the set

$$Y = k\iota(X) = \{k\iota(x) \mid x \in X\},$$

where $k\iota(x)$ denotes the sum of $k$ copies of $\iota(x)$ in $(G(X, r), +)$. When $k \notin \{1, -1\}$ this no longer is a cycle base of $A$, since $Y$ does not generate $(G(X, r), +)$, but it is nonetheless invariant under the $\theta$-action. From Lemma 1.2.34 we find that $Y$ is a subsolution of $(A, r_A)$, indeed, note that the proof of this fact uses only the invariance under the $\theta$-action. Since $(G(X, r), +)$ is the free abelian group on $X$, we find that the map

$$X \to Y : x \mapsto k\iota(x)$$

is bijective, so we can transfer the solution on $Y$ to the set $X$. We call this the *$k$-cabled solution* and denote it by $(X, r^{(k)})$. Alternatively, note that, if we introduce the notation $r^{(k)}(x, y) = (\sigma_x^{(k)}(y), \tau_y^{(k)}(x))$, then $\sigma_x^{(k)}$ is precisely $k\sigma_x$, the $k$-th power of $\sigma_x$ in $(\mathcal{G}(X, r), +)$. The functoriality of the construction of the structure brace also implies the functoriality of cabling.

It is a direct consequence of its definition that the permutation group of $(X, r^{(k)})$ is contained in that of $(X, r)$. We claim that it is even a subbrace. Let us denote the $\lambda$-map of $\mathcal{G}(X, r^{(k)})$ by $\lambda^{(k)}$ and the $\lambda$-map of $\mathcal{G}(X, r)$ simply by $\lambda$, then by definition we have

$$\lambda^{(k)}_{\sigma_x}(\sigma_y) = \sigma_{(k\sigma_x)(y)} = \lambda_{k\sigma_x}(\sigma_y).$$

We find that the addition $+_k$ in $\mathcal{G}(X, r^{(k)})$ is given by

$$\begin{aligned}\sigma_x^{(k)} +_k \sigma_y^{(k)} &= \sigma_x^{(k)} \circ \left(\lambda_{\sigma_x}^{(k)}\right)^{-1} \sigma_y^{(k)} \\ &= (k\sigma_x) \circ \lambda_{k\sigma_x}^{-1}(k\sigma_y) \\ &= (k\sigma_x) + (k\sigma_y) = \sigma_x^{(k)} + \sigma_y^{(k)}.\end{aligned}$$

### 1.2.5 Cycle sets

Let $(X, r)$ be an involutive solution, then as a direct consequence of (1.6) we find that the maps $\tau_x$ are completely determined if we know all of the maps $\sigma_x$. So in a certain sense, the second component of the map $r$ is redundant; everything should be expressible in terms of the maps $\sigma_x$. Indeed, one can axiomatize these properties in terms of structures with only one binary operation, called cycle sets, as proved by Rump [131].

**Definition 1.2.38.** A *cycle set* $(X, \cdot)$ is a non-empty set with a binary operation such that

1. $(x \cdot y) \cdot (x \cdot z) = (y \cdot x) \cdot (y \cdot z)$ for all $x, y, z \in X$,
2. the map $X \to X : y \mapsto x \cdot y$ is a bijection for all $x \in X$,
3. the *square map* $\mathrm{Sq} : X \to X : x \mapsto x \cdot x$ is bijective.

A map $f : (X, \cdot) \to (Y, \cdot)$ between cycle sets is a *homomorphism* if $f(x \cdot y) = f(x) \cdot f(y)$ for all $x, y \in X$.

*Remark* 1.2.39. In fact, Definition 1.2.38 defines a *non-degenerate* cycle set, but we will omit the predicate non-degenerate, as we also do for solutions. Also, regarding the possible clash of notation with the additive operation of a skew brace; we will only make use of cycle sets in Chapter 5, where all the skew braces that appear are braces, whose additive group operation we will denote by $+$. This means that throughout Chapter 5 one can safely assume that $\cdot$ denotes the operation of a cycle set.

**Proposition 1.2.40.** *Let $X$ be a non-empty set. Then the following data are equivalent:*

1. *A map $r : X^2 \to X^2$ such that $(X, r)$ is an involutive solution.*
2. *A binary operation on $X$ such that $(X, \cdot)$ is a cycle set.*

*Moreover, this correspondence is functorial.*

*Proof.* We only give the constructions. Let $(X, r)$ be an involutive solution, then $x \cdot y = \sigma_x^{-1}(y)$ yields a cycle set structure $(X, \cdot)$. Conversely, assume that we are given a cycle set $(X, \cdot)$. Define $\sigma_x$ as the inverse of the map $y \mapsto x \cdot y$ and

$$r : X^2 \to X^2 : (x, y) \mapsto (\sigma_x(y), \sigma_x(y) \cdot x).$$

Then $(X, r)$ is an involutive solution. □

Let $(X, \cdot)$ be a cycle set. As in the proof of Proposition 1.2.40, we define $\sigma_x(y)$ by $x \cdot \sigma_x(y) = y$. This means that $\sigma_x$ is the inverse of the map $y \mapsto x \cdot y$. We should remark that this conflicts with the more usual notation for cycle sets where $\sigma_x(y) = x \cdot y$, but our definition is more consistent with the established notation for solutions.

All notions that we have introduced for involutive solutions, like the structure brace, permutation brace, retract, multipermutation level, indecomposability, cabling, etc. also make sense for cycle sets through the correspondence given in Proposition 1.2.40. We will freely use this in Chapter 5.

## 1.3 Post-Lie algebras

Throughout the entire section, unless specified otherwise, $R$ denotes a commutative ring.

**Definition 1.3.1.** A *Lie algebra* over $R$ consists of an $R$-module $\mathfrak{g}$ together with a bilinear map,

$$\mathfrak{g}^2 \to \mathfrak{g} : (x, y) \mapsto [x, y],$$

called the (Lie) bracket of $\mathfrak{g}$, that satisfies

$$\begin{aligned} [x, x] &= 0, \\ [x, [y, z]] + [z, [x, y]] + [y, [z, x]] &= 0, \end{aligned}$$

for all $x, y, z \in \mathfrak{g}$. If $R = \mathbb{Z}$, then $\mathfrak{a}$ is a *Lie ring*. A *homomorphism* of Lie algebras $f : \mathfrak{g} \to \mathfrak{h}$ is a linear map preserving the Lie bracket and an *isomorphism* is a bijective homomorphism.

*Remark* 1.3.2. Most of the time, we will simply talk about Lie algebras, thereby meaning Lie algebras over $R$. If the ring $R$ is not specified, then it can be any commutative ring. Similarly, whenever talking about linear maps and modules, this always means $R$-linear maps and $R$-modules.

**Example 1.3.3.** Let $\mathfrak{a}$ be a Lie algebra. Recall that a linear map $\delta : \mathfrak{a} \to \mathfrak{a}$ is a *derivation* if

$$\delta([x, y]) = [\delta(x), y] + [x, \delta(y)],$$

holds for all $x, y \in \mathfrak{a}$. The set of derivations of $\mathfrak{a}$ is denoted $\mathfrak{der}(\mathfrak{g})$ and forms itself a Lie algebra for the commutator Lie bracket $[\delta, \chi] = \delta\chi - \chi\delta$.

**Example 1.3.4.** Let $A$ be an algebra, then the commutator Lie bracket $[a, b] = ab - ba$ makes $A$ into a Lie algebra. If $\mathfrak{a}$ is a Lie algebra and we say that a map $f : \mathfrak{a} \to A$ is a Lie algebra homomorphism, we will always consider $A$ as a Lie algebra with the commutator Lie bracket. Explicitly, this means that we demand that $f([a, b]) = f(a)f(b) - f(b)f(a)$ for all $a, b \in A$.

A *post-Lie algebra* over $R$ is a Lie algebra $\mathfrak{a}$, whose Lie bracket we will always assume to be given by $[-, -]$, together with a bilinear map

$$\triangleright : \mathfrak{a} \times \mathfrak{a} \to \mathfrak{a} : (x, y) \mapsto x \triangleright y$$

satisfying

$$x \triangleright [y, z] = [x \triangleright y, z] + [y, x \triangleright z], \tag{P1}$$

$$[x, y] \triangleright z = (x, y, z)_{\triangleright} - (y, x, z)_{\triangleright}, \tag{P2}$$

for all $x, y, z \in \mathfrak{a}$, with $(x, y, z)_{\triangleright}$ defined as the associator $x \triangleright (y \triangleright z) - (x \triangleright y) \triangleright z$. If the bracket on $\mathfrak{a}$ is trivial, then $(\mathfrak{a}, \triangleright)$ is a *pre-Lie algebra*. A post-Lie algebra or pre-Lie algebra over $\mathbb{Z}$ is called a *post-Lie ring* or *pre-Lie ring* respectively. A map $f : (\mathfrak{a}, \triangleright) \to (\mathfrak{b}, \triangleright)$ between post-Lie algebras is a *homomorphism* if it is a homomorphism of the underlying Lie algebras and it also respects the operation $\triangleright$.

Pre-Lie algebras, also called *left-symmetric algebras*, arose as early as 1881 in the work of Cayley [47], only to resurface again 80 years later in the works of Vinberg [167] and Koszul [108]. One of the motivations to study pre-Lie algebras comes from regular actions of Lie groups by affine transformations on $\mathbb{R}^n$, see for example [98]. By the discussion in Section 1.1.5, we know that there is a close relation between such actions

and skew braces. The motivation to study such actions can be traced back to the study of crystallographic groups, see [8, 76, 121]. More recently, the notion of a post-Lie algebra was introduced in the works of Vallette [163], see also [68].

The following lemma follows from [30] for $R$ a field of characteristic 0, but the general proof proceeds by the exact same steps.

**Lemma 1.3.5.** *Let $\mathfrak{a}$ be a Lie algebra and $\triangleright$ an operation satisfying* (P1)*. Then $(\mathfrak{a}, \triangleright)$ is a post-Lie algebra if and only if*

$$\{a, b\} := [a, b] + a \triangleright b - b \triangleright a, \tag{1.10}$$

*defines a Lie bracket on the module $\mathfrak{a}$. We call this the* sub-adjacent Lie algebra *and denote it by $\mathfrak{a}^\circ$.*

Let $(\mathfrak{a}, \triangleright)$ be a post-Lie algebra and $x \in \mathfrak{a}$. From now onward we denote left $\triangleright$-multiplication by $x$ as

$$\mathcal{L}_x : \mathfrak{a} \to \mathfrak{a} : y \mapsto x \triangleright y,$$

It is a direct consequence of (P1) that $\mathcal{L}_x$ is a derivation of the Lie algebra $\mathfrak{a}$. Moreover, from (P2) we find

$$\begin{aligned} \mathcal{L}_{\{x,y\}}(z) &= [x, y] \triangleright z + (x \triangleright y) \triangleright z - (y \triangleright x) \triangleright z \\ &= x \triangleright (y \triangleright z) - y \triangleright (x \triangleright z) \\ &= [\mathcal{L}_x, \mathcal{L}_y](z), \end{aligned}$$

meaning that

$$\mathcal{L} : \mathfrak{a}^\circ \to \mathfrak{der}(\mathfrak{a}) : x \mapsto \mathcal{L}_x,$$

is a Lie algebra homomorphism.

**Example 1.3.6.** Let $A$ be a (possibly non-unital) algebra and consider it as a Lie algebra with the trivial commutator bracket. Then $(A, \triangleright)$ with $x \triangleright y = xy$ is a pre-Lie algebra since the associator $(x, y, z)_\triangleright$ is 0 for all $x, y, z \in A$.

**Example 1.3.7.** Let $\mathfrak{a}$ be a Lie algebra and let $x \triangleright y = 0$ for all $x, y \in \mathfrak{a}$. Then we obtain the *trivial* post-Lie algebra on $\mathfrak{a}$.

**Example 1.3.8.** For $\mathfrak{a}$ a Lie algebra with Lie bracket $[-, -]$, we can consider its *opposite* Lie algebra $\mathfrak{a}_{\mathrm{op}}$, which has the same underlying module but its Lie bracket is given by

$$[x, y]_{\mathrm{op}} = [y, x] = -[x, y].$$

Then $(\mathfrak{a}_{\mathrm{op}}, \triangleright)$ with $x \triangleright y = [x, y]$ is the *almost trivial* post-Lie algebra on $\mathfrak{a}$. Indeed, both (P1) and (P2) reduce to the Jacobi identity.

**Definition 1.3.9.** Let $(\mathfrak{a}, \triangleright)$ be a post-Lie algebra and $L \subseteq \mathfrak{a}$. Then $L$ is

1. a *post-Lie subalgebra* if $L$ is a Lie subalgebra of $\mathfrak{a}$ and also $L \triangleright L \subseteq L$.
2. a *left ideal* if $L$ is a Lie subalgebra of $\mathfrak{a}$ and also $\mathfrak{a} \triangleright L \subseteq L$.
3. a *strong left ideal* if $L$ is an ideal of the Lie algebra $\mathfrak{a}$ and also $\mathfrak{a} \triangleright L \subseteq L$.
4. an *ideal* if it is an ideal of the Lie algebras $\mathfrak{a}$ and $\mathfrak{a}^\circ$, and also $\mathfrak{a} \triangleright L \subseteq L$.

*Remark* 1.3.10. Equivalently, $L$ is an ideal of a post-Lie algebra $(\mathfrak{a}, \triangleright)$ if and only if it is a strong left ideal of $(\mathfrak{a}, \triangleright)$ such that also $L \triangleright \mathfrak{a} \subseteq L$. This is a direct consequence of (1.10).

If $L$ is an ideal of a post-Lie algebra $(\mathfrak{a}, \triangleright)$, then both

$$[x + L, y + L] := [x, y] + L, \quad (x + L) \triangleright (y + L) := (x \triangleright y) + L$$

are well-defined operations on the quotient module $\mathfrak{a}/L$. We obtain the *quotient* post-Lie algebra $(\mathfrak{a}/L, \triangleright)$.

Let us consider some examples. We remark that the names and notations here are chosen to correspond to their skew brace theoretic counterparts and are not the common ones that appear in literature on post-Lie algebras.

**Example 1.3.11.** Let $(\mathfrak{a}, \triangleright)$ be a post-Lie algebra. The *fix* of $(\mathfrak{a}, \triangleright)$ is defined as

$$\mathrm{Fix}(\mathfrak{a}, \triangleright) = \{x \in \mathfrak{a} \mid y \triangleright x = 0 \text{ for all } y \in \mathfrak{a}\},$$

and is a left ideal of $(\mathfrak{a}, \triangleright)$.

**Example 1.3.12.** Let $(\mathfrak{a}, \triangleright)$ be a post-Lie algebra. The *socle* of $(\mathfrak{a}, \triangleright)$ is defined as

$$\mathrm{Soc}(\mathfrak{a}, \triangleright) = \{x \in \mathfrak{a} \mid x \triangleright y = [x, y] = 0 \text{ for all } y \in \mathfrak{a}\},$$

and is an ideal of $(\mathfrak{a}, \triangleright)$. Indeed, it is an ideal of $\mathfrak{a}$ since it is contained in its center. Also, for any $x \in \mathfrak{a}$, $y \in \mathrm{Soc}(\mathfrak{a}, \triangleright)$ we find

$$x \triangleright y = \{x, y\} - [x, y] + y \triangleright x = \{x, y\} \in \ker \mathcal{L}.$$

Moreover, $x \triangleright y \in Z(\mathfrak{a})$ since any derivation maps $Z(\mathfrak{a})$ to itself. Hence, $x \triangleright y \in \ker \mathcal{L} \cap Z(\mathfrak{a}) = \mathrm{Soc}(\mathfrak{a}, \triangleright)$ and thus $\mathrm{Soc}(\mathfrak{a}, \triangleright)$ is a strong left ideal. Since $\mathrm{Soc}(\mathfrak{a}, \triangleright) \triangleright \mathfrak{a} = \{0\} \subseteq \mathrm{Soc}(\mathfrak{a}, \triangleright)$, we conclude from Remark 1.3.10 that $\mathrm{Soc}(\mathfrak{a}, \triangleright)$ is an ideal. The quotient $(\mathfrak{a}, \triangleright)/\mathrm{Soc}(\mathfrak{a}, \triangleright)$ is the *retract* of $(\mathfrak{a}, \triangleright)$.

**Example 1.3.13.** Let $(\mathfrak{a}, \triangleright)$ be a post-Lie algebra. Then

$$\ker \mathcal{L} = \{x \in \mathfrak{a} \mid x \triangleright y = 0 \text{ for all } y \in \mathfrak{a}\},$$

is a post-Lie subalgebra of $(\mathfrak{a}, \triangleright)$. Indeed, it clearly is an ideal of $\mathfrak{a}^\circ$ and also $[x, y] = \{x, y\}$ for all $x, y \in \ker \mathcal{L}$. If $\mathfrak{a}$ is a trivial Lie algebra, then $\ker \mathcal{L} = \mathrm{Soc}(\mathfrak{a}, \triangleright)$ and thus $\ker \mathcal{L}$ is an ideal, but in general this is not always the case.

**Example 1.3.14.** Let $(\mathfrak{a}, \triangleright)$ be a post-Lie algebra. The *annihilator* of $(\mathfrak{a}, \triangleright)$ is defined as

$$\mathrm{Ann}(\mathfrak{a}, \triangleright) = \{x \in \mathfrak{a} \mid x \triangleright y = y \triangleright x = [x, y] = 0 \text{ for all } y \in \mathfrak{a}\},$$

and is an ideal of $(\mathfrak{a}, \triangleright)$.

**Example 1.3.15.** Let $(\mathfrak{a}, \triangleright)$ be a post-Lie algebra. Then every characteristic ideal of $\mathfrak{a}$ is a strong left ideal of $(\mathfrak{a}, \triangleright)$.

**Example 1.3.16.** Let $(\mathfrak{a}, \triangleright)$ be a post-Lie algebra and $r \in R$. Then $r\mathfrak{a}$ and $\{x \in \mathfrak{a} \mid rx = 0\}$ are ideals of $(\mathfrak{a}, \triangleright)$.

As for skew braces, we can also define the *opposite* post-Lie algebra. A particular example of this appeared in Examples 1.3.7 and 1.3.8

**Proposition 1.3.17.** *Let* $(\mathfrak{a}, \triangleright)$ *be a post-Lie algebra. Then* $(\mathfrak{a}_{\mathrm{op}}, \triangleright_{\mathrm{op}})$ *with*

$$x \triangleright_{\mathrm{op}} y = x \triangleright y + [x, y],$$

*is a post-Lie algebra whose sub-adjacent Lie algebra coincides with that of* $(\mathfrak{a}, \triangleright)$.

*Proof.* Let $x, y, z \in \mathfrak{a}$, then

$$\begin{aligned}[x \triangleright_{\mathrm{op}} y, z]_{\mathrm{op}} + [y, x \triangleright_{\mathrm{op}} z]_{\mathrm{op}} &= -[x \triangleright y, z] - [[x, y], z] - [y, x \triangleright y] - [y, [x, z]] \\ &= -x \triangleright [y, z] - [x, [y, z]] \\ &= x \triangleright_{\mathrm{op}} [y, z]_{\mathrm{op}}.\end{aligned}$$

The sub-adjacent Lie algebra of $(\mathfrak{a}_{\mathrm{op}}, \triangleright_{\mathrm{op}})$ coincides with that of $(\mathfrak{a}, \triangleright)$ since

$$\begin{aligned}[x, y]_{\mathrm{op}} + x \triangleright_{\mathrm{op}} y - y \triangleright_{\mathrm{op}} x &= -[x, y] + x \triangleright y + [x, y] - y \triangleright x - [y, x] \\ &= [x, y] + x \triangleright y - y \triangleright x \\ &= \{x, y\}.\end{aligned}$$

The statement now follows from Lemma 1.3.5. □

### 1.3.1 The affine Lie algebra

Let $\mathfrak{g}, \mathfrak{a}$ be Lie algebras and let

$$\delta : \mathfrak{g} \to \mathfrak{der}(\mathfrak{a}),$$

be a homomorphism of Lie algebras. We define the *semidirect sum* of $\mathfrak{g}$ and $\mathfrak{a}$, denoted $\mathfrak{a} \oplus_\delta \mathfrak{g}$, as the direct sum of the underlying modules $\mathfrak{a}$ and $\mathfrak{g}$ and

$$[(a, x), (b, y)] = ([a, b] + \delta_x(b) - \delta_y(a), [x, y]),$$

for $a, b \in \mathfrak{a}$, $x, y \in \mathfrak{g}$.

**Proposition 1.3.18.** *Let* $\mathfrak{g}, \mathfrak{a}$ *be Lie algebras and let*

$$\delta : \mathfrak{g} \to \mathfrak{der}(\mathfrak{a}),$$

*be a Lie algebra homomorphism. Then* $\mathfrak{a} \oplus_\delta \mathfrak{g}$*, as defined above, is a Lie algebra.*

We will particularly be interested in the semidirect sum

$$\mathfrak{aff}(\mathfrak{a}) := \mathfrak{a} \oplus_\delta \mathfrak{der}(\mathfrak{a}),$$

where $\delta = \mathrm{id}_{\mathfrak{der}(\mathfrak{a})}$. We call this the *affine Lie algebra on* $\mathfrak{a}$.

**Example 1.3.19.** Let $\mathfrak{a}$ be a Lie algebra and assume that $\mathfrak{a}$ can be embedded in an algebra $A$ (seen as a Lie algebra with its canonical Lie bracket) such that every derivation of $\mathfrak{a}$ extends uniquely to a derivation of the algebra $A$. This is, for example, the case if $R$ is a field and $A$ is the universal enveloping algebra $\mathcal{U}(\mathfrak{a})$. Recall that a linear map $\delta : A \to A$ is a *derivation* of the algebra $A$ if $\delta(ab) = \delta(a)b + a\delta(b)$ for all $a, b \in A$. Define

$$\rho : \mathfrak{aff}(\mathfrak{a}) \to \mathrm{End}(A, +) : (x, \delta) \mapsto \rho_{(x,\delta)},$$

where $\rho_{(x,\delta)}(y) = xy + \delta(y)$ and where $\mathrm{End}(A,+)$ is the algebra of module endomorphisms of $(A,+)$. Here, for $\delta \in \mathfrak{der}(\mathfrak{a})$, we also denote its unique extension to a derivation of $A$ by $\delta$. For $x, y \in \mathfrak{a}$ and $\delta, \chi \in \mathfrak{der}(\mathfrak{a})$ we find

$$\begin{aligned}
\left(\rho_{(x,\delta)}\rho_{(y,\chi)} - \rho_{(y,\chi)}\rho_{(x,\delta)}\right)(z) &= \rho_{(x,\delta)}(yz + \chi(z)) - \rho_{(y,\chi)}(xz + \delta(z)) \\
&= x(yz + \chi(z)) + \delta(yz + \chi(z)) - y(xz + \delta(z)) - \chi(xz + \delta(z)) \\
&= xyz - yxz + x\chi(z) - \chi(xz) + \delta(yz) - y\delta(z) + \delta\chi(z) - \chi\delta(z) \\
&= [x,y]z - \chi(x)z + \delta(y)z + [\delta,\chi](z) \\
&= \rho_{([x,y]+\delta(y)-\chi(x),[\delta,\chi])}(z) \\
&= \rho_{[(x,\delta),(y,\chi)]}(z).
\end{aligned}$$

We conclude that $\rho$ is an injective Lie algebra homomorphism. Although not every Lie algebra $\mathfrak{a}$ admits such an embedding, this is a nice interpretation of $\mathfrak{aff}(\mathfrak{a})$ to keep in mind, as a natural counterpart of the action of the holomorph of a group on itself.

**Example 1.3.20.** Let us discuss a special case of Example 1.3.19 for a pre-Lie algebra $(\mathfrak{a}, \triangleright)$ over $R$. Consider $A = R \oplus \mathfrak{a}$ with multiplication

$$(r,x)(s,y) = (rs, ry + sx),$$

then $A$ is an algebra with unit $(1,0)$. Moreover, $\mathfrak{a}$ embeds into $A$ since

$$(0,x)(0,y) = (0,0),$$

for any $x, y \in \mathfrak{a}$. Moreover, given a linear map $\delta : \mathfrak{a} \to \mathfrak{a}$ we can uniquely extend $\delta$ to a derivation of $A$ by setting $\delta(r,x) = (0, \delta(x))$. Here, it is crucial to note that the derivation of an algebra always maps 1 to 0. We find that $A$ satisfies the properties of Example 1.3.19. If $R = K$ is a field and $\mathfrak{a}$ is of finite dimension $n$, then we can identify $\mathfrak{a} = K^n$ and find that $\rho$ maps $\mathfrak{aff}(\mathfrak{a})$ to the ring of $(n+1) \times (n+1)$-matrices with 0 on the bottom row. More precisely, for $x \in K^n$ and $\delta$ and $n \times n$-matrix,

$$\rho_{(x,\delta)} = \begin{pmatrix} \delta & x \\ 0 & 0 \end{pmatrix},$$

where we interpret $\delta$ as a $n \times n$-matrix, $x$ as a column vector and the bottom left $0$ should be interpreted as a zero row vector of length $n$.

**Definition 1.3.21.** Let $\mathfrak{a}$ be a Lie algebra and let $\mathrm{pr}_{\mathfrak{a}} : \mathfrak{aff}(\mathfrak{a}) \to \mathfrak{a}$ denote the projection onto the first component. A Lie subalgebra $\mathfrak{g}$ of $\mathfrak{aff}(\mathfrak{a})$ is

1. *t-bijective* if $\mathrm{pr}_{\mathfrak{a}}$ restricts to a bijection $\mathfrak{g} \to \mathfrak{a} : (x,\delta) \mapsto x$. Equivalently, for every element $x \in \mathfrak{a}$ there exists a unique $\delta \in \mathfrak{der}(\mathfrak{a})$ such that $(x,\delta) \in \mathfrak{g}$.
2. *t-injective* if $\mathrm{pr}_{\mathfrak{a}}$ is injective on $\mathfrak{g}$. Equivalently, for every element $x \in \mathfrak{a}$ there exists at most one $\delta \in \mathfrak{der}(\mathfrak{a})$ such that $(x,\delta) \in \mathfrak{g}$.
3. *t-surjective* if the restriction of $\mathrm{pr}_{\mathfrak{a}}$ to $\mathfrak{g}$ is surjective. Equivalently, for every element $x \in \mathfrak{a}$ there exists at least one $\delta \in \mathfrak{der}(\mathfrak{a})$ such that $(x,\delta) \in \mathfrak{g}$.

**Proposition 1.3.22** ([30, Proposition 2.12])**.** *Let $\mathfrak{a}$ be a Lie algebra. There exists a bijective correspondence between operations $\triangleright$ such that $(\mathfrak{a}, \triangleright)$ is a post-Lie algebra and t-bijective Lie subalgebras of $\mathfrak{aff}(\mathfrak{a})$.*

*Proof.* Assume that we are given an operation $\triangleright$ such that $(\mathfrak{a}, \triangleright)$ is a post-Lie algebra. Then (P1) is satisfied if and only if $\mathcal{L}_x : y \mapsto x \triangleright y$ is a derivation of $\mathfrak{a}$ for all $x \in \mathfrak{a}$. Consider the following submodule of $\mathfrak{aff}(\mathfrak{a})$

$$\mathfrak{g} := \{(x, \mathcal{L}_x) \mid x \in \mathfrak{a}\}.$$

We claim that $\mathfrak{g}$ is a $t$-bijective Lie subalgebra of $\mathfrak{aff}(\mathfrak{a})$. It suffices to show that it is a Lie subalgebra; the $t$-bijectivity follows trivially. For $x, y \in \mathfrak{a}$, we find

$$[(x, \mathcal{L}_x), (y, \mathcal{L}_y)] = ([x, y] + x \triangleright y - y \triangleright x, [\mathcal{L}_x, \mathcal{L}_y]),$$

this element is contained in $\mathfrak{g}$ if and only if $\mathcal{L}_{[x,y]+x\triangleright y-y\triangleright x} = [\mathcal{L}_x, \mathcal{L}_y]$. Evaluating this equality in an element $z \in \mathfrak{a}$, we obtain

$$[x, y] \triangleright z + (x \triangleright y) \triangleright z - (y \triangleright x) \triangleright z = x \triangleright (y \triangleright z) - y \triangleright (x \triangleright z),$$

which is precisely (P2). We conclude that $\mathfrak{g}$ is a $t$-bijective Lie subalgebra of $\mathfrak{aff}(\mathfrak{a})$.

Conversely, assume that we are given a $t$-bijective Lie subalgebra $\mathfrak{g}$ of $\mathfrak{aff}(\mathfrak{a})$. For $x \in \mathfrak{g}$ we define $\mathcal{L}_x \in \mathfrak{der}(\mathfrak{a})$ as the unique derivation such that $(x, \mathcal{L}_x) \in \mathfrak{g}$. By exactly the same argument as before, we find that $(\mathfrak{a}, \triangleright)$, with $x \triangleright y := \mathcal{L}_x(y)$, is a post-Lie algebra. □

Note that the sub-adjacent Lie bracket of a post-Lie algebra $(\mathfrak{a}, \triangleright)$ is precisely the Lie bracket such that

$$\mathfrak{a}^\circ \to \mathfrak{aff}(\mathfrak{a}) : x \mapsto (x, \mathcal{L}_x),$$

is a Lie algebra homomorphism. Assume moreover that $R$ is a field and that $\mathfrak{a}$ is finite dimensional. By the above homomorphism, combined with Example 1.3.20, the following result follows.

**Proposition 1.3.23.** *Let $(\mathfrak{a}, \triangleright)$ be a pre-Lie algebra of dimension $n$ over a field $K$. Then the sub-adjacent Lie algebra $\mathfrak{a}^\circ$ has a representation of dimension $n + 1$.*

### 1.3.2 Nilpotency

One can define multiple notions of nilpotency for post-Lie algebras. We decide to name them similarly to what is common for skew braces.

**Definition 1.3.24.** Let $(\mathfrak{a}, \triangleright)$ be a post-Lie algebra. We define $\mathfrak{a}^1 = \mathfrak{a}$ and $\mathfrak{a}^{n+1} = \mathfrak{a} \triangleright \mathfrak{a}^n$ for $n \geq 1$. The descending series of strong left ideals

$$\mathfrak{a}^1 \supseteq \mathfrak{a}^2 \supseteq \dots,$$

is called the *left series* of $(\mathfrak{a}, \triangleright)$. If there exists some $n \geq 1$ such that $\mathfrak{a}^n = \{0\}$, then $(\mathfrak{a}, \triangleright)$ is *left nilpotent*. In this case, the smallest $n \geq 0$ such that $A^{n+1} = \{0\}$ is called the *left nilpotency class* of $(\mathfrak{a}, \triangleright)$.

**Definition 1.3.25.** A post-Lie algebra $(\mathfrak{a}, \triangleright)$ is *left nil* if for any $x \in \mathfrak{a}$ the map $\mathcal{L}_x$ is nilpotent.

**Proposition 1.3.26.** *Let $(\mathfrak{a}, \triangleright)$ be a finite dimensional post-Lie algebra over a field $K$. Then $(\mathfrak{a}, \triangleright)$ is left nil if and only if $(\mathfrak{a}, \triangleright)$ is left nilpotent.*

*Proof.* One implication is trivial. The other implication is a direct consequence of Engel's theorem since the Lie algebra $\mathfrak{a}^\circ$ acts on the vector space $\mathfrak{a}$ by nilpotent endomorphisms. □

**Corollary 1.3.27.** *Let $(\mathfrak{a}, \triangleright)$ be a post-Lie algebra of finite size. Then $(\mathfrak{a}, \triangleright)$ is left nil if and only if $(\mathfrak{a}, \triangleright)$ is left nilpotent.*

*Proof.* One implication is trivial. For the other implication, assume that $(\mathfrak{a}, \triangleright)$ is left nil and let $p$ be a prime dividing the order of $\mathfrak{a}$. Then the quotient $(\mathfrak{a}, \triangleright)/(p\mathfrak{a})$ is finite dimensional over the field $\mathbb{F}_p$ of order $p$. By Proposition 1.3.26 there exists some $n_p \geq 1$ such that $\mathfrak{a}^{n_p} \subseteq p\mathfrak{a}$. In particular, we find $\mathfrak{a}^{n_p+1} \subseteq p\mathfrak{a}^2$ and continuing in this way we find $\mathfrak{a}^{2n_p} \subseteq p^2\mathfrak{a}$ and more generally $\mathfrak{a}^{rn_p} \subseteq p^r\mathfrak{a}$ for $r \geq 1$. Let $p_1^{r_1} \dots p_n^{r_n}$ be the prime decomposition of $|\mathfrak{a}|$, then for $m = \max\{n_{p_i} r_i \mid 1 \leq i \leq n\}$ we find $\mathfrak{a}^m \subseteq \bigcap_{i=1}^n p_i^{r_i}\mathfrak{a} = \{0\}$. □

**Definition 1.3.28.** For a post-Lie algebra $(\mathfrak{a}, \triangleright)$ we define $\mathfrak{a}^{(1)} = A$ and $\mathfrak{a}^{(n+1)} = \mathfrak{a}^{(n)} \triangleright \mathfrak{a}$ for $n \geq 1$. The descending series of ideals

$$\mathfrak{a} = \mathfrak{a}^{(1)} \supseteq \mathfrak{a}^{(2)} \supseteq \mathfrak{a}^{(3)} \supseteq \dots$$

is called the *right series* of $(\mathfrak{a}, \triangleright)$. We say that $(\mathfrak{a}, \triangleright)$ is *right nilpotent* if the right series reaches $\{0\}$. The smallest integer $n$ such that $\mathfrak{a}^{(n+1)} = \{0\}$ is called its *right nilpotency class*.

A post-Lie algebra $(\mathfrak{a}, \triangleright)$ is *transitive* if the map $x \mapsto x \triangleright y + x$ is a bijection for all $x \in \mathfrak{a}$. If the right multiplication

$$x \mapsto x \triangleright y,$$

is nilpotent for all $y \in \mathfrak{a}$, then clearly $(\mathfrak{a}, \triangleright)$ is transitive. A post-Lie algebra satisfying this property is *right nil*. The following theorem combines results of Scheuneman, Helmstetter and Segal.

**Theorem 1.3.29** ([85, 141, 142])**.** *Let $(\mathfrak{a}, \triangleright)$ be a finite dimensional pre-Lie algebra over the field $\mathbb{R}$ or $\mathbb{C}$. Then the following statements hold:*

1. *$(\mathfrak{a}, \triangleright)$ is transitive if and only if it is right nil,*
2. *if $(\mathfrak{a}, \triangleright)$ is left nilpotent, then it is right nil,*
3. *if $(\mathfrak{a}, \triangleright)$ is right nil and $\mathfrak{a}^\circ$ is nilpotent, then $(\mathfrak{a}, \triangleright)$ is left nilpotent.*

*Remark* 1.3.30. One can also define *right nil* skew braces in a similar way using the operation $*$, but not much is known about them, see [164]. For *left nil* braces, a similar result to Proposition 1.3.26 was proved by Smoktunowicz [144].

Auslander [8] conjectured that the socle of any transitive finite dimensional pre-Lie algebra over $\mathbb{R}$ is non-trivial. The following counterexample of dimension 4 was provided by Fried [75]. For left nilpotent pre-Lie algebras of dimension at most 3, Kim proved that the conjecture holds [98, Corollary 2.7].

**Example 1.3.31.** Consider $(\mathfrak{a}, \triangleright)$ where $\mathfrak{a}$ is the trivial Lie algebra on $\mathbb{R}^4$ and define

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \\ t_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \\ t_2 \end{pmatrix} = \begin{pmatrix} 0 \\ t_1 x_2 \\ t_1 y_2 \\ -x_1 z_2 + y_1 y_2 - z_1 x_2 \end{pmatrix},$$

Then

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \\ t_1 \end{pmatrix} \triangleright \left( \begin{pmatrix} x_2 \\ y_2 \\ z_2 \\ t_2 \end{pmatrix} \triangleright \begin{pmatrix} x_3 \\ y_3 \\ z_3 \\ t_3 \end{pmatrix} \right) = \begin{pmatrix} x_1 \\ y_1 \\ z_1 \\ t_1 \end{pmatrix} \triangleright \begin{pmatrix} 0 \\ t_2 x_3 \\ t_2 y_3 \\ -x_2 z_3 + y_2 y_3 - z_2 x_3 \end{pmatrix}$$
$$= \begin{pmatrix} 0 \\ 0 \\ t_1 t_2 x_3 \\ -x_1 t_2 y_3 + y_1 t_2 x_3 \end{pmatrix},$$

and

$$\left(\begin{pmatrix}x_1\\y_1\\z_1\\t_1\end{pmatrix}\triangleright\begin{pmatrix}x_2\\y_2\\z_2\\t_2\end{pmatrix}\right)\triangleright\begin{pmatrix}x_3\\y_3\\z_3\\t_3\end{pmatrix}=\begin{pmatrix}0\\t_1x_2\\t_1y_2\\-x_1z_2+y_1y_2-z_1x_2\end{pmatrix}\triangleright\begin{pmatrix}x_3\\y_3\\z_3\\t_3\end{pmatrix}$$
$$=\begin{pmatrix}0\\(-x_1z_2+y_1y_2-z_1x_2)x_3\\(-x_1z_2+y_1y_2-z_1x_2)y_3\\t_1x_2y_3-t_1y_2x_3\end{pmatrix},$$

hence

$$\begin{pmatrix}x_1\\y_1\\z_1\\t_1\end{pmatrix}\triangleright\left(\begin{pmatrix}x_2\\y_2\\z_2\\t_2\end{pmatrix}\triangleright\begin{pmatrix}x_3\\y_3\\z_3\\t_3\end{pmatrix}\right)-\left(\begin{pmatrix}x_1\\y_1\\z_1\\t_1\end{pmatrix}\triangleright\begin{pmatrix}x_2\\y_2\\z_2\\t_2\end{pmatrix}\right)\triangleright\begin{pmatrix}x_3\\y_3\\z_3\\t_3\end{pmatrix}$$
$$=\begin{pmatrix}0\\x_1z_2x_3-y_1y_2x_3+z_1x_2x_3\\t_1t_2x_3+x_1z_2y_3-y_1y_2y_3+z_1x_2y_3\\-x_1t_2y_3+y_1t_2x_3-t_1x_2y_3+t_1y_2x_3\end{pmatrix}$$
$$=\begin{pmatrix}0\\(x_1z_2+z_1x_2)x_3-y_1y_2x_3\\t_1t_2x_3+(x_1z_2+z_1x_2)y_3-y_1y_2y_3\\(t_1x_2+x_1t_2)y_3-(t_1y_2+y_1t_2)x_3\end{pmatrix},$$

which is invariant under changing the indices 1 and 2, so $(\mathfrak{a},\triangleright)$ is indeed a pre-Lie algebra. The pre-Lie algebra $(\mathfrak{a},\triangleright)$ is left nilpotent hence transitive, but $\mathrm{Soc}(\mathfrak{a},\triangleright)=\{0\}$.

## 1.4 Filtered algebraic structures

The Lazard correspondence [112] is an intriguing display of how an idea from differential geometry leads to strong results when mimicked in a purely algebraic context. The objects of interest in this correspondence are filtered Lie rings and filtered groups. In this section, we first treat such filtered structures. We then discuss how these can be interpreted as metric spaces, which leads to a natural notion of a completion in this context, which we see from a category theoretical perspective. At last, we introduce the Lazard correspondence starting from a differential-geometric point of view.

### 1.4.1 Filtrations on algebraic structures

**Definition 1.4.1.** A *filtered group* is a group $G$ together with a descending chain of normal subgroups

$$G=G_1\supseteq G_2\supseteq\dots$$

such that $[G_i,G_j]\subseteq G_{i+j}$. Such a chain is a *filtration* on $G$. A filtration is *finite* if there exists some $i\geq 1$ such that $G_i=\{1\}$. Any subgroup $H$ of a filtered group $G$ has a natural filtration given by $H_i=H\cap G_i$. A *homomorphism* of filtered groups $f:G\to H$ is a group homomorphism such that $f(G_i)\subseteq H_i$ for all $i\geq 1$.

The following statement is a well-known consequence of the three subgroup lemma and shows that the lower central series of a group is a filtration.

**Lemma 1.4.2.** *Let $G$ be a group. Set $\gamma^1(G) = G$ and $\gamma^{i+1}(G) = [G, \gamma^i(G)]$ for $i \geq 1$. Then $[\gamma^i(G), \gamma^j(G)] \subseteq \gamma^{i+j}(G)$ for all $i, j \geq 1$.*

**Definition 1.4.3.** A *filtered Lie algebra* is a Lie algebra $\mathfrak{a}$ with a descending chain of ideals

$$\mathfrak{a} = \mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \dots$$

such that $[\mathfrak{a}_i, \mathfrak{a}_j] \subseteq \mathfrak{a}_{i+j}$ for all $i, j \geq 1$. Such a chain is a *filtration* on $\mathfrak{a}$. A filtration is *finite* if there exists some $i \geq 1$ such that $\mathfrak{g}_i = \{0\}$. A *homomorphism* of filtered Lie algebra $f : \mathfrak{a} \to \mathfrak{b}$ is a Lie algebra homomorphism such that $f(\mathfrak{a}_i) \subseteq \mathfrak{b}_i$ for all $i \geq 1$.

The following lemma is a well-known consequence of the Jacobi identity and proves that the lower central series of a Lie algebra is a filtration.

**Lemma 1.4.4.** *Let $\mathfrak{g}$ be a Lie algebra. Set $\gamma^1(\mathfrak{g}) = \mathfrak{g}$ and $\gamma^{i+1}(\mathfrak{g}) = [\mathfrak{g}, \gamma^i(\mathfrak{g})]$ for $i \geq 1$, then $[\gamma^i(\mathfrak{g}), \gamma^j(\mathfrak{g})] \subseteq \gamma^{i+j}(\mathfrak{g})$ for all $i, j \geq 1$.*

**Definition 1.4.5.** A *filtered algebra* is an algebra $A$ together with a descending chain of ideals

$$A = A_0 \supseteq A_1 \supseteq A_2 \supseteq \dots$$

such that $A_i A_j \subseteq A_{i+j}$. Such a chain is a *filtration* on $A$. A filtration is *finite* if there exists some $i \geq 0$ such that $A_i = \{0\}$. A *homomorphism* of filtered algebras $f : A \to B$ is an algebra homomorphism such that $f(A_i) \subseteq B_i$ for all $i \geq 0$.

*Remark* 1.4.6. Contrary to groups and Lie algebras, we start the filtration of an algebra at index 0 instead of 1. This is because otherwise the presence of a unit would imply $x = 1^n x \in A_n$ for all $x \in A$ and $n \geq 1$.

**Example 1.4.7.** Let $A$ be a algebra and $I$ an ideal of $A$, then we have a natural filtration where $A_0 = A$ and $A_1 = I$ and $A_{i+1} = IA_i$. This filtration is finite if and only if $I$ is a nilpotent ideal.

**Example 1.4.8.** Let $M$ be a filtered abelian group and consider the algebra $\mathrm{End}_f(M)$ of all group endomorphisms $f : M \to M$ such that $f(M_i) \subseteq M_i$. Then $\mathrm{End}_f(M)$ has a canonical filtration given by

$$\mathrm{End}_f(M)_i = \{f \in \mathrm{End}_f(M) \mid f(M_j) \subseteq M_{i+j} \text{ for all } j \geq 1\}.$$

Note in particular that if $M_{d+1} = \{0\}$, then $\mathrm{End}_f(M)_d = \{0\}$.

**Example 1.4.9.** Let $R$ be a commutative ring and $X$ a set, then $R[X]$, the polynomial ring over $R$ with variables $X$, has a natural filtration given by

$$R[X]_i = \{f \in R[X] \mid f \text{ is a linear combination of monomials of degree at least } i\}.$$

**Example 1.4.10.** Let $R$ be a commutative ring and $X$ a set. Recall that $R[[X]]$, the $R$-algebra of *formal power series over $R$ with variables $X$*, is the set

$$\left\{ \sum_{i=0}^{\infty} f_i \mid f_i \text{ is a linear combination of monomials of degree } i \text{ in } R[X] \right\},$$

with addition and multiplication

$$\sum_{i=0}^{\infty} f_i \sum_{i=0}^{\infty} g_i = \sum_{i=0}^{\infty} (f_i + g_i), \quad \left(\sum_{i=0}^{\infty} f_i\right)\left(\sum_{i=0}^{\infty} g_i\right) = \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} f_j g_{i-j}\right).$$

Then $R[[X]]$ has a natural filtration given by

$$R[[X]]_j = \left\{ \sum_{i=j}^{\infty} f_i \in R[[X]] \right\}.$$

**Example 1.4.11.** Let $A$ be a filtered algebra, then $\mathfrak{a} = A_1$ has a filtered Lie algebra structure where the Lie bracket is the commutator bracket and the filtration is given by $\mathfrak{a}_i = A_i$.

**Example 1.4.12.** Let $\mathfrak{g}$ be a filtered Lie algebra over a field $K$. Then the universal enveloping algebra $\mathcal{U}(\mathfrak{g})$ has a natural filtration given by

$$\mathcal{U}(\mathfrak{g})_i := \operatorname{span}\{x_1 \cdots x_r \mid r \geq 1, x_j \in \mathfrak{g}_{n_j} \text{ with } n_1 + \cdots + n_r \geq i\},$$

for $i \geq 1$, see [33, Section 3].

**Example 1.4.13.** Let $A$ be a filtered algebra. Then for any $i \geq 1$, the set $1 + A_i$ is closed under multiplication. Let $G$ be a subgroup of the multiplicative monoid $1 + A_1$. Then $G$ has a natural filtration given by $G_i = G \cap (1 + A_i)$. Indeed, if we take an element $1 + x \in G_i$ and consider its inverse $1 + x' \in G$, then

$$1 = (1 + x)(1 + x') = 1 + x + x' + xx', \tag{1.11}$$

hence $(1+x)x' = -x \in A_i$ and thus $(1+x')(1+x)x' = x' \in A_i$. This implies that $G_i$ is a subgroup of $G$. Also, let $(1 + x) \in G_i$, $(1 + y) \in G_j$ with respective inverses $1 + x' \in G_i$ and $1 + y' \in G_j$. Then, working in the quotient $A/A_{i+j}$ we find

$$\begin{aligned}(1 + x)(1 + y)(1 + x')(1 + y') + A_{i+j} &= (1 + x + y)(1 + x' + y') + A_{i+j} \\ &= 1 + x + y + x' + xx' + yx' + y' + xy' + yy' + A_{i+j} \\ &= 1 + x + y + x' + xx' + y' + yy' + A_{i+j} \\ &= 1 + A_{i+j},\end{aligned}$$

where we used (1.11) to obtain the last equality. We conclude that $G$ is indeed a filtered group for the given filtration.

## 1.4.2 Complete algebraic structures

We now discuss the notion of completeness for filtered groups. Mutatis mutandi, the same definitions also work for filtered Lie algebras and filtered algebras.

Let $G$ be a filtered group. The limit of the diagram

$$\ldots \longrightarrow G/G_3 \longrightarrow G/G_2 \longrightarrow G/G_1$$

in the category of filtered groups exists and can be explicitly constructed as

$$\varprojlim G/G_i = \{(g_iG_i)_{i\geq 1} \mid g_{i+1}G_i = g_iG_i \text{ for all } i \geq 1\},$$

with the filtration given by

$$(\varprojlim G/G_i)_j = \{(g_iG_i)_{i\geq 1} \in \varprojlim G/G_i \mid g_i \in G_j \text{ for all } i \geq 1\},$$

for $j \geq 1$, and the homomorphisms

$$\varprojlim G/G_i \to G/G_k : (g_iG_i)_{i\geq 1} \mapsto g_kG_k.$$

**Definition 1.4.14.** A filtered group $G$ is *complete* if the canonical homomorphism $G \to \varprojlim G/G_i$ is an isomorphism.

We shortly discuss why the term completeness is justified here. For any $a, b \in G$, the set

$$\{i \geq 1 \mid aG_i = bG_i\}$$

is non-empty since it definitely contains 1. Therefore, the map

$$d : G^2 \to G : (a, b) \mapsto \inf\{2^{-i} \mid aG_i = bG_i\}$$

is well-defined and it is symmetric and subadditive, hence it defines a pseudometric on $G$. This pseudometric is non-degenerate if and only if for any $a \neq b \in G$ there exists some $i$ such that $aG_i \neq bG_i$, or equivalently if $\bigcap_{i\geq 1} G_i = \{1\}$.

**Proposition 1.4.15.** *A filtered group $G$ is complete if and only if $(G, d)$ is a complete metric space.*

*Proof.* First of all, note that the kernel of the canonical homomorphism $f : G \to \varprojlim G/G_i$ is precisely $\bigcap_{i\geq 1} G_i$, hence $f$ is injective if and only if $d$ defines a metric on $G$. Also, since $f^{-1}((\varprojlim G/G_i)_k) = G_k$ we find $d(f(a), f(b)) = d(a, b)$ for all $a, b \in G$. Moreover, $f(G)$ is dense in $\varprojlim G/G_i$ since for any $(a_iG_i)_{i\geq 1} \in \varprojlim G/G_i$ and $k \geq 1$ we find

$$d(f(a_k), (a_iG_i)_{i\geq 1}) \leq 2^{-k}.$$

We therefore find that $G$ is complete if and only if $f(G)$ is complete. It is left as an exercise to verify that $\varprojlim G/G_i$ is complete. Since $f(G)$ is dense in $\varprojlim G/G_i$ we find that $G$ is complete precisely when $f$ is bijective. At last, if $f$ is bijective, then since $f^{-1}((\varprojlim G/G_i)_k) = G_k$ it follows that $f$ is an isomorphism. □

**Example 1.4.16.** If $G$ is a filtered group with a finite filtration, say $G_d = \{1\}$, then $d(a, b) < 2^{-d}$ if and only if $a = b$. It follows that $G$ is a discrete space, which in particular implies that it is complete.

**Example 1.4.17.** Let $R$ be a commutative ring and $X$ a set. Then $R[X]$, with the filtration as in Example 1.4.9, is a metric space since $\bigcap_{i=0}^{\infty} R[X] = \{0\}$ but it is not complete since for example the sequence

$$1, 1 + x, 1 + x + x^2, 1 + x + x^2 + x^3, \ldots$$

is Cauchy, but it does not have a limit in $R[X]$. However, this sequence does have a limit in $R[[X]]$, namely the element $\sum_{i=0}^{\infty} x^i$. More generally, one sees that $R[[X]]$ is complete and $R[X]$ is a dense subset of $R[[X]]$ since

$$\sum_{i=0}^{\infty} f_i = \lim_{k\to\infty} \sum_{i=0}^{k} f_i,$$

for any $\sum_{i=0}^{\infty} f_i \in R[[X]]$.

**Example 1.4.18.** Let $A$ be a complete filtered algebra, then the filtered Lie algebra structure on $A_1$ as in Example 1.4.11 is also complete.

**Example 1.4.19.** Let $A$ be a complete filtered algebra, then $1 + x \in 1 + A_1$ has a multiplicative inverse given by $\sum_{i=0}^{\infty}(-1)^i x^i$. Moreover, the group $G = 1 + A_1$, seen as a filtered group as in Example 1.4.13, is complete since the inclusion map $G \to A$ is an isometry (with the metric on both structures coming from their filtration) and $1 + A_1$ is closed in $R$.

### 1.4.3 The Lazard correspondence

Although we use slightly different terminology, all of the statements in this section are contained in or are a direct consequence of [96, 112].

Let us consider $\mathbb{Q}[[x, y]] := \mathbb{Q}[[\{x, y\}]]$ as a complete filtered ring as in Example 1.4.10. Then we can define the exponential of any $f \in \mathbb{Q}[[x, y]]_1$ using its usual power series. The sequence

$$1, 1 + f, 1 + f + \frac{1}{2}f^2, \ldots, \sum_{k=0}^{i} \frac{1}{k!} f^k, \ldots$$

is a Cauchy series since $f^k \in \mathbb{Q}[[x, y]]_k$. We define the *exponential* of $f$ as

$$\exp(f) = \sum_{k=0}^{\infty} \frac{1}{k!} f^k = \lim_{i\to\infty} \sum_{k=0}^{i} \frac{1}{k!} f^k.$$

Clearly, $\exp(f) \in 1 + \mathbb{Q}[[x, y]]_1$. Conversely, if we let $f \in 1 + \mathbb{Q}[[x, y]]_1$, then we can define its *logarithm* as

$$\log(f) = \sum_{k=1}^{\infty} (-1)^{k+1} \frac{1}{k} (f - 1)^k = \lim_{i\to\infty} \sum_{k=1}^{i} (-1)^{k+1} \frac{1}{k} (f - 1)^k.$$

Note that this limit exists since $(f - 1)^k \in \mathbb{Q}[[x, y]]_k$.

The Baker–Campbell–Hausdorff formula is the element of $\mathbb{Q}[[x, y]]$, so a formal series in two variables, defined by

$$\mathrm{BCH}(x, y) = \log(\exp(x) \exp(y)), \tag{1.12}$$

and its remarkable property is that it can be expressed using only the elements $x, y$ and the commutator Lie bracket. Its first terms are given by

$$\mathrm{BCH}(x, y) = x + y + \frac{1}{2}[x, y] + \frac{1}{12}([x, [x, y]] + [y, [y, x]]) - \frac{1}{24}[y, [x, [x, y]]] + \ldots, \tag{1.13}$$

where higher terms are of order at least 5. Recall that the origin of the Baker–Campbell–Hausdorff formula lies in Lie theory. If $G$ is a Lie group with associated Lie algebra $\mathfrak{g}$, then the exponential map $\exp : \mathfrak{g} \to G$ can always be restricted to a diffeomorphism $\exp : U \to V$ for $0 \in U$ an open subset of $\mathfrak{g}$ and $1 \in V$ an open subset of $G$. Moreover, $U$ and $V$ can always be chosen such that (1.13) converges on $U^2$ and $\exp(\mathrm{BCH}(x, y)) = \exp(x) \exp(y)$ for all $x, y \in U$. So the BCH formula locally transfers the group structure onto the Lie algebra. The underlying idea of the Lazard correspondence is to exploit this behavior in a, as general as possible, purely algebraic setting. The two obstacles to overcome here are that the BCH formula is, in general, an infinite series and that we need to be able to divide by certain integers.

Let us more carefully study which denominators can appear. For $\mathcal{P}$ a set of primes, we define

$$\mathbb{Q}_{\mathcal{P}} = \left\{ \frac{n}{m} \in \mathbb{Q} \mid \text{the prime factors of } m \text{ are contained in } \mathcal{P} \right\}.$$

For $i \geq 0$, we define $\mathcal{P}_i$ as the set of all prime numbers less than or equal to $i$. We now define

$$\mathcal{Q} = \left\{ \sum_{i=0}^{\infty} \alpha_i f_i \in \mathbb{Q}[[x,y]] \mid \alpha_i \in \mathbb{Q}_{\mathcal{P}_i}, f_i \text{ is a sum of monomials of degree } i \right\}.$$

Since the rings $\mathbb{Q}_{\mathcal{P}_i}$ form an ascending chain, it follows that $\mathcal{Q}$ is a closed subring of $\mathbb{Q}[[x,y]]$. Also, if $\sum_{i=j}^{\infty} \alpha_i f_i \in \mathcal{Q}_j$, then $\beta(\sum_{i=j}^{\infty} \alpha_i f_i) \in \mathcal{Q}_j$ for all $\beta \in \mathbb{Q}_{\mathcal{P}_j}$. In particular, we find that the exponential and logarithmic maps restrict to a bijection between $1 + \mathcal{Q}_1$ and $\mathcal{Q}_1$. As the elements $x, y$ are contained in $\mathcal{Q}_1$ it follows that $\mathrm{BCH}(x,y) \in \mathcal{Q}_1$. Since an iterated Lie bracket of order $n$ (meaning, involving $n-1$ Lie brackets and thus $n$ arguments) in the elements $x$ and $y$ is clearly contained in $\mathcal{Q}_n \setminus \mathcal{Q}_{n-1}$, we find that the coefficients of order $n$ in (1.13) are contained in $\mathbb{Q}_{\mathcal{P}_n}$.

**Definition 1.4.20.** Let $G$ be a group and $\mathcal{P}$ a set of prime numbers. Then $G$ is *$\mathcal{P}$-divisible* if for every element $g \in G$ and every $n$ whose prime divisors are contained in $\mathcal{P}$, there exists a unique $h \in G$ such that $h^n = g$. This unique element is denoted $g^{\frac{1}{n}}$. If $G$ is an abelian group and its group operation is denoted by $+$, then we use the notation $\frac{1}{n}g$.

**Definition 1.4.21.** A *Lazard Lie algebra* is a Lie algebra $\mathfrak{g}$ together with a finite filtration such that $(\mathfrak{g}_i, +)$ is $\mathcal{P}_i$-divisible for all $i \geq 1$.

Note that in a Lazard Lie algebra $\mathfrak{g}$ the a priori infinite series $\mathrm{BCH}(x,y)$ terminates at some point for all $x, y \in \mathfrak{g}$ since the term of order $i$ is contained in $\mathfrak{g}_i$. Moreover, since any term of order $i$ is contained in $\mathfrak{g}_i$ and we have the earlier observation that the denominators of coefficients of order $i$ only involve primes at most $i$, we can also give sense to these denominators in a unique way. We thus obtain the first construction in the Lazard correspondence.

**Theorem 1.4.22.** *Let $\mathfrak{g}$ be a Lazard Lie algebra. Then the operation*

$$\mathrm{BCH} : \mathfrak{g}^2 \to \mathfrak{g} : (x,y) \mapsto \mathrm{BCH}(x,y),$$

*defines a group operation on $\mathfrak{g}$ and the $\mathfrak{g}_i$ form a filtration on this group. We denote this filtered group by $\mathbf{Laz}(\mathfrak{g})$.*

Clearly, if $\mathfrak{g}$ is a Lazard Lie algebra, then $0$ is the identity element of $\mathbf{Laz}(\mathfrak{g})$. Also, if $x, y \in \mathfrak{g}$ are such that $[x,y] = 0$, then $\mathrm{BCH}(x,y) = x + y$. In particular, the $n$-th power of $x$ in $\mathbf{Laz}(\mathfrak{g})$ is $nx$.

**Definition 1.4.23.** A *Lazard algebra* is an algebra together with a finite filtration such that $(A_i, +)$ is $\mathcal{P}_i$-divisible for all $i \geq 0$.

Let $A$ be a Lazard algebra. Similar to as in $\mathcal{Q}$ as above, we can define mutually inverse maps $\exp : R_1 \to 1 + R_1$ and $\log : 1 + R_1 \to R_1$ by

$$\exp(a) = \sum_{k=0}^{\infty} \frac{1}{k!} a^k,$$

$$\log(a) = \sum_{k=1}^{\infty} (-1)^{k+1} \frac{1}{k} (a-1)^k.$$

and thus we also obtain map

$$\mathrm{BCH} : A_1^2 \to A_1 : (a, b) \mapsto \log(\exp(a)\exp(b)).$$

Since $A$ is Lazard, for any $a, b \in A_1$ there exists a unique filtered ring homomorphism $\psi : \mathcal{Q} \to A$ mapping $x$ to $a$ and $y$ to $b$ and thus we can really interpret $\mathrm{BCH}(a, b)$ as evaluating the expression (1.13) in the elements $a, b$. This implies that if a Lazard Lie algebra embeds into a Lazard algebra, then we can explicitly calculate the BCH formula on the Lie algebra by using the logarithmic and exponential maps in the enveloping algebra.

**Proposition 1.4.24.** *Let $\mathfrak{g}$ be a Lazard Lie algebra and let $A$ be a Lazard algebra. If $f : \mathfrak{g} \to A$ is a homomorphism of filtered Lie algebras, then*

$$\mathbf{Laz}(\mathfrak{g}) \to \exp(f(\mathfrak{g})) : x \mapsto \exp(f(x)),$$

*is a group homomorphism, where the group operation on $\exp(f(\mathfrak{g}))$ is the ring multiplication in $A$.*

Once again working in the filtered ring $\mathcal{Q}$, set $g = \exp(x)$ and $h = \exp(y)$ and define

$$P(g, h) = \exp(\log(g) + \log(h)), \tag{1.14}$$
$$Q(g, h) = \exp(\log(g)\log(h) - \log(g)\log(h)). \tag{1.15}$$

Let $G = 1 + \mathcal{Q}_1$, which we consider as a complete filtered group as in Example 1.4.13. Then $P(g, h)$ can be expressed as an infinite product in $G$, more precisely $P(g, h) = \lim_{i\to\infty} \prod_{k=1}^{i} P_i$, where $P_i \in G_i$ and each $P_i$ can be expressed as a product of rational powers of group commutators of order $i$ in the elements $g$ and $h$. More precisely,

$$P(g, h) = gh[g, h]^{-\frac{1}{2}}[g, [g, h]]^{\frac{1}{12}}[g, [g, [g, h]]]^{-\frac{1}{24}}[h, [h, [g, h]]]^{\frac{1}{24}} \cdots, \tag{1.16}$$

where in this case $[g, h]$ is the group theoretic commutator in $G$ and further factors are of order at least 5. The same is true for $Q(g, h)$ and

$$Q(g, h) = [g, h][g, [g, h]]^{\frac{1}{2}}[h, [g, h]]^{\frac{1}{2}}[g, [g, [g, h]]]^{\frac{1}{3}}[h, [g, [g, h]]]^{\frac{1}{4}}[h, [h, [g, h]]]^{\frac{1}{3}} \cdots, \tag{1.17}$$

where further factors are of order at least 5. Note that the roots in the above expressions make sense since $\log(x^n) = n\log(x)$ for all $i \geq 1$, $x \in 1 + \mathcal{Q}_i$ and $n \in \mathbb{Z}$, hence $\exp(\frac{1}{n}\log(x)) \in 1 + \mathcal{Q}_i$ is the unique element in $1 + \mathcal{Q}_1$ that satisfies $(\exp(\frac{1}{n}\log(x)))^n = x$. In other words, $G_i$ is $\mathcal{P}_i$-divisible.

**Definition 1.4.25.** A *Lazard group* is a group $G$ with a finite filtration such that $G_i$ is $\mathcal{P}_i$-divisible for every $i \geq 1$.

If $H$ is a Lazard group and $g, h \in H$, then $P(g, h)$ and $Q(g, h)$ are well-defined elements in $H$ since the infinite product becomes a finite one and all of the rational powers are well-defined.

**Theorem 1.4.26.** *Let $G$ be a Lazard group. Then the operations*

$$g + h = P(g, h),$$
$$[g, h]s = Q(g, h),$$

*make $G$ into a Lie ring and the $G_i$ form a filtration on this Lie ring. We denote this Lazard Lie ring by $\mathbf{Laz}^{-1}(G)$.*

**Theorem 1.4.27** (Lazard correspondence)**.** *The constructions* $\mathbf{Laz}$ *and* $\mathbf{Laz}^{-1}$ *are functorial and mutually inverse, therefore yielding an isomorphism between the categories of Lazard Lie rings and Lazard groups.*

**Lemma 1.4.28.** *Let* $(M,+)$ *be an abelian group and* $\mathcal{P}$ *a set of primes. Then* $G$ *is* $\mathcal{P}$*-divisible if and only if* $G$ *can be given the structure of a* $\mathbb{Q}_{\mathcal{P}}$*-module.*

**Corollary 1.4.29.** *Let* $\mathfrak{a}$ *be a filtered Lie algebra over a field* $K$ *of characteristic* $0$*. Then* $\mathfrak{a}$ *is Lazard if and only if the filtration is finite.*

**Lemma 1.4.30.** *Let* $(M,+)$ *be an abelian Lazard group. Then also the filtered ring* $\mathrm{End}_f(M)$ *is Lazard.*

*Proof.* Let $f \in \mathrm{End}_f(M)_i$. Since then $f(M) \subseteq M_{i+1}$ we can define for all $r \in \mathbb{Q}_{\mathcal{P}_i}$ the endomorphism

$$r\delta : \mathfrak{g} \to \mathfrak{g} : x \mapsto r\delta(x),$$

which is also contained in $\mathrm{End}_f(M)_i$. This gives $\mathrm{End}_f(M)_i$ the structure of a $\mathbb{Q}_{\mathcal{P}_i}$-module, hence the result follows from Lemma 1.4.28. □

Note that for an element $x$ of a Lazard Lie algebra $\mathfrak{g}$, the adjoint map

$$\mathrm{ad}_x : \mathfrak{g} \to \mathfrak{g} : y \mapsto [x,y],$$

is contained in $\mathrm{End}_f(\mathfrak{g},+)_1$. Here, $\mathrm{End}_f(\mathfrak{g},+)$ is as in Example 1.4.8, where we consider $\mathfrak{g}$ simply as a filtered abelian group. By Lemma 1.4.30 we find that $\exp(\mathrm{ad}_x)$ is well-defined in $\mathrm{End}_f(\mathfrak{g})$. The following lemma relates conjugation in $\mathbf{Laz}(\mathfrak{g},+)$ to the Lie bracket in $\mathfrak{g}$.

**Lemma 1.4.31.** *Let* $\mathfrak{g}$ *be a Lazard Lie algebra. Then*

$$\mathrm{BCH}(x, \mathrm{BCH}(y,-x)) = \exp(\mathrm{ad}_x)(y),$$

*for all* $x, y \in \mathfrak{g}$*.*

**Lemma 1.4.32.** *Let* $G$ *be a* $p$*-group for some prime* $p$ *and let* $\mathcal{P}$ *be a set of prime numbers. Then* $G$ *is* $\mathcal{P}$*-divisible if and only if* $p \notin \mathcal{P}$*.*

*Proof.* Let $g \in G$ and let $n \in \mathbb{Z}$ be coprime to $p$. Since $|g|$, the order of $g$, is a power of $p$, there exist some $r, s \in \mathbb{Z}$ such that $rn + s|g| = 1$. It follows that $(g^r)^n = g^{rn+s|g|} = g$, hence $g$ has an $n$-th root. Moreover, if $h \in G$ is such that $h^n = g$, then $|h| = |g|$ hence $g^r = (h^n)^r = h^{rn+s|g|} = h$ which proves the uniqueness. □

As a direct consequence of Lemma 1.4.28 we obtain a concrete characterization of Lazard $p$-groups and thus a specific case of the Lazard correspondence for groups and Lie rings of prime power cardinality.

**Proposition 1.4.33.** *Let* $p$ *be a prime and let* $G$ *be a filtered* $p$*-group. Then* $G$ *is Lazard if and only if* $G_p = \{1\}$*.*

**Theorem 1.4.34.** *Let* $p^n$ *be a prime power and* $k < p$*. The Lazard correspondence restricts to nilpotent Lie rings of order* $p^n$ *and nilpotency class* $k$*, and groups of order* $p^n$ *and nilpotency class* $k$*, where we consider all structures with the filtration coming from their lower central series.*

**Corollary 1.4.35.** *Let* $p$ *be a prime and* $n < p$*. The Lazard correspondence restricts to nilpotent Lie rings of order* $p^n$ *and groups of order* $p^n$*, where we consider all structures with the filtration coming from their lower central series.*

**Example 1.4.36.** Let $p > 2$ be a prime. Recall that the *Heisenberg Lie algebra* over a field $K$ is the Lie algebra on the vector space $K^3$ with Lie bracket

$$\left[\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix}\right] = \begin{pmatrix} 0 \\ 0 \\ x_1y_2 - y_1x_2 \end{pmatrix}.$$

When the characteristic of $K$ is not 2, then $\mathfrak{a}$ is a Lazard Lie algebra for the filtration coming from its lower central series. The group $\mathbf{Laz}(\mathfrak{a})$ is the *Heisenberg group* whose multiplication is given by

$$\mathrm{BCH}\left(\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix}\right) = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ z_1 + z_2 + \frac{1}{2}(x_1y_2 - y_1x_2) \end{pmatrix}.$$

If $K = \mathbb{F}_p$ for $p > 2$, then the obtained group is the *extraspecial group* of order $p^3$ and exponent $p$.

**Example 1.4.37.** Let $p$ be a prime. Then $\mathfrak{a} = \mathbb{Z}/p \times \mathbb{Z}/p^2$ with Lie bracket

$$\left[\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}\right] = \begin{pmatrix} 0 \\ p(x_1y_2 - y_1x_2) \end{pmatrix},$$

is a nilpotent Lie ring of class 2. Therefore, for $p > 2$ we find that $\mathfrak{a}$ is Lazard for the filtration coming from its lower central series. We find that the group operation in $\mathbf{Laz}(\mathfrak{a})$ is given by

$$\mathrm{BCH}\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}\right) = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + \frac{1}{2}p(x_1y_2 - y_1x_2) \end{pmatrix},$$

which is easily seen to be the unique extraspecial group of order $p^3$ and exponent $p^2$. We therefore say that $\mathfrak{a}$ is the *extraspecial Lie ring* of order $p^3$ and characteristic $p^2$.

As a particular case of the Lazard correspondence, we obtain the Malcev correspondence, proved prior to the Lazard correspondence in [119]. A group is $\mathbb{Q}$*-powered* if it is $\mathcal{P}$-divisible, where $\mathcal{P}$ is the set of all primes.

**Theorem 1.4.38** (Malcev correspondence)**.** *The Lazard correspondence restricts to a correspondence between nilpotent rational Lie algebras and nilpotent $\mathbb{Q}$-powered groups, where we consider all structures with the filtration coming from their lower central series.*

Let $\mathfrak{g}$ be a finite dimensional nilpotent Lie algebra over $\mathbb{R}$, which we equip with the filtration given by its lower central series. Since in particular $\mathfrak{g}$ is a finite dimensional vector space, it has a natural differential manifold structure, and the map $\mathrm{BCH} : \mathfrak{g}^2 \to \mathfrak{g}$ is polynomial, hence smooth, with respect to this manifold structure. Therefore, $\mathbf{Laz}(\mathfrak{g})$ is a Lie group. Since it is homeomorphic to a vector space, it is connected and simply connected.

**Proposition 1.4.39.** *Let $\mathfrak{g}$ be a nilpotent finite dimensional Lie algebra over $\mathbb{R}$. Then $\mathbf{Laz}(\mathfrak{g})$ is a connected, simply connected Lie group such that its associated Lie algebra is isomorphic to $\mathfrak{g}$ in such a way that $\mathfrak{g} \to \mathbf{Laz}(\mathfrak{g})$ is the Lie theoretic exponential map.*

*Proof.* Let $\mathcal{U}(\mathfrak{g})$ be the universal enveloping algebra of $\mathfrak{g}$, with its filtration as in Example 1.4.12 and let $A = \mathcal{U}(\mathfrak{g})/\mathcal{U}(\mathfrak{g})_{n+1}$ where $n$ is the dimension of $\mathfrak{g}$. Note that $A$ has finite dimension, bounded above by $1 + n + n^2 + \ldots + n^n$. Since $\mathfrak{g}_n = \{0\}$, we find that the canonical map

$$\iota : \mathfrak{g} \to A : x \mapsto x + \mathcal{U}(\mathfrak{g})_{n+1},$$

is injective and $\iota([x,y]) = \iota(x)\iota(y) - \iota(y)\iota(x)$. In particular, it follows from Proposition 1.4.24 that $\mathbf{Laz}(\mathfrak{g})$ is isomorphic to $\exp(\iota(\mathfrak{g}))$. Since $A$ is finite dimensional we can see it as a matrix ring and thus the statement now follows directly from classical Lie theory. □

At last, let us formulate the Lazard correspondence in its general form as it was stated in [112]. Let $\mathfrak{g}$ be a complete filtered Lie ring such that $\mathfrak{g}/\mathfrak{g}_i$ is Lazard for all $i \geq 1$ and identify $\mathfrak{g}$ with

$$\varprojlim \mathfrak{g}/\mathfrak{g}_i = \{(x_i + \mathfrak{g}_i)_{i\geq 1} \mid x_{i+1} + \mathfrak{g}_i = x_i + \mathfrak{g}_i \text{ for all } i \geq 1\}.$$

Then for $(x_i + \mathfrak{g}_i)_{i\geq 1}, (y_i + \mathfrak{g}_i)_{i\geq 1} \in \mathfrak{g}$ we define

$$\mathrm{BCH}((x_i + \mathfrak{g}_i)_{i\geq 1}, (y_i + \mathfrak{g}_i)_{i\geq 1}) = (\mathrm{BCH}(x_i, y_i) + \mathfrak{g}_i)_{i\geq 1},$$

and this makes $\mathfrak{g}$ together with operation BCH into a filtered group for the filtration given by the $\mathfrak{g}_i$. We denote this group by $\mathbf{Laz}(\mathfrak{g})$, which is justified since if $\mathfrak{g}$ is Lazard then it coincides with the earlier construction. The newly obtained filtered group $\mathbf{Laz}(\mathfrak{g})$ is complete and $\mathbf{Laz}(\mathfrak{g})/\mathfrak{g}_i = \mathbf{Laz}(\mathfrak{g}/\mathfrak{g}_i)$. Similarly, if $G$ is a complete filtered group such that $G/G_i$ is Lazard for all $i \geq 1$, then we can define a Lie ring structure $\mathbf{Laz}^{-1}(G)$ on the set $G$ such that $\mathbf{Laz}^{-1}(G) \cong \varprojlim \mathbf{Laz}^{-1}(G/G_i)$.

**Theorem 1.4.40.** *The constructions* $\mathbf{Laz}$ *and* $\mathbf{Laz}^{-1}$ *provide a functorial bijective correspondence between complete filtered Lie rings* $\mathfrak{g}$ *such that* $\mathfrak{g}/\mathfrak{g}_i$ *is Lazard for all* $i \geq 1$*, and complete filtered groups* $G$ *such that* $G/G_i$ *is Lazard for all* $i \geq 1$*.*

# 1.5 Hopf theory

In this last preliminary section, we discuss Hopf–Galois structures. These were initially introduced in the context of purely inseparable extensions by Chase and Sweedler [56], but after that they were mainly studied for separable extensions, providing a generalization of classical Galois theory. Our main interest lies in Galois field extensions, for which Greither and Pareigis proved a strong characterization in group theoretic terms. In order to formulate their result, we need the theory of Galois descent.

We will not give the definition of a Hopf algebra; instead, we refer the reader to a standard reference, for example [95]. Our notation will be standard: the maps $\Delta, \epsilon, \eta$ and $S$ denote the comultiplication, counit, unit and antipode respectively. For the comultiplication, we use Sweedler notation. All of the field extensions in this section are assumed to be finite.

## 1.5.1 Hopf–Galois structures

Let $K$ be a field and $H$ a $K$-Hopf algebra. A *$H$-module algebra* is a $K$-algebra $A$ which is moreover a module of the algebra $H$, whose action we usually denote byw $\star$, such that

$$h \star 1_A = \epsilon(h)1_A, \quad h \star (ab) = (h_1 \star a)(h_2 \star b),$$

are satisfied for all $a, b \in A$, $h \in H$.

**Example 1.5.1.** Let $H$ be a Hopf algebra and let $A$ be an $H$-module algebra. Recall that $g \in H$ is *grouplike* if $\Delta(g) = g \otimes g$. In that case, we find $g \star 1_A = 1_A$ and $g \star (ab) = (g \star a)(g \star b)$ for all $a, b \in A$. We conclude that grouplike elements of $H$ act by algebra automorphisms. In particular, if we consider a group algebra $K[G]$ with its canonical Hopf algebra structure, then a $K[G]$-module algebra $A$ is the same as an algebra $A$ together with an action of $G$ on $A$ by algebra automorphisms.

**Example 1.5.2.** Let $H$ be a Hopf algebra and let $A$ be an $H$-module algebra. Recall that $x \in H$ is *primitive* if $\Delta(g) = x \otimes 1 + 1 \otimes x$. In that case, $x \star 1_A = 0$ and $x \star (ab) = (x \star a)b + a(x \star b)$, meaning that $x$ acts by algebra derivations. In particular, if we consider the universal enveloping algebra $\mathcal{U}(\mathfrak{g})$ of a Lie algebra with its canonical Hopf algebra structure, then a $\mathcal{U}(\mathfrak{g})$-module algebra $A$ is the same as an algebra $A$ and a representation of $\mathfrak{g}$ on $A$ by algebra derivations.

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

$$L \otimes_K H \to \mathrm{End}_K(L), \quad x \otimes h \mapsto (y \mapsto x(h \star y)) \tag{1.18}$$

is bijective. Let there be given two Hopf–Galois structures on $L/K$, with Hopf algebras $H$ and $H'$. Then we consider these structures as equal if there exists an isomorphism between $H$ and $H'$ such that their action on $L$ respects this isomorphism. For more insights on the definition, we refer to [58].

**Example 1.5.3.** Assume that $L/K$ is Galois with Galois group $G$. Then we have a canonical $K[G]$-module algebra structure on $L$ coming from the action of $G$ on $L$. Then the map (1.18) is bijective since $G$ is an $L$-basis of $\mathrm{End}_K(L)$. We call this the *classical structure*.

**Example 1.5.4.** The following example is given in [82]. Consider the field extension $\mathbb{Q}(\omega)/\mathbb{Q}$ with $\omega = \sqrt[3]{2}$. This extension is separable but not normal. Define $\mathbb{Q}$-linear maps $s, c : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega)$ by:

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

Then $x \in \mathbb{Q}(\omega)$ is in $\mathbb{Q}$ if and only if $c(x) = x$ and $s(x) = 0$. The maps $c$ and $s$ are not automorphisms of $\mathbb{Q}(\omega)$ but satisfy $c(xy) = c(x)c(y) - 3s(x)s(y)$ and $s(xy) = c(x)s(y) + s(x)c(y)$ for all $x, y \in \mathbb{Q}(\omega)$. We claim that $\mathrm{id}_{\mathbb{Q}(\omega)}, c, s$ are linearly independent over $\mathbb{Q}(\omega)$. Indeed, let $x_1, x_2, x_3 \in \mathbb{Q}(\omega)$ be such that $x_1 \,\mathrm{id}_{\mathbb{Q}(\omega)} + x_2 c + x_3 s = 0$. Evaluating this expression in 1 yields $x_1 + x_2 = 0$, evaluating in $\omega$ yields $\frac{1}{2}(2x_1 - x_2 + x_3)\omega = 0$ and evaluating in $\omega^2$ we find $\frac{1}{2}(2x_1 - x_2 - x_3)\omega^2 = 0$. From the second and third equations we get $x_3 = 0$, this then implies that $2x_1 - x_2 = 0$, which, together with the first equation, then implies that $x_1 = x_2 = 0$.

One verifies that

$$H = \mathbb{Q}[c, s]/(3s^2 + c^2 - 1, (2c + 1)s, (2c + 1)(c - 1)),$$

with

$$\Delta(c) = c \otimes c - 3s \otimes s, \quad \Delta(s) = c \otimes s + s \otimes c, \quad \epsilon(c) = 1, \quad \epsilon(s) = 0,$$

defines a $\mathbb{Q}$-Hopf algebra with an action $\mathbb{Q}(\omega)$ which makes into a $H$-module algebra. Since the maps $\mathrm{id}_{\mathbb{Q}(\omega)}, c, s$ are $L$-linearly independent, we obtain a Hopf–Galois structure on $\mathbb{Q}(\omega)/\mathbb{Q}$.

Following [56], given a Hopf–Galois structure on $L/K$ with $K$-Hopf algebra $H$, we can attach to each $K$-sub Hopf algebra $H'$ of $H$ an intermediate field $F$ of $L/K$, as follows:

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

We obtain in this way the *Hopf–Galois correspondence*, which is always injective. We remark that the $F$-Hopf algebra $F \otimes_K H'$ acts on $L$ naturally and gives a Hopf–Galois structure on $L/F$, and in particular, $[L : F]$ equals the dimension of $H'$ as $K$-vector space; see also [63, section 7] for more details.

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

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

If $H'$ is a normal $K$-sub Hopf algebra of $H$, then by [122, Lemma 3.4.2 and Proposition 3.4.3] there exists a short exact sequence

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

of $K$-Hopf algebras, in the sense of [7, Proposition 1.2.3]. Moreover, if $F = L^{H'}$, then the action of $H$ on $L$ yields an action of $\overline{H}$ on $F$ which gives a Hopf–Galois structure on $F/K$; see [35, Lemma 4.1].

### 1.5.2 Galois Descent

We give only a brief summary of Galois descent and refer the interested reader to [58, section 2.12] for a more extensive treatment of the subject. Suppose that $L/K$ is Galois with Galois group $G$. An action $\star$ of $G$ on an $L$-vector space $V$ is *$L$-semilinear* if

$$\sigma \star (xv) = \sigma(x)(\sigma \star v),$$

for all $\sigma \in G$, $x \in L$ and $v \in V$. Given an $L$-Hopf algebra $M$ on which $G$ acts semilinearly, we say that $M$ is *$G$-compatible* if all the maps defining the structure of $M$ as an $L$-Hopf algebra are $G$-equivariant. Here $G$ acts on $L$ via the Galois action and on $M \otimes_L M$ diagonally.

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

- If $H \in \mathbf{Hopf}_K$, then $L \otimes_K H \in \mathbf{Hopf}_L^G$, where $G$ acts on the first factor of the tensor product; given a morphism $\varphi\colon H_1 \to H_2$ in $\mathbf{Hopf}_K$, we have that $\mathrm{id} \otimes \varphi\colon L \otimes_K H_1 \to L \otimes_K H_2$ is a morphism in $\mathbf{Hopf}_L^G$.
- If $M \in \mathbf{Hopf}_L^G$, then

  $$M^G = \{m \in M \mid m \text{ is fixed under the action of } G\},$$

  is $K$-Hopf algebra. Given a morphism $\psi\colon M_1 \to M_2$ in $\mathbf{Hopf}_L^G$, the restriction of $\psi$ to $M_1^G$ is a morphism $M_1^G \to M_2^G$.
- If $H \in \mathbf{Hopf}_K$, then

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

  is an isomorphism in $\mathbf{Hopf}_K$, and if $M \in \mathbf{Hopf}_L^G$, then

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

  is an isomorphism in $\mathbf{Hopf}_L^G$.

We immediately derive some consequences:

- Let $M \in \mathbf{Hopf}_L^G$. Then there exists a bijective correspondence between $K$-Hopf subalgebra of $M^G$ and $L$-Hopf subalgebra of $M$ that are invariant under the action of $G$ on $M$. Explicitly, given such an $L$-sub Hopf algebra $M'$, the corresponding $K$-sub Hopf algebra is $(M')^G$, and $M'$ is normal in $M$ if and only if $(M')^G$ is normal in $M^G$.
- Let
$$L \to A \to M \to B \to L$$
be a short exact sequence of $L$-Hopf algebras. If all the $L$-Hopf algebras are $G$-compatible and all the $L$-Hopf algebra homomorphisms are $G$-equivariant, then
$$K \to A^G \to M^G \to B^G \to K$$
is a short exact sequence of $K$-Hopf algebras.
- For all $M_1, M_2 \in \mathbf{Hopf}_L^G$, we have that $(M_1 \otimes_L M_2)^G$ and $M_1^G \otimes_K M_2^G$ are isomorphic as $K$-Hopf algebras.
- Let $M \in \mathbf{Hopf}_L^G$, and take $h \in M^G$. Then $h$ is a grouplike element of $M^G$ if and only if $h$ is a grouplike element of $M$.

**Example 1.5.5.** As before, let $L/K$ be a Galois field extension with Galois group $G$. Let $N$ be a finite group on which $G$ acts via automorphisms, and extend this to an action of $G$ on $L[N]$, where $G$ acts on $L$ via the Galois action. Then $L[N]$ is a $G$-compatible $L$-Hopf algebra. Here the $L$-Hopf subalgebras of $L[N]$ are the group algebras $L[N']$ for subgroups $N'$ of $N$ (see [67, Proposition 2.1]), and almost by definition, $L[N']$ is normal in $L[N]$ if and only if $N'$ is normal in $N$. We deduce that the $K$-Hopf subalgebras of $L[N]^G$ are of the form $L[N']^G$ for subgroups $N'$ of $N$ invariant under the action of $G$, and $L[N']^G$ is normal in $L[N]^G$ if and only if $N'$ is normal in $N$. Note that moreover, the lattices of $K$-Hopf subalgebra of $L[N]^G$ and subgroups of $N$ invariant under the action of $G$ are isomorphic.

If $N'$ is a normal subgroup of $N$ invariant under the action of $G$, then, by [58, Proposition 4.14],
$$L \to L[N'] \to L[N] \to L[N/N'] \to L,$$
is a short exact sequence of $L$-Hopf algebras which are $G$-compatible, where all the $L$-Hopf algebra homomorphisms are $G$-equivariant, so
$$K \to L[N']^G \to L[N]^G \to L[N/N']^G \to K,$$
is a short exact sequence of $K$-Hopf algebras.

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

### 1.5.3 Greither–Pareigis theory

Let $L/K$ be a separable field extension and let $\tilde{L}$ be the normal closure of $L/K$. Also, let $G = \mathrm{Aut}(\tilde{L}/K)$ and $G' = \mathrm{Aut}(\tilde{L}/L)$. For $\sigma \in G$, we let $\mathcal{L}_\sigma \in \mathbb{S}_{G/G'}$ denote the left regular permutation $\tau G' \mapsto \sigma\tau G'$. Since the kernel of the induced action of $G$ on $G/G'$ is the normal core of $G'$ (which is trivial since $\tilde{L}$ is the normal closure of $L/K$), we find that this induces an embedding $\mathcal{L} : G \to \mathbb{S}_{G/G'}$

**Theorem 1.5.6** ([82, Theorem 2.1])**.** *Let $L/K$ be a separable field extension. With the notation as above, there exists a bijective correspondence between:*

1. *Hopf–Galois structures on $L/K$.*
2. *Regular subgroups of $\mathbb{S}_{G/G'}$ normalized by $\mathcal{L}(G)$.*

*The* type *of a Hopf–Galois structure is defined as the isomorphism class of the corresponding regular subgroup of $\mathbb{S}_{G/G'}$.*

If $L/K$ is Galois, then $\tilde{L} = L$ and $G' = \{\mathrm{id}\}$, so the above theorem specializes to a bijective correspondence between Hopf–Galois structures on $L/K$ and regular subgroups of $\mathbb{S}_G$ normalized by $\mathcal{L}(G)$. Let us explicitly describe one direction of this correspondence in this setting.

Let $N$ be a regular subgroup of $\mathbb{S}_G$ normalized by $\mathcal{L}(G)$. In order to obtain its associated Hopf–Galois structure, we first consider the $L$-Hopf algebra $L[N]$, where $G$ acts on $L$ via the Galois action and on $N$ via conjugation by $\mathcal{L}(G)$. Recall that this is precisely the setting that appeared in Example 1.5.5. Then via Galois descent take the $K$-Hopf algebra $L[N]^G$, which gives a Hopf–Galois structure on $L/K$ with the following action on $L$:

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

**Example 1.5.7.** Let $L/K$ be a Galois and for $\sigma \in G$ let $\mathcal{R}_\sigma \in \mathbb{S}_G$ denote the right translation by $g$. The resulting subgroup $\mathcal{R}(G)$ of $\mathbb{S}_G$ clearly is regular and centralizes, thus normalizes, the subgroup $\mathcal{L}(G)$. Since the conjugation action of $\mathcal{L}(G)$ on $\mathcal{R}(G)$ is trivial, $G$ acts on $L[\mathcal{R}(G)]$ by

$$\tau \cdot \left(\sum_{\sigma\in G} \ell_\sigma \mathcal{R}_\sigma\right) = \sum_{\sigma\in G} \tau(\ell_\sigma)\mathcal{R}_\sigma.$$

As a result, we find that the $K$-Hopf algebra $H = L[\mathcal{R}(G)]^G = K[\mathcal{R}(G)]$ is the group $K$-Hopf algebra on $\mathcal{R}(G)$ and its action is given by

$$\left(\sum_{\sigma\in G} \ell_\sigma \mathcal{R}_\sigma\right) \star x = \sum_{\sigma\in G} \ell_\sigma(\mathcal{R}_\sigma^{-1}(1))(x) = \sum_{\sigma\in G} \ell_g \sigma^{-1}(x).$$

After identifying $K[G]$ with $K[\mathcal{R}(G)]$ through the $K$-algebra isomorphism

$$\sum_{\sigma\in G} \ell_\sigma \sigma \mapsto \sum_{\sigma\in G} \ell_\sigma \mathcal{R}_{\sigma^{-1}},$$

we recover the classical Hopf–Galois structure as described in Example 1.5.3.

**Example 1.5.8.** Let $L/K$ be a Galois field extension. Since $\mathcal{L}(G)$ normalizes itself, we can construct its associated Hopf–Galois structure. First of all, the action of $G$ on $L[\mathcal{L}(G)]$ is given by

$$\tau \cdot \left(\sum_{\sigma\in G} \ell_\sigma \mathcal{L}_\sigma\right) = \sum_{\sigma\in G} \tau(\ell_\sigma)\mathcal{L}_{\tau\sigma\tau^{-1}}.$$

As a result, we find that the $K$-Hopf algebra $H = L[\mathcal{L}(G)]^G$ consist of all $\sum_{\sigma\in G} \ell_\sigma \mathcal{L}_\sigma \in L[\mathcal{R}(G)]$ such that $\tau(\ell_\sigma) = \ell_{\tau\sigma\tau^{-1}}$ for all $\tau \in G$. The action of $H$ on $L/K$ is given by

$$\left(\sum_{\sigma\in G} \ell_\sigma \mathcal{L}_\sigma\right) \star x = \sum_{\sigma\in G} \ell_\sigma(\mathcal{L}_\sigma^{-1}(1))(x) = \sum_{\sigma\in G} \ell_g \sigma^{-1}(x).$$

After identifying $K[G]$ with $K[\mathcal{L}(G)]$ through the $K$-algebra isomorphism

$$\sum_{\sigma\in G} \ell_\sigma \sigma \mapsto \sum_{\sigma\in G} \ell_\sigma \mathcal{L}_\sigma,$$

we obtain the *canonical non-classical Hopf–Galois structure*.

We now go back to the setting where $L/K$ is separable but not necessarily Galois. Let $N$ be a regular subgroup of $\mathbb{S}_{G/G'}$ normalized by $\mathcal{L}(G)$. Since $N$ acts regularly, the map

$$N \to G/G' : \eta \mapsto \eta(G'),$$

is a bijection, which we can use to identify the groups $\mathbb{S}_N$ and $\mathbb{S}_{G/G'}$. Explicitly, the subgroup $N$ of $\mathbb{S}_{G/G'}$ then corresponds to the subgroup of left translations $\mathcal{L}(N) \subseteq \mathbb{S}_N$. Since $\mathcal{L}(G)$ normalizes $N$, we find that the corresponding subgroup in $\mathbb{S}_N$ normalizes $\mathcal{L}(N)$. The normalizer of $\mathcal{L}(N)$ in $\mathbb{S}_N$ is precisely $\mathrm{Hol}(N)$. We recover [57, Proposition 1].

**Proposition 1.5.9.** *Let $N$ be a regular subgroup of $\mathbb{S}_{G/G'}$ and identify $N$ with $G/G'$ through the bijection*

$$N \to G/G' : \eta \mapsto \eta(G').$$

*Then $N$ normalizes $\mathcal{L}(G)$ if and only if $\mathcal{L}(G)$ is a subgroup of $\mathrm{Hol}(N)$.*

In particular, questions like "Does there exist a Hopf–Galois structure of type $N$ on a separable extension $L/K$?" get reduced to "Can one embed $G$ into $\mathrm{Hol}(N)$ such that $G'$ is the stabilizer of $1$?"

# Chapter 2

# Bi-skew braces and brace blocks

Motivated by the connection between skew braces and Hopf–Galois theory, Childs introduced bi-skew braces in [61]. Caranti subsequently studied different characterizations of bi-skew braces and gave various constructions in [41]. These characterizations were formulated both using gamma functions and from the point of view of regular subgroups of the holomorph. Bi-skew braces were further studied by Koch in [100], where a construction for bi-skew braces is given starting from group endomorphisms with abelian image. An iterative version of this construction was then obtained in [101], where the notion of a brace block also appears for the first time. The constructions by Koch and a construction of Caranti [40] were subsequently generalized by Caranti and Stefanello in [42, 43]. In [19], Bardakov, Neshchadim and Yadav give an iterative construction to obtain a brace block from a given bi-skew brace satisfying a certain property.

The main objective of this chapter is to obtain a better theoretical understanding of bi-skew braces, $\lambda$-homomorphic skew braces and brace blocks. We subsequently use this to construct new families of examples and to solve a classification problem proposed by Vendramin [164].

This chapter is organized as follows. In Section 2.1 we state several structural results of bi-skew braces. We relate structural properties of a bi-skew brace to those of its associated skew brace with swapped operations and also to properties of a suitable group associated with the skew brace. In Section 2.2, we state a characterization of $\lambda$-homomorphic skew braces. This characterization bears a strong resemblance to a characterization of bi-skew braces by Caranti. This resemblance is further emphasized when we discuss two slightly different constructions. One yields a new construction of $\lambda$-homomorphic skew braces and the other is a new way to obtain examples of bi-skew braces described by Childs. Section 2.3 contains two classification results. We first prove an upper bound on the nilpotency class of braces whose multiplicative group is isomorphic to $\mathbb{Z}^n$. In particular, we recover the known result that such a brace is trivial if $n = 1$ and the new result that it is a bi-skew brace if $n = 2$. Secondly, in Theorem 2.3.6 we use bi-skew braces to solve an open problem posed by Vendramin concerning the classification of skew braces with a multiplicative group isomorphic to $\mathbb{Z}$. At last, in Section 2.4 we investigate brace blocks. We start with a general characterization of brace blocks on a given group in Theorem 2.4.1. It is only when we add an extra condition that we obtain a more manageable characterization in Theorem 2.4.5, from which we then construct new brace blocks. Nonetheless, we illustrate that this more restrictive characterization still covers all known constructions of brace blocks in the literature. Moreover, from Theorem 2.4.5 we obtain brace blocks starting from abelian groups, a case where most known constructions only yield trivial examples. We further give two new concrete constructions of brace blocks using rings and semidirect products.

All results in this chapter for which no external reference is given were obtained in collaboration with

Lorenzo Stefanello and have been published in [154].

## 2.1 Bi-skew braces

Recall that for a bi-skew brace $(A, \cdot, \circ)$, we use the notation $A_\leftrightarrow = (A, \circ, \cdot)$. The $\lambda$-maps associated to $A_\leftrightarrow$ are denoted by $\lambda_a^\leftrightarrow$ and its $*$-operation by $*_\leftrightarrow$, so explicitly

$$\lambda_a^\leftrightarrow(b) = \overline{a} \circ (a \cdot b),$$

and

$$a *_\leftrightarrow b = \overline{a} \circ (a \cdot b) \circ \overline{b},$$

where $a, b \in A$. We start by relating the structure of a bi-skew brace $A$ with that of $A_\leftrightarrow$.

**Lemma 2.1.1.** *Let $A$ be a bi-skew brace. Then the (left) ideals of $A$ and $A_\leftrightarrow$ coincide.*

*Proof.* Let $I$ be a skew subbrace of $A$. As $\lambda_a^\leftrightarrow = \lambda_a^{-1} = \lambda_{\overline{a}}$, we have that $I$ is mapped to itself by $\lambda_a$ for all $a \in A$ if and only if $I$ is mapped to itself by $\lambda_a^\leftrightarrow$ for all $a \in A$. □

**Lemma 2.1.2.** *Let $A$ be a bi-skew brace, and let $I$ be a left ideal 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 left ideal of $A$. Take $a \in A$ and $b \in I$. We have

$$\begin{aligned} a * b &= \lambda_a(b) \cdot b^{-1} \\ &= (\lambda_a(b) \circ \overline{b} \circ b) \cdot b^{-1} \\ &= (\lambda_a(b) \circ \overline{b}) \cdot \lambda_{\lambda_a(b) \circ \overline{b}}(b) \cdot b^{-1} \\ &= (\overline{a} *_\leftrightarrow b) \cdot ((\overline{a} *_\leftrightarrow b) * b). \end{aligned} \tag{2.1}$$

Hence $\overline{a} *_\leftrightarrow b = (a * b) \cdot ((\overline{a} *_\leftrightarrow b) * b)^{-1} \in A * I$, and thus $A *_\leftrightarrow I \subseteq A * I$. By a symmetric argument and Lemma 2.1.1, we also obtain $A * I \subseteq A *_\leftrightarrow I$.

Suppose now that $I$ is an ideal. By (2.1) with $a \in I$ and $b \in A$ and Lemma 2.1.1, we get that $I *_\leftrightarrow A \subseteq I * A$. Therefore, the result follows by a symmetric argument. □

As a consequence, we derive the following propositions.

**Proposition 2.1.3.** *Let $A$ be a bi-skew brace. Then $A$ is solvable of class $n$ if and only if $A_\leftrightarrow$ is solvable of class $n$.*

**Proposition 2.1.4.** *Let $A$ be a bi-skew brace. Then $A$ is left nilpotent, respectively right nilpotent, strongly nilpotent, of class $n$ if and only if $A_\leftrightarrow$ is left nilpotent, respectively right nilpotent, strongly nilpotent, of class $n$.*

We show now that we can check whether a bi-skew brace is right nilpotent or solvable just by looking at a suitable group. A prominent role is played by Theorem 1.1.34. Also, we freely use the fact that if $A$ is a bi-skew brace, then $\ker \lambda$ is an ideal of $A$. This follows directly from the proof of Theorem 1.1.34.

**Theorem 2.1.5.** *Let $A \neq \{1\}$ be a bi-skew brace. Then $A$ is right nilpotent of class $n+1$ if and only if $\lambda(A)$ is a nilpotent group of class $n$.*

*Proof.* Since $A$ is a bi-skew brace, we know that $\ker\lambda$ is an ideal. Because $A \neq \{1\}$, it is clear that $A$ is right nilpotent of class $n+1$ if and only if $A/\ker\lambda$ is right nilpotent of class $n$.

As $A^2_{\mathrm{op}} \subseteq \ker\lambda$, we know that $A/\ker\lambda$ is an almost trivial skew brace. In particular, $A/\ker\lambda$ is right nilpotent of class $n$ if and only if the group $(A/\ker\lambda, \circ)$ is nilpotent of class $n$. The group $(A/\ker\lambda, \circ)$ is clearly isomorphic to $\lambda(A)$. □

**Corollary 2.1.6.** *Let $A$ be a bi-skew brace such that $(A,\cdot)$ or $(A,\circ)$ is nilpotent. Then $A$ is right nilpotent.*

*Proof.* It suffices to note that $\lambda(A)$ is a quotient of both $(A,\cdot)$ and $(A,\circ)$, and then to apply Theorem 2.1.5. □

**Corollary 2.1.7.** *Let $A$ be a bi-skew brace. Then $A$ is left nilpotent if and only if $A$ is strongly nilpotent.*

*Proof.* By Theorem 1.1.30, it suffices to show that in this case left nilpotency implies right nilpotency. If $A$ is left nilpotent, then so is the skew brace $A/\ker\lambda$. But as $A/\ker\lambda$ is almost trivial, we find that this is equivalent to the group $(A/\ker\lambda, \circ) \cong \lambda(A)$ being nilpotent. The result then follows from Theorem 2.1.5. □

**Proposition 2.1.8.** *Let $A$ be a bi-skew brace. Then $A$ is a solvable skew brace if and only if $\lambda(A)$ is a solvable group.*

*Proof.* As $A$ is a bi-skew brace, $\ker\lambda$ is an ideal, trivial as a skew brace. Therefore, $A$ is solvable if and only if $A/\ker\lambda$ is solvable.

Now, as $A^2_{\mathrm{op}} \subseteq \ker\lambda$, we know that $A/\ker\lambda$ is an almost trivial skew brace. In particular, $A/\ker\lambda$ is solvable if and only if the group $(A/\ker\lambda, \circ)$ is solvable, and $(A/\ker\lambda, \circ)$ is clearly isomorphic to $\lambda(A)$. □

We conclude this section by proving that Byott's conjecture holds for bi-skew braces.

**Theorem 2.1.9.** *Let $A$ be a bi-skew brace. Then $(A,\cdot)$ is solvable if and only if $(A,\circ)$ is solvable. Moreover, in this case, $A$ is also solvable as a skew brace.*

*Proof.* Assume that $(A,\cdot)$ is solvable. As $A/A^2_{\mathrm{op}}$ is an almost trivial skew brace, its multiplicative and additive groups are isomorphic. In particular, it follows from the assumption that both are solvable. Since $A^2_{\mathrm{op}}$ is a trivial skew brace, clearly $(A^2_{\mathrm{op}},\cdot) \cong (A^2_{\mathrm{op}},\circ)$. It once again follows from the assumption that both groups are solvable. We conclude that $(A/A^2_{\mathrm{op}},\circ)$ and $(A^2_{\mathrm{op}},\circ)$ are solvable, so $(A,\circ)$ is also solvable. The exact same argument proves the other implication.

To prove that in this case $A$ is also solvable as a skew brace, it suffices to note that $\lambda(A)$ is a solvable group as it is a quotient of $(A,\circ)$. The solubility of $A$ then follows by Proposition 2.1.8. □

*Remark* 2.1.10. The same idea can be used to prove that Byott's conjecture holds for skew braces with a composition series where the factors are trivial or almost trivial skew braces, so in particular for solvable skew braces.

## 2.2 $\lambda$-homomorphic skew braces

We start with a theorem for $\lambda$-homomorphic skew braces similar to Theorem 1.1.34.

**Theorem 2.2.1.** *Let $A$ be a skew brace. Then the following are equivalent:*

1. *$A$ is $\lambda$-homomorphic.*
2. *$A^2$ is contained in* $\ker\lambda$.
3. *$A$ is right nilpotent of class at most* 2.

*Proof.* Assume that $A$ is $\lambda$-homomorphic. Then for all $a, b \in A$,

$$\lambda_{a*b} = \lambda_a^{-1}\lambda_a\lambda_b\lambda_b^{-1} = 1.$$

It follows that $A^2 \subseteq \ker\lambda$. Conversely, assume that $\ker\lambda$ contains $A^2$. As $A/A^2$ is a trivial skew brace it follows for all $a, b \in A$ that $(a \cdot b) \circ A^2 = (a \circ b) \circ A^2$. The assumption then implies

$$\lambda_{a\cdot b} = \lambda_{a\circ b} = \lambda_a\lambda_b.$$

The equivalence of the second and third condition follows directly since $A^2 * A = \{0\}$ if and only if $A^2$ is contained in $\ker\lambda$. □

Recall that a skew brace $A$ is *metatrivial* if it is solvable of class at most 2, which by definition means that $A^2$ is a trivial skew brace. As a consequence of Theorem 2.2.1, we find a short proof of [18, Theorem 2.12], as follows.

**Corollary 2.2.2.** *Every $\lambda$-homomorphic skew brace is metatrivial.*

*Proof.* Let $A$ be a $\lambda$-homomorphic skew brace. Then by Theorem 2.2.1, $A^{(3)} = \{1\}$, and this clearly implies that $A^2 * A^2 \subseteq A^2 * A = \{1\}$. □

Note that the converse does not hold.

**Example 2.2.3.** Let $A = \mathrm{opTriv}(\mathbb{S}_3)$, with $\mathbb{S}_3$ the symmetric group on 3 elements. Then $A$ is metatrivial because $\mathbb{S}_3$ is metabelian. As $\mathbb{S}_3$ is not nilpotent, it follows that $A$ is not right nilpotent and in particular not $\lambda$-homomorphic.

**Example 2.2.4.** Let $A$ be a Jacobson radical ring. By Theorem 1.1.34 (or equivalently, Theorem 2.2.1), we find that the corresponding two-sided brace is a bi-skew brace (or equivalently, a $\lambda$-homomorphic skew brace) if and only if $A^{(3)} = A^3 = \{1\}$, as already shown in [61, Proposition 4.1] when $A$ is finite or nilpotent.

We conclude the section by showing that one can use the semidirect product of skew braces to obtain two slightly different constructions, one yielding $\lambda$-homomorphic skew braces and one yielding bi-skew braces. For bi-skew braces, it turns out that we find a different construction for examples that were already described by Childs.

**Example 2.2.5.** Let $G$ and $H$ be groups, and let $H$ act by automorphisms on $G$, with the action denoted by $\alpha$. This induces an action of the trivial skew brace $B = \mathrm{Triv}(H)$ on the trivial skew brace $A = \mathrm{Triv}(G)$. By the semidirect product construction, we find a skew brace $A \rtimes B$. Explicitly,

$$(g, h) \cdot (g', h') = (gg', hh'),$$
$$(g, h) \circ (g', h') = (g\alpha_h(g'), hh').$$

We have recovered in this way [83, Example 1.4]. Note that here the $\lambda$-action is given by

$$\lambda_{(g,h)}(g', h') = (\alpha_h(g'), h').$$

In particular, $A \rtimes B$ is a $\lambda$-homomorphic skew brace, and it is a bi-skew brace if and only if the commutator subgroup $[H, H]$ is contained in the kernel of $\alpha$, as an immediate computation shows.

**Example 2.2.6.** Let $G$ and $H$ be groups, and let $H$ act by automorphisms on $G$, with the action denoted by $\alpha$. This induces an action of the almost trivial skew brace $B = \mathrm{opTriv}(H)$ on the trivial skew brace $A = \mathrm{Triv}(G)$. By the semidirect product construction, we find a skew brace $A \rtimes B$. Explicitly,

$$(g,h)\cdot(g',h') = (gg',hh'),$$
$$(g,h)\circ(g',h') = (g\alpha_h(g'),hh').$$

The $\lambda$-action of the skew brace $A \rtimes B$ is given by

$$\lambda_{(g,h)}(g',h') = (\alpha_h(g'),\phi_h(h')),$$

where $\phi_h$ denotes conjugation by $h$. This immediately implies that $A \rtimes B$ is a bi-skew brace, already obtained in [61, Proposition 7.1] from the semidirect product of the groups $G$ and $H$. Moreover it is $\lambda$-homomorphic if and only if $[H,H] \subseteq \ker\alpha \cap Z(H)$. Note that when $H$ is abelian, this construction coincides with the one in Example 2.2.5.

## 2.3 Skew braces with a free abelian multiplicative group

We begin this section by showing that all the braces with a multiplicative group isomorphic to $\mathbb{Z}^2$ are in fact bi-skew braces. We need the following result.

**Theorem 2.3.1.** *Let $(A,\cdot,\circ)$ be a two-sided brace such that $(A,\circ)$ is finitely generated abelian of rank $n$. Then $(A,\cdot)$ is finitely generated abelian of rank $n$.*

*Proof.* By [168, Theorem 3], if $(A,\circ)$ is finitely generated abelian, then $(A,\cdot)$ is finitely generated. By [4, Theorem B], the ranks of $(A,\circ)$ and $(A,\cdot)$ coincide. □

**Proposition 2.3.2.** *Let $A$ be a brace whose multiplicative group is isomorphic to $\mathbb{Z}^n$. Then $A$ is right nilpotent of class at most $n$.*

*Proof.* By Theorem 2.3.1, $(A,\cdot)$ is finitely generated of rank $n$. Let $T$ be the (necessarily finite) torsion subgroup of $(A,\cdot)$. As $T$ is a characteristic subgroup of $(A,\cdot)$, it is a left ideal of $A$, so also a finite subgroup of $(A,\circ)$, and thus $T$ is trivial. It follows that $(A,\cdot) \cong \mathbb{Z}^n$.

Now, for a prime $p$, let $I_p$ be the characteristic subgroup of $(A,\cdot)$ generated by all $p$-powers of elements. Then $A/I_p$ has order $p^n$, and therefore it is left nilpotent of class at most $n$ by Theorem 1.1.24. As $A/I_p$ is a two-sided brace, it is also right nilpotent of class at most $n$, or equivalently, $A^{(n+1)} \subseteq I_p$. We conclude that

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

We immediately recover [55, Theorem 5.5], and we find the result we have claimed.

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

**Corollary 2.3.4.** *Let $A$ be a brace with a multiplicative group isomorphic to $\mathbb{Z}^2$. Then $A$ is a bi-skew brace.*

*Proof.* It follows from Proposition 2.3.2 that $A$ is right nilpotent of degree at most 2. The statement then follows from Theorem 1.1.34 and the fact that $A_{\mathrm{op}} = A$. □

Motivated by Corollary 2.3.3, we now want to classify all the skew braces with a multiplicative group isomorphic to $\mathbb{Z}$, as asked in [164, Problem 2.27]. Let $(A, \cdot)$ be an infinite cyclic group with generator $x$. We can define the following operation on $A$:

$$x^i \circ x^j = x^{i+(-1)^i j}.$$

Then, as shown in the proof of [133, Proposition 6], the operation $\circ$ is the unique one such that $(A, \cdot, \circ)$ is a non-trivial brace, and $(A, \circ)$ is isomorphic to the infinite dihedral group

$$\langle x, y \mid y^2 = 1, yxy = x^{-1} \rangle \cong \mathbb{Z} \rtimes C_2.$$

Also, $(A, \cdot, \circ)$ is a bi-skew brace since

$$x^i * x^j = x^{-i} \cdot x^{i+(-1)^i j} \cdot x^{-j} = x^{((-1)^i - 1)j} \in \ker \lambda.$$

Moreover, there are just two group automorphisms of $(A, \cdot)$, namely the identity and the inversion, and they both are also automorphisms of the skew brace $(A, \cdot, \circ)$ and therefore also of $(A, \circ, \cdot)$. Indeed, for all $i, j \in \mathbb{Z}$ we have that

$$x^{-i} \circ x^{-j} = x^{-i+(-1)^{-i}(-j)} = x^{-(i+(-1)^i j)} = (x^i \circ x^j)^{-1}.$$

We claim that $(A, \circ, \cdot)$ is not isomorphic to its opposite skew brace. They are clearly not equal, as $(A, \circ)$ is not abelian. Therefore, the only candidate for an isomorphism is given by the inversion automorphism of $(A, \cdot)$, which also induces an automorphism of $(A, \circ)$. If this yields an isomorphism of skew braces, then it would be both an automorphism and an antiautomorphism of $(A, \circ)$, which implies that $(A, \circ)$ is abelian. As $(A, \circ)$ is isomorphic to the infinite dihedral group, this is a contradiction.

In the remainder of this section, we prove that the two non-isomorphic skew braces with infinite cyclic multiplicative group as described above are, in fact, the only non-trivial ones.

**Lemma 2.3.5.** *Let $A$ be a skew brace with an abelian multiplicative group. Then for all $X, Y \subseteq A$, the equality $X * Y = Y *_{\mathrm{op}} X$ holds.*

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

$$a * b = a^{-1} \cdot (a \circ b) \cdot b^{-1} = a^{-1} \cdot (b \circ a) \cdot b^{-1} = b *_{\mathrm{op}} a. \qquad \square$$

**Theorem 2.3.6.** *Let $(A, \circ) = \{x^{\circ i} \mid i \in \mathbb{Z}\}$ be an infinite cyclic group. If $A = (A, \cdot, \circ)$ is a skew brace, then the additive operation is given by one of the following equalities:*

$$x^{\circ i} \cdot x^{\circ j} = x^{\circ(i+j)}, \tag{2.2}$$

$$x^{\circ i} \cdot x^{\circ j} = x^{\circ(i+(-1)^i j)}, \tag{2.3}$$

$$x^{\circ i} \cdot x^{\circ j} = x^{\circ(j+(-1)^j i)}. \tag{2.4}$$

*Proof.* If $(A, \cdot)$ is abelian, then $\cdot$ is given by (2.2) by Corollary 2.3.3.

From now on, we assume that $(A, \cdot)$ is not abelian. As $A$ is a two-sided skew brace, it follows from [123, Lemma 4.5] that $(A^2, \cdot)$ is abelian. In particular, $A^2 \neq A$. Moreover, note that $A^2 \neq \{1\}$, otherwise $A$ would be trivial, so $(A, \cdot)$ would be abelian. We deduce that there exists $n \geq 2$ such that

$$A^2 = \{x^{\circ nk} \mid k \in \mathbb{Z}\}.$$

As $A^2$ is a brace with multiplicative group isomorphic to $\mathbb{Z}$, it follows from Corollary 2.3.3 that $A^2$ is a trivial skew brace. Because $(A/A^2, \circ) \cong C_n$, we find that $A/A^2 \cong \mathrm{Triv}(C_n)$.

Since $x$ generates $(A, \circ)$, its equivalence class in $A/A^2$ generates $(A/A^2, \circ)$, and therefore it also generates $(A/A^2, \cdot)$. If we take $a \in A^2$ to be a generator of $(A^2, \cdot)$, then $(A, \cdot)$ is generated by $a$ and $x$. Denote by $\psi$ the inner automorphism on $(A^2, \cdot)$ induced by $x$ in $(A, \cdot)$. As $(A, \cdot)$ is not abelian, $\psi$ is not trivial, so necessarily $\psi$ is the inversion automorphism. Likewise, $\lambda_x$ restricts to an automorphism of $(A^2, \cdot)$, which is either the identity or equals $\psi$.

1. If $\lambda_x$ is the identity on $A^2$, then using Lemma 2.3.5 we find $A^2 *_{\mathrm{op}} A = A * A^2 = \{1\}$, so $A_{\mathrm{op}}$ is a bi-skew brace. This means that $(A, \circ, \cdot_{\mathrm{op}})$ is a non-trivial skew brace, so the operation $\cdot$ is necessarily given by (2.4).

2. If $\lambda_x$ restricts to the inversion automorphism on $(A^2, \cdot)$, and therefore is equal to $\psi$ on $A^2$, then $\lambda_x^{\mathrm{op}}$ equals $\psi^2 = \mathrm{id}$ on $A^2$. Using Lemma 2.3.5 we find $A^2_{\mathrm{op}} * A = A *_{\mathrm{op}} A^2_{\mathrm{op}} = \{1\}$. So $(A, \circ, \cdot)$ is a non-trivial skew brace, which implies that $\cdot$ is given by (2.3). □

## 2.4 Brace blocks

In order to give a characterization of brace blocks, we begin with a result on the transitivity of bi-skew braces.

**Theorem 2.4.1.** *Let $(A, \cdot, \circ_1)$ and $(A, \cdot, \circ_2)$ be bi-skew braces with $\lambda$-maps $\lambda_1$ and $\lambda_2$, respectively. Then $(A, \circ_1, \circ_2)$ is a bi-skew brace if and only if the following conditions hold: for all $a, b \in A$ and $i, j \in \{1, 2\}$ with $i \neq j$,*

$$\lambda_{i,a}\lambda_{j,b}\lambda_{i,a}^{-1} = \lambda_{j,\lambda_{i,a}(b)}.$$

*Proof.* By symmetry, we can just look at when $(A, \circ_1, \circ_2)$ is a skew brace. As

$$a \circ_2 b = a \cdot \lambda_{2,a}(b) = a \circ_1 \lambda_{1,a}^{-1}\lambda_{2,a}(b),$$

we need to find under which conditions the map

$$\lambda : A \to \mathbb{S}_A : a \mapsto \lambda_a = \lambda_{1,a}^{-1}\lambda_{2,a},$$

satisfies the conditions of Lemma 1.1.10 on $(A, \circ_1)$.

The first condition to check is whether for all $a \in A$, we have $\lambda_a \in \mathrm{Aut}(A, \circ_1)$, or equivalently, $\lambda_{2,a} \in \mathrm{Aut}(A, \circ_1)$. Here we have

$$\lambda_{2,a}(b \circ_1 c) = \lambda_{2,a}(b \cdot \lambda_{1,b}(c)) = \lambda_{2,a}(b) \cdot \lambda_{2,a}\lambda_{1,b}(c),$$

and

$$\lambda_{2,a}(b) \circ_1 \lambda_{2,a}(c) = \lambda_{2,a}(b) \cdot \lambda_{1,\lambda_{2,a}(b)}\lambda_{2,a}(c).$$

We find that $\lambda_a \in \mathrm{Aut}(A, \circ_1)$ if and only if for all $a, b \in A$,

$$\lambda_{2,a}\lambda_{1,b}\lambda_{2,a}^{-1} = \lambda_{1,\lambda_{2,a}(b)}. \tag{2.5}$$

Now suppose that (2.5) holds. We claim that this is enough to deduce that $\lambda : (A, \circ_2) \to \mathrm{Aut}(A, \circ_1)$ is a group homomorphism. For all $a, b \in A$,

$$\begin{aligned}\lambda_{a\circ_2 b} &= \lambda^{-1}_{1,a\circ_2 b}\lambda_{2,a\circ_2 b}\\ &= \lambda^{-1}_{1,a\cdot\lambda_{2,a}(b)}\lambda_{2,a\circ_2 b}\\ &= \lambda^{-1}_{1,a}\lambda^{-1}_{1,\lambda_{2,a}(b)}\lambda_{2,a}\lambda_{2,b}\\ &= \lambda^{-1}_{1,a}\lambda_{2,a}\lambda^{-1}_{1,b}\lambda_{2,a}.\end{aligned}$$

□

**Definition 2.4.2.** Let $(A, \cdot)$ be a group. A *brace block on* $(A, \cdot)$ is a brace block $(A, \circ_i)_{i\in I}$ such that $(A, \circ_k) = (A, \cdot)$ for some $k \in I$.

We deduce the following characterization for brace blocks on a given group.

**Theorem 2.4.3.** *Let $(A, \cdot)$ be a group. Then the following data are equivalent:*

1. *A brace block on $(A, \cdot)$.*
2. *A family of maps $(\lambda_i)_{i\in I}$ such that the following conditions hold:*
   - *$\lambda_i : (A, \cdot) \to \mathrm{Aut}(A, \cdot)$ is an antihomomorphism for all $i \in I$.*
   - *There exists $k \in I$ such that $\lambda_{k,a} = \mathrm{id}$ for all $a \in A$.*
   - *For all $i, j \in I$ and $a, b \in A$,*
   $$\lambda_{i,a}\lambda_{j,b}\lambda^{-1}_{i,a} = \lambda_{j,\lambda_{i,a}(b)}.$$

*Proof.* For all $i \in I$, we find that $(A, \cdot, \circ_i)$ is a bi-skew brace because $\lambda_i$ is a group antihomomorphism and the last condition for $i = j$ implies that

$$\lambda_{i,a\cdot\lambda_{i,a}(b)} = \lambda_{i,a}\lambda_{i,b}.$$

Now apply Theorem 2.4.1. □

*Remark* 2.4.4. A similar condition was found in a particular case in [153, Theorem 4.30], where the problem of finding mutually normalizing regular subgroups in the holomorph of a cyclic group of prime order was dealt with. This problem is equivalent to looking for brace blocks; see [43, section 7] for more details.

Since the obtained characterization in Theorem 2.4.3 is quite technical, we propose a more restrictive but also more straightforward construction of brace blocks, which can already provide several examples.

**Theorem 2.4.5.** *Let $(A, \cdot)$ be a group, let $M$ be an abelian subgroup of $\mathrm{Aut}(A, \cdot)$, and let $\mathcal{S}$ be the set of group homomorphisms $\lambda : A \to M$ such that $\lambda_{\psi(a)} = \lambda_a$ for all $a \in A$ and $\psi \in M$. Then $(A, \circ_\lambda)_{\lambda\in\mathcal{S}}$ is a brace block, where*

$$a \circ_\lambda b = a \cdot \lambda_a(b).$$

*Moreover, $(A, \circ_{\lambda_1}, \circ_{\lambda_2})$ is $\lambda$-homomorphic for all $\lambda_1, \lambda_2 \in \mathcal{S}$.*

*Proof.* The first part is immediate from Theorem 2.4.3. To conclude the second part, recall that the $\lambda$-map $\lambda_{1,2}$ of $(A, \circ_{\lambda_1}, \circ_{\lambda_2})$ is given by $\lambda_{1,2,a} = \lambda^{-1}_{1,a}\lambda_{2,a}$. As $\lambda_{1,2}(A) \subseteq M$, so in particular it is abelian, we find that $(A, \circ_{\lambda_1}, \circ_{\lambda_2})$ is $\lambda$-homomorphic by Lemma 1.1.35. □

**Example 2.4.6.** Let $R$ be a ring. For each $x \in R$, define the following map:

$$\lambda_x : (R^2, +) \to \mathrm{Aut}(R^2, +) : \begin{pmatrix} r \\ s \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ xr & 1 \end{pmatrix},$$

where $R^2$ denotes the cartesian product $R \times R$. Then for all $x \in R$,

$$\lambda_x(R^2) \subseteq M = \left\{ \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} \mid y \in R \right\},$$

Since multiplication of two elements in $M$ is the same as adding the bottom left entries, we find that $M$ is isomorphic to $(R, +)$ and that $\lambda_x$ is a group homomorphism. Also, for all $x \in R$, $a \in R^2$, and $\psi \in M$, we have $\lambda_{x,\psi(a)} = \lambda_{x,a}$. We conclude that $(R^2, \circ_x)_{x \in R}$ is a brace block, where

$$\begin{pmatrix} r \\ s \end{pmatrix} \circ_x \begin{pmatrix} r' \\ s' \end{pmatrix} = \begin{pmatrix} r + r' \\ s + s' + xrr' \end{pmatrix}.$$

Moreover, all the operations are distinct, because for all $x \in R$,

$$\begin{pmatrix} r \\ s \end{pmatrix} \circ_x \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} r + 1 \\ s + xr \end{pmatrix}.$$

Assume that $R$ is commutative and that for all $r \in R$ there exists a unique $r' \in R$ such that $2r' = r^2 - r$ (by abuse of notation, we say $r' = \frac{r^2 - r}{2}$), which is for example the case if $R$ is $\mathbb{Z}$ or a ring of characteristic coprime to 2. In that case,

$$f : (R^2, +) \to (R^2, \circ_{\lambda_x}) : \begin{pmatrix} r \\ s \end{pmatrix} \mapsto \begin{pmatrix} r \\ s + \frac{x(r^2 - r)}{2} \end{pmatrix},$$

is a group homomorphism since for all $r, r', s, s' \in R$ we have that

$$\begin{aligned} f \begin{pmatrix} r + r' \\ s + s' \end{pmatrix} &= \begin{pmatrix} r + r' \\ s + s' + \frac{x((r+r')^2 - (r+r'))}{2} \end{pmatrix} \\ &= \begin{pmatrix} r + r' \\ s + s' + \frac{x(r^2 + 2rr' + (r')^2 - (r+r'))}{2} \end{pmatrix} \\ &= \begin{pmatrix} r \\ s + x\frac{r^2 - r}{2} \end{pmatrix} + \begin{pmatrix} r' \\ s' + \frac{x((r')^2 - r')}{2} + xrr' \end{pmatrix} \\ &= \begin{pmatrix} r \\ s + x\frac{r^2 - r}{2} \end{pmatrix} \circ_x \begin{pmatrix} r' \\ s' + \frac{x((r')^2 - r')}{2} \end{pmatrix} \\ &= f \begin{pmatrix} r \\ s \end{pmatrix} \circ_x f \begin{pmatrix} r' \\ s' \end{pmatrix}. \end{aligned}$$

**Example 2.4.7.** In the previous example, take $R = \mathbb{Z}$ and $x, y \in \mathbb{Z}$. If $x \neq \pm y$ then the braces $(\mathbb{Z}^2, +, \circ_x)$ and $(\mathbb{Z}^2, +, \circ_y)$ are non-isomorphic. Indeed,

$$\begin{pmatrix} r \\ s \end{pmatrix} * \begin{pmatrix} r' \\ s' \end{pmatrix} = \begin{pmatrix} 0 \\ xrr' \end{pmatrix}$$

and therefore $(\mathbb{Z}^2,+,\circ_x)/(\mathbb{Z}^2,+,\circ_x)^2 \cong \mathrm{Triv}(\mathbb{Z}\times C_{|x|})$. This nicely contrasts the case where the additive group is $\mathbb{Z}$, where only 2 distinct group operations $\circ$ giving a skew brace $(\mathbb{Z},+,\circ)$ are possible. One can show that the skew braces $(\mathbb{Z}^2,+,\circ_x)$ are isomorphic to the $\lambda$-cyclic skew braces with infinite cyclic image constructed in [18, Section 4].

**Example 2.4.8.** Let us reconsider Example 2.4.6 with $R$ a field of characteristic not 2. As explained above, we obtain a brace block $(R^2,\circ_x)_{x\in R}$, where $(R^2,+)\cong(R^2,\circ_x)$ for all $x\in R$. In this case all bi-skew braces of the form $(R^2,\circ_x,\circ_y)$, where $x,y\in R$ and $x\neq y$, are isomorphic. An explicit isomorphism of skew braces is given by

$$f:(R^2,+,\circ_{\lambda_1})\to(R^2,\circ_{\lambda_x},\circ_{\lambda_y}):\begin{pmatrix}r\\ s\end{pmatrix}\mapsto\begin{pmatrix}r\\ (y-x)s+\frac{x(r^2-r)}{2}\end{pmatrix}.$$

Indeed, a similar calculation as in Example 2.4.6 shows that $f$ is a skew brace homomorphism. Since we assume that $R$ is a field, the element $x-y$ has an inverse, from which it follows that $\ker f$ is trivial. Also,

$$f\left(\begin{matrix}r\\ (y-x)^{-1}\left(s-\frac{x(r^2-r)}{2}\right)\end{matrix}\right)=\begin{pmatrix}r\\ s\end{pmatrix},$$

so $f$ is surjective.

Let now $G$ and $H$ be groups. We have seen in Section 2.1 that semidirect products of the form $\mathrm{Triv}(G)\rtimes\mathrm{Triv}(H)$, respectively $\mathrm{Triv}(G)\rtimes\mathrm{opTriv}(H)$, are an easy way to construct $\lambda$-homomorphic skew braces, respectively bi-skew braces. It is therefore natural to try to generalize this construction in order to obtain brace blocks.

For a group homomorphism $\alpha:H\to\mathrm{Aut}(G)$, we write $\circ_\alpha$ for the group operation on $G\times H$ given by the semidirect product of $G$ and $H$.

**Proposition 2.4.9.** *Let $G$ and $H$ be groups, let $M$ be an abelian subgroup of $\mathrm{Aut}(G)$, and let $\mathcal{S}$ be the set of group homomorphisms $\alpha:H\to M$. Then $(G\times H,\circ_\alpha)_{\alpha\in\mathcal{S}}$ is a brace block.*

*Proof.* For $\alpha\in\mathcal{S}$, let $\lambda_\alpha$ be the $\lambda$-map associated with $(G\times H,\cdot,\circ_\alpha)$:

$$\lambda_\alpha:G\times H\to\mathrm{Aut}(G)\times\mathrm{Aut}(H)\subseteq\mathrm{Aut}(G\times H):(g,h)\mapsto(\alpha_h,\mathrm{id}).$$

These images are all contained in the abelian subgroup $M\times\{\mathrm{id}\}$ of $\mathrm{Aut}(G\times H)$. In order to apply Theorem 2.4.5, it suffices to check that $\lambda_{\alpha,\psi(g,h)}=\lambda_{\alpha,(g,h)}$ for all $\alpha\in\mathcal{S}$, $\psi=(\psi',\mathrm{id})\in\{\mathrm{id}\}\times M$, and $(g,h)\in G\times H$. We find

$$\lambda_{\alpha,\psi(g,h)}=\lambda_{\alpha,(\psi'(g),h)}=(\alpha_h,\mathrm{id})=\lambda_{\alpha,(g,h)},$$

from which the statement follows. □

**Example 2.4.10.** For all $n\geq 0$, define the group homomorphism

$$\alpha_n:\mathbb{Z}\to\mathrm{GL}_2(\mathbb{Z}):x\mapsto\begin{pmatrix}1&0\\ nx&1\end{pmatrix}.$$

As

$$B=\left\{\begin{pmatrix}1&0\\ x&1\end{pmatrix}\mid x\in\mathbb{Z}\right\}$$

is an abelian subgroup of $\mathrm{GL}_2(\mathbb{Z})$, from Proposition 2.4.9 we obtain a brace block $(\mathbb{Z}\times\mathbb{Z}^2,\circ_n)_{n\geq 0}$ with

$$\begin{pmatrix}x\\y\\z\end{pmatrix}\circ_n\begin{pmatrix}x'\\y'\\z'\end{pmatrix}=\begin{pmatrix}x+x'\\y+y'\\z+z'+nxy'\end{pmatrix}.$$

In particular, if $n\neq m$, then $(\mathbb{Z}\times\mathbb{Z}^2,\circ_{\alpha_n})$ and $(\mathbb{Z}\times\mathbb{Z}^2,\circ_{\alpha_m})$ are non-isomorphic, as the abelianization of $(\mathbb{Z}\times\mathbb{Z}^2,\circ_{\alpha_n})$ is isomorphic to $\mathbb{Z}^2\times C_n$. We have thus obtained a brace block with countably many non-isomorphic groups.

**Example 2.4.11.** Let $(A,\cdot)$ be a group, and let $B$ be a subgroup of $A$. Assume that the group of inner automorphisms of $(A,\cdot)$ induced by $B$, which we denote by $\mathrm{Inn}_B(A)$, is abelian. It is easy to check that this is equivalent to $[B,B]\subseteq Z(A)$.

For all group homomorphisms $\lambda:(A,\cdot)\to\mathrm{Inn}_B(A)$ and $a\in A$, $b\in B$ we find

$$\lambda_{b\cdot a\cdot b^{-1}}=\lambda_b\lambda_a\lambda_b^{-1}=\lambda_a,$$

This means that if we denote by $\mathcal{S}$ the set of group homomorphisms from $A$ to $\mathrm{Inn}_B(A)$, we obtain a brace block $(A,\circ_\lambda)_{\lambda\in\mathcal{S}}$ with

$$a\circ_\lambda b=a\cdot\lambda_a(b).$$

Note that the groups homomorphisms $A\to\mathrm{Inn}_B(A)$ correspond precisely to the group homomorphisms $A\to B/(B\cap Z(A))$, because $\mathrm{Inn}_B(A)\cong B/(B\cap Z(A))$. For example, every group homomorphism $\psi:A\to B$ yields a group homomorphism $A\to B/(B\cap Z(A))$, which we can use for our construction. Moreover, we have $\psi[A,A]\subseteq[B,B]\subseteq Z(A)$, so we find precisely the condition described in [42, Theorem 1.2]. In particular, when $B$ is abelian, we recover [100, 101]. Indeed, all the bi-skew braces found in these works are associated with $\lambda$-maps which act by conjugation and have a common abelian codomain; see also Remark 2.4.14.

**Example 2.4.12.** We show now how the main construction of [43] follows from Theorem 2.4.5. Let $(A,\cdot)$ be a group, let $B$ be a subgroup of $(A,\cdot)$ such that $[B,B]$ is contained in $Z(A)$ (so that $\mathrm{Inn}_B(A)$, defined as before, is abelian), and let $K$ be a subgroup of $B$ contained in $Z(A)$. Note that we do not require that $B/K$ is abelian. Define

$$\mathcal{A}=\{\psi:A/K\to B/K\text{ group homomorphism}\},$$
$$\mathcal{B}=\{\alpha:A\times A\to K\mid\alpha\text{ is bilinear and }\alpha(A,K)=\alpha(K,A)=\{1\}\}.$$

For $\psi\in\mathcal{A}$ and $\alpha\in\mathcal{B}$, define

$$a\circ_{\psi,\alpha}b=a\cdot\psi(aK)\cdot b\cdot\psi(aK)^{-1}\cdot\alpha(a,b),$$

where $\psi(aK)\cdot b\cdot\psi(aK)^{-1}$ is to be interpreted as the conjugation of $b$ by any element in the coset $\psi(aK)$. In [43] it is shown that $(A,\circ_{\psi,\alpha})_{(\psi,\alpha)\in\mathcal{A}\times\mathcal{B}}$ is a brace block. We can write

$$a\circ_{\psi,\alpha}b=a\cdot\lambda_{1,a}\lambda_{2,a}(b),$$

where $\lambda_{1,a}$ denotes conjugation by any element of $\psi(a)$ and

$$\lambda_{2,a}:b\mapsto b\cdot\alpha(a,b).$$

Consider now the following subgroup of central automorphisms of $(A, \cdot)$:

$$L = \{\beta \in \mathrm{Aut}(A, \cdot) \mid \beta(b) \cdot b^{-1} \in K \text{ and } \beta(k) = k \text{ for all } b \in A \text{ and } k \in K\}.$$

The group $L$ is abelian and it centralizes the subgroup of inner automorphisms of $\mathrm{Aut}(A, \cdot)$, so that $M = \mathrm{Inn}_B(A)L$ is abelian. Now define $\mathcal{S}$ as in Theorem 2.4.5, with respect to $M$. Clearly, $\lambda_{1,a} \in \mathrm{Inn}_B(A)$ and $\lambda_{2,a} \in L$ for all $a \in A$, hence the map $a \mapsto \lambda_{1,a}\lambda_{2,a}$ is an element of $\mathcal{S}$, so we apply Theorem 2.4.5 to derive our claim.

Note that in fact there is no need for the codomain of the maps in $\mathcal{A}$ to be $B/K$. We could just consider group homomorphisms from $A/K$ to $B/(B \cap Z(A))$ and find that the construction still works. This means that we do not require any relation between $K$ and $B$; in this way, we find a further generalization of the original construction.

We now use Theorem 2.4.5 to obtain an iterative construction of brace blocks.

**Corollary 2.4.13.** *Let $(A, \cdot, \circ)$ be a $\lambda$-homomorphic bi-skew brace, and for all $n \in \mathbb{Z}$ and $a \in A$, let $\lambda_{n,a} = \lambda_{a^n} = \lambda_a^n$. Then $(A, \circ_n)_{n\in\mathbb{Z}}$ is a brace block, where*

$$a \circ_n b = a \cdot \lambda_{n,a}(b).$$

*Proof.* Apply Theorem 2.4.5 with $M = \lambda(A)$, which is abelian by Lemma 1.1.35. □

*Remark* 2.4.14. This construction presents some similarities with Koch's construction [101] (or more precisely, the variation presented in [43, Example 5.2]), but the operations we find are different. Indeed, let $(A, \cdot)$ be a group, and let $\psi$ be an abelian endomorphism. Then $(A, \cdot, \circ)$ is a $\lambda$-homomorphic bi-skew brace, where $\lambda_a$ is conjugation by $\psi(a)$. Both Corollary 2.4.13 and [43, Example 5.2] yield a brace block $(A, \circ_n)_{n\in\mathbb{Z}}$, where

$$a \circ_n b = a \cdot \psi_n(a) \cdot b \cdot \psi_n(a)^{-1}.$$

for some maps $\psi_n : A \to A$. In Koch's case,

$$\psi_n(a) = \prod_{i=1}^{n} \psi^i \left(a^{\binom{n}{i}}\right),$$

while in our case, $\psi_n(a) = \psi(a^n)$.

*Remark* 2.4.15. Corollary 2.4.13, which is a natural application of Theorem 2.4.5, also appears in [19, Theorem 4.12], where the approach followed is significantly different.

**Example 2.4.16.** Let

$$\lambda : \mathbb{Z}^2 \to \mathrm{GL}_2(\mathbb{Z}) : \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}.$$

This yields a $\lambda$-homomorphic bi-skew brace, and applying Corollary 2.4.13 we find precisely the $\lambda_n$, $n \geq 0$, as in Example 2.4.7. In particular, this iterative construction yields a brace block containing countably many non-isomorphic skew braces.

It is natural to ask whether a similar construction as Corollary 2.4.13 is still possible when we are not necessarily starting from a $\lambda$-homomorphic bi-skew brace. The following proposition shows that this is indeed the case.

**Proposition 2.4.17.** *Let $A$ be a skew brace, and let $\psi$ be a group endomorphism of $(A,\cdot)$ such that for all $a,b\in A$, the equation*

$$\psi(\lambda_{\psi(a)}(b))=\lambda_{\psi(a)}(\psi(b)),$$

*holds. Then $(A,\cdot,\circ_\psi)$ is a skew brace, where*

$$a\circ_\psi b=a\cdot\lambda_{\psi(a)}(b).$$

*Proof.* It suffices to prove that the map

$$A\to\mathrm{Aut}(A,\cdot):a\mapsto\lambda_{\psi(a)},$$

satisfies the conditions of Lemma 1.1.10. For all $a,b\in A$, we find that

$$\begin{aligned}\lambda_{\psi(a\cdot\lambda_{\psi(a)}(b))}&=\lambda_{\psi(a)\cdot\psi(\lambda_{\psi(a)}(b))}\\&=\lambda_{\psi(a)\cdot\lambda_{\psi(a)}\psi(b)}\\&=\lambda_{\psi(a)\circ\psi(b)}\\&=\lambda_{\psi(a)}\lambda_{\psi(b)}.\end{aligned}$$

□

The relation with Corollary 2.4.13 is especially clear when we look at the following straightforward corollary, which in particular applies to Jacobson radical rings.

**Corollary 2.4.18.** *Let $(A,+,\circ)$ be a (two-sided) brace. Then $(A,+,\circ_n)$ is a (two-sided) brace for all $k\in\mathbb{Z}$, where*

$$a\circ_k b=a+\lambda_{ka}(b).$$

*Proof.* The fact that $(A,\cdot,\circ_n)$ is a brace follows by applying Proposition 2.4.17, with

$$\psi:(A,+)\to(A,+):a\mapsto ka.$$

Note that $a*_k b=(ka)*b$, where we $*_k$ denotes the $*$-operation in $(A,+,\circ_k)$. Therefore, if $(A,+,\circ)$ is two-sided then

$$a*_k(b*_k c)=(ka)*((kb)*c)=k^2(a*(b*c))=k^2((a*b)*c)=(k((ka)*b)*c=(a*_k b)*_k c,$$

so we conclude from Proposition 1.1.17 that also $(A,+,\circ_k)$ is two-sided. □

*Remark* 2.4.19. Note the similarity with cabling of involutive solutions, as described in Section 1.2.5. Let $(X,r)$ be an involutive solution and identify $X$ with its image in $G(X,r)$. We know then that $(X,r)$ is precisely the restriction of the solution $(G(X,r),R_{G(X,r)})$ to $X$. The $k$-cabled solution $(X,r^{(k)})$ is precisely the solution one obtains by restricting the solution on $(G(X,r),+,\circ_k)$ to $X$.

Similarly, given a brace $A$, the solution $(A,r_{(A,\cdot,\circ_k)})$ is precisely the $k$-cabling of the solution $(A,r_A)$.

# Chapter 3

# Two-sided skew braces

Recall that left braces were introduced by Rump as a generalization of Jacobson radical rings in [132]. More precisely, he established a correspondence between Jacobson radical rings and two-sided braces, as recalled in Proposition 1.1.14. Since the Jacobson radical of a ring is indispensable in ring theory, Jacobson radical rings have been extensively studied; see for example [5, 6, 157, 168]. The notion of two-sidedness equally makes sense for skew braces. However, results on two-sided skew braces are scarce in the literature, with most results due to Nasybullov [123].

In this chapter, we build further upon some ideas by Nasybullov and combine them with novel techniques in order to obtain the main result that every two-sided skew brace is an extension of a weakly trivial skew brace by a two-sided brace, and use this to obtain structural results on two-sided skew braces.

The chapter is organized as follows. In Section 3.1, we introduce the new notion of weakly trivial skew braces and we prove that they are the subdirect products of a trivial and an almost trivial skew brace. After adapting Goursat's lemma to skew braces, we obtain a precise characterization of weakly trivial skew braces through pairs of groups with isomorphic abelianizations in Theorem 3.1.12. In Section 3.2, we then obtain our main results. For example, in Theorem 3.2.7 we show that aside from trivial and almost trivial skew braces on simple groups, the only simple two-sided skew braces are infinite two-sided braces. Also, we generalize some results of Jacobson radical rings to two-sided skew braces and improve some of the results obtained in [123] on the connection between the additive and multiplicative groups of two-sided skew braces. In [107], prime and semiprime skew braces were introduced by Konovalov, Smoktunowicz and Vendramin. Subsequently, in [149] strongly prime and strongly semiprime skew braces were introduced by Smoktunowicz. For two-sided braces, both variations coincide with the usual notions for rings. It is not clear from the discussion in [149] whether they are in fact different. In Theorems 3.3.5 and 3.3.6, we answer this question in the negative for two-sided skew braces. Note that in [16] an example appears of a brace of size 32 that is prime but not strongly prime, therefore affirmatively answering the more general question.

All results in this chapter for which no external reference is given are the author's own work and are published in [158].

## 3.1 Weakly trivial skew braces

In this section, we introduce the new notion of weakly trivial skew braces. Other than being a generalization of both trivial and almost trivial skew braces, the real motivation for this definition will become clear in

Section 3.2.

**Definition 3.1.1.** A skew left brace $A$ is *weakly trivial* if $A^2 \cap A^2_{\mathrm{op}} = \{0\}$.

**Example 3.1.2.** All trivial and almost trivial skew braces are weakly trivial. Also, direct products and skew subbraces of weakly trivial skew braces are weakly trivial.

**Definition 3.1.3.** Let $G$ and $H$ be groups. A *subdirect product* of $G$ and $H$ is a subgroup $F$ of $G \times H$ such that $\mathrm{pr}_G(F) = G$ and $\mathrm{pr}_H(F) = H$, where $\mathrm{pr}_G$, respectively $\mathrm{pr}_H$, is the canonical projection of $G \times H$ onto $G$, respectively $H$. A *subdirect product of skew braces* is defined analogously.

**Proposition 3.1.4.** *A skew brace $A$ is weakly trivial if and only if it embeds into a product of a trivial and almost trivial skew brace. In particular, it embeds as a subdirect product into $A/A^2 \times A/A^2_{\mathrm{op}}$.*

*Proof.* One implication is trivial. For the converse implication, consider the canonical surjections $\pi_1 : A \to A/A^2$ and $\pi_2 : A \to A/A^2_{\mathrm{op}}$. The skew brace homomorphism

$$\iota : A \to A/A^2 \times A/A^2_{\mathrm{op}} : a \mapsto (\pi_1(a), \pi_2(a))$$

has kernel $A^2 \cap A^2_{\mathrm{op}} = \{0\}$. As $\iota(A)$ is a subdirect product, $A/A^2$ is trivial and $A/A^2_{\mathrm{op}}$ is almost trivial, this concludes the proof. □

*Remark* 3.1.5. A weakly trivial skew brace $A$ might be constructed as a subdirect product of a trivial and an almost trivial skew brace in multiple ways. Take for example two non-abelian groups $G$ and $H$ and consider the direct, hence subdirect, product $A = \mathrm{Triv}(G) \times \mathrm{opTriv}(H)$. It is easily seen that $A/A^2 \cong \mathrm{Triv}(G) \times \mathrm{Triv}(\mathrm{Ab}(H))$ and $A/A^2_{\mathrm{op}} \cong \mathrm{Triv}(\mathrm{Ab}(G)) \times \mathrm{opTriv}(H)$, where $\mathrm{Ab}(H)$ is the abelianization of $H$. We conclude that $A$ is a subdirect product of

$$(\mathrm{Triv}(G) \times \mathrm{Triv}(\mathrm{Ab}(H))) \times (\mathrm{Triv}(\mathrm{Ab}(G)) \times \mathrm{opTriv}(H)).$$

Although one might argue that it is more desirable to write $A$ as a direct product when possible, the embedding into $A/A^2 \times A/A^2_{\mathrm{op}}$ provides a canonical choice which will prove to be useful in the classification in Theorem 3.1.12.

**Corollary 3.1.6.** *Every weakly trivial skew brace is two-sided.*

*Proof.* Let $A$ be a weakly trivial skew brace. As $A/A^2$ and $A/A^2_{\mathrm{op}}$ are two-sided, so is $A/A^2 \times A/A^2_{\mathrm{op}}$ and therefore also $A$ by Proposition 3.1.4. □

**Proposition 3.1.7.** *Let $A$ be a skew brace, then $A/(A^2 \cap A^2_{\mathrm{op}})$ is a weakly trivial skew brace.*

*Proof.* Note that we have a natural embedding $\iota : A/(A^2 \cap A^2_{\mathrm{op}}) \to A/A^2 \times A/A^2_{\mathrm{op}}$. The statement then follows from Proposition 3.1.4. □

We now classify all weakly trivial skew braces. Our main tool for this is a generalization of Goursat's lemma [81] to skew braces. For this, we first need the existence of pullbacks in the category of skew braces. This construction is classical and we therefore omit the proof.

**Proposition 3.1.8.** *Let $B, C, D$ be skew braces with skew brace homomorphisms $f : B \to D$, $g : C \to D$. Then the pullback of*

$$\begin{array}{ccc} & & B \\ & & \downarrow f \\ C & \xrightarrow{g} & D \end{array}$$

*exists and is, up to isomorphism, given by*

$$B \times_D C := \{(a, b) \mid f(a) = g(b)\} \subseteq B \times C,$$

*together with the projection maps $\mathrm{pr}_B : B \times_D C \to B$ and $\mathrm{pr}_C : B \times_D C \to C$.*

The following version of Goursat's lemma holds for skew braces.

**Lemma 3.1.9.** *There is a bijective correspondence between subdirect products of skew braces $B$ and $C$ and triples $(I, J, \rho)$ where $I$, respectively $J$, is an ideal of $B$, respectively $C$, and $\rho : B/I \to C/J$ is an isomorphism of skew braces.*

*Proof.* We only give a sketch of the construction. Further details are just as in the classical case and are left to the reader. Let $A$ be a subdirect product of $B$ and $C$. Let $I \subseteq B$ be $B$ such that

$$I \times \{0\} = A \cap (B \times \{0\}),$$

and $J \subseteq C$ such that

$$\{0\} \times J = A \cap (\{0\} \times C).$$

Then $I$, respectively $J$, is an ideal of $B$, respectively $C$, and the map $\rho : B/I \to C/J$, given by $\rho(a) = b$ if and only if $(a, b) \in A$, is a well-defined skew brace isomorphism. We therefore obtain a triple $(I, J, \rho)$.

Conversely, if a triple $(I, J, \rho)$ is given, the pullback of

$$\begin{array}{ccccc} & & & & B \\ & & & & \downarrow \\ C & \longrightarrow & C/J & \xrightarrow{\rho} & B/J \end{array}$$

yields a subdirect product of $B$ and $C$. □

Recall from Example 1.1.22 that the commutator of a skew brace $A$ is $A' = A^2 \cdot A^2_{\mathrm{op}}$.

**Lemma 3.1.10.** *Let $A$ be a weakly trivial skew brace. Then $A$ fits in the following pullback diagram:*

$$\begin{array}{ccc} A & \longrightarrow & A/A^2 \\ \downarrow & & \downarrow \\ A/A^2_{\mathrm{op}} & \longrightarrow & A/A' \end{array}$$

*Proof.* We denote the image of the embedding of $A$ into $A/A^2 \times A/A^2_{\mathrm{op}}$ by $B$ and now proceed as explained in the proof of Lemma 3.1.9. Clearly

$$B \cap (A/A^2 \times \{0\}) = \{(a \cdot A^2, 0) \mid a \in A^2_{\mathrm{op}}\} = (A^2)^2_{\mathrm{op}} \times \{0\}.$$

Likewise, one finds that $B \cap (\{0\} \times A/A^2_{\mathrm{op}}) = \{0\} \times (A/A^2)^2_{\mathrm{op}}$. Since $A' = A^2 \cdot A^2_{\mathrm{op}}$, it follows that

$$(A/A^2_{\mathrm{op}})/(A/A^2_{\mathrm{op}})^2 \cong A/A',$$

and

$$(A/A^2)/(A/A^2)^2_{\mathrm{op}} \cong A/A'.$$

The isomorphism

$$\rho : A/A' \cong (A/A^2_{\mathrm{op}})/(A/A^2_{\mathrm{op}})^2 \to (A/A^2)/(A/A^2)^2_{\mathrm{op}} \cong A/A',$$

must clearly be the identity in order to make the above diagram commute. □

**Definition 3.1.11.** Consider the class of triples $(G, H, \theta)$ with $G$ and $H$ groups and $\theta : \mathrm{Ab}(G) \to \mathrm{Ab}(H)$ an isomorphism. We say that two such triples $(G_1, H_1, \theta_1)$ and $(G_2, H_2, \theta_2)$ are equivalent if there exist group isomorphisms $\phi_G : G_1 \to G_2$, $\phi_H : H_1 \to H_2$ such that

$$\begin{array}{ccccccc} G_1 & \longrightarrow & \mathrm{Ab}(G_1) & \xrightarrow{\theta_1} & \mathrm{Ab}(H_1) & \longleftarrow & H_1 \\ \downarrow{\scriptstyle \phi_G} & & \downarrow{\scriptstyle \overline{\phi_G}} & & \downarrow{\scriptstyle \overline{\phi_H}} & & \downarrow{\scriptstyle \phi_H} \\ G_2 & \longrightarrow & \mathrm{Ab}(G_2) & \xrightarrow{\theta_2} & \mathrm{Ab}(H_2) & \longleftarrow & H_2 \end{array}$$

commutes, where $\overline{\phi_G}$ and $\overline{\phi_H}$ are the unique induced group isomorphisms making the square on the left and right-hand side commute.

**Theorem 3.1.12.** *There exists a bijection between isomorphism classes of weakly trivial skew braces and equivalence classes of triples as described in Definition 3.1.11.*

*Proof.* Let $A$ be a weakly trivial skew brace. We know that

$$\mathrm{Ab}(A/A^2, \circ) \cong (A/A', \circ) \cong \mathrm{Ab}(A/A^2_{\mathrm{op}}, \circ).$$

Hence $((A/A^2, \circ), (A/A^2_{\mathrm{op}}, \circ), \rho)$, where $\rho$ is the above group isomorphism, is a triple as described in Definition 3.1.11.

Conversely, given a triple $(G, H, \rho)$ we can construct the pullback of the diagram

$$\begin{array}{ccccc} & & & & \mathrm{Triv}(G) \\ & & & & \downarrow \\ \mathrm{opTriv}(H) & \longrightarrow & \mathrm{opTriv}(\mathrm{Ab}(H)) & \xrightarrow{\rho} & \mathrm{Triv}(\mathrm{Ab}(G)) \end{array}$$

which clearly is a weakly trivial skew brace.

It follows from Lemma 3.1.10 that if we start from a weakly trivial skew brace, consider its associated triple $((A/A^2, \circ), (A/A^2_{\mathrm{op}}, \circ), \rho)$ and then again take the pullback as described above we end up with a skew brace isomorphic to $A$.

Conversely, start from a triple $(G, H, \rho)$ and let $A \subseteq \mathrm{Triv}(G) \times \mathrm{opTriv}(H)$ be its associated pullback. We want to prove that the triple associated to $A$ is isomorphic to $(G, H, \rho)$, which we can do by showing that

the kernels of the vertical maps in the following commutative diagram are $A^2$, $A'$, $A'$ and $A^2_{\mathrm{op}}$ respectively.

$$\begin{array}{ccccccc} (A,\circ) & \xrightarrow{\mathrm{id}} & (A,\circ) & \xrightarrow{\mathrm{id}} & (A,\circ) & \xleftarrow{\mathrm{id}} & (A,\circ) \\ \downarrow{\scriptstyle \mathrm{pr}_G} & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{pr}_H} \\ G & \longrightarrow & \mathrm{Ab}(G) & \xrightarrow{\theta_2} & \mathrm{Ab}(H) & \longleftarrow & H \end{array}$$

The kernel of the first vertical map is clearly $A \cap (\{0\} \times H) = \{0\} \times [H, H]$. Also, $A^2$ is generated by the elements $(g_1, h_1) * (g_2, h_2) = (h_2^{-1} h_1 h_2 h_1^{-1})$ for $(g_1, h_1), (g_2, h_2) \in A$. As every element of $H$ can appear as the second coordinate of an element of $A$, the equality $A \cap (\{0\} \times H) = A^2$ follows. Similarly, it follows that the kernel of $\mathrm{pr}_H$ is equal to $A^2_{\mathrm{op}}$. The kernel of the second vertical map must correspond to the commutator subgroup of $(A/A^2, \circ)$, which is $(A/A^2)^2_{\mathrm{op}}$, and similar for the third vertical map. □

When one looks at weakly trivial skew braces of small size, using for example the YangBaxter GAP package [165], it appears that their additive and multiplicative group are always isomorphic. The following example shows that this is not always the case.

**Example 3.1.13.** Consider the group

$$G := \langle a, b \mid a^5 = b^4 = 0, b^{-1}ab = a^2 \rangle \cong C_5 \rtimes C_4.$$

Its derived subgroup is the subgroup generated by $a$, hence $\mathrm{Ab}(G) \cong C_4$ is generated by the equivalence class of $b$. Let $A$ be the weakly trivial skew brace associated to the triple $(G, G, \mathrm{id})$. Then

$$A = \{(a^k b^l, a^m b^l) \mid k, l, m \in \mathbb{Z}\} \subseteq \mathrm{Triv}(G) \times \mathrm{opTriv}(G).$$

The multiplicative group $(A, \circ)$ is isomorphic to the semidirect product

$$C_5^2 \rtimes_1 C_4 := \langle x, y, z \mid x^5 = y^5 = z^4 = 0, xy = yx, z^{-1}xz = x^2, z^{-1}yz = y^2 \rangle,$$

where $(a, 0) \mapsto x$, $(0, a) \mapsto y$ and $(b, b) \mapsto z$. Meanwhile, as $b^{-1} \cdot a \cdot b = bab^{-1} = a^{-2} = a^3$ in $\mathrm{opTriv}(G)$, we find that $(A, \cdot)$ is isomorphic to

$$C_5^2 \rtimes_2 C_4 := \langle x, y, z \mid x^5 = y^5 = z^4 = 0, xy = yx, z^{-1}xz = x^2, z^{-1}yz = y^3 \rangle,$$

where $(a, 0) \mapsto x$, $(0, a) \mapsto y$ and $(b, b) \mapsto z$. However, $C_5^2 \rtimes_1 C_4$ is not isomorphic to $C_5^2 \rtimes_2 C_4$, as in the first group all subgroups of order 5 are normal, but in the latter the subgroup of order 5 generated by $xy$ is not normal.

**Example 3.1.14.** The previous example can be generalized by replacing $G$ by $\mathrm{Hol}(C_p) = C_p \rtimes \mathrm{Aut}(C_p)$ with $p > 3$ a prime. In this way, one obtains an infinite number of weakly trivial skew braces with non-isomorphic additive and multiplicative groups.

Although the class of weakly trivial skew braces is closed under taking direct products and skew subbraces, it is only closed under quotients by an ideal if the ideal satisfies some extra property.

**Lemma 3.1.15.** *Let $A$ be a weakly trivial skew brace and $\iota : A \to A/A^2 \times A/A^2_{\mathrm{op}}$ its canonical embedding. Then $I \subseteq A$ is an ideal of $A$ if and only if $\iota(I)$ is a normal subgroup of $(A/A^2 \times A/A^2_{\mathrm{op}}, \circ)$.*

*Proof.* Clearly $\lambda_{(a_1,a_2)}(b_1,b_2) = (b_1, a_2 \circ b_2 \circ \overline{a_2})$ and $\lambda^{\mathrm{op}}_{(a_1,a_2)}(b_1,b_2) = (\overline{a_1} \circ b_1 \circ a_1, b_2)$, for all $(a_1,a_2),(b_1,b_2) \in \iota(A)$. As the projections $\iota(A) \to A/A^2$ and $\iota(A) \to A/A^2_{\mathrm{op}}$ are surjective, the result follows. □

**Lemma 3.1.16.** *Let $A$ be a weakly trivial skew brace and $I$ an ideal of $A$. Then $A/I$ is weakly trivial if and only if $(I \cap A^2) \cdot (I \cap A^2_{\mathrm{op}}) = I \cap A'$.*

*Proof.* Let $I$ be an ideal of $A$ and consider the skew brace $A/I$. Assume that $a \cdot I \in (A/I)^2 \cap (A/I)^2_{\mathrm{op}}$. This means that there exist elements $b \in A^2$ and $c \in A^2_{\mathrm{op}}$ such that $a \cdot I = b \cdot I = c \cdot I$. If $a \notin I$ then also, $b, c \notin I$. Hence, $b \cdot c^{-1} \in I \cap A'$ is an element contained in $I \cap A'$ but not in $(I \cap A^2) \cdot (I \cap A^2_{\mathrm{op}})$. If $b \cdot c$, where $b \in A^2$ and $c \in A^2_{\mathrm{op}}$, is contained in $I \cap A'$ but not in $(I \cap A^2) \cdot (I \cap A^2_{\mathrm{op}})$ then $b \cdot I = c^{-1} \cdot I \in (A/I)^2 \cap (A/I)^2_{\mathrm{op}}$. □

**Example 3.1.17.** Let $G = D_8$, the dihedral group of order 8, and $A$ the weakly trivial skew brace associated to the triple $(G, G, \mathrm{id})$. Then

$$A = \{(g,h) \mid g \cdot [G,G] = h \cdot [G,G]\}.$$

In particular, $I = \{(g,g) \mid g \in Z(G)\} \subseteq A$ as $Z(G) = [G,G]$. By Lemma 3.1.15, it follows that $I$ is an ideal of $A$. But $I \cap A^2 = I \cap A^2_{\mathrm{op}} = \{0\}$, so from Lemma 3.1.16 it follows that $A/I$ is not weakly trivial. The same argument can be repeated for any group $G$ such that $Z(G) \cap [G,G]$ is non-trivial.

To conclude this section, we study some structural properties of weakly trivial skew braces.

**Lemma 3.1.18.** *Let $\iota : G \to G_1 \times G_2$ be a subdirect product of groups. Then $G$ is solvable if and only if $G_1 \times G_2$ is solvable, and in that case, the derived length of $G$ and $G_1 \times G_2$ coincide. Similarly, $G$ is nilpotent if and only if $G_1 \times G_2$ is nilpotent and the nilpotency class of $G$ and $G_1 \times G_2$ coincide.*

*Proof.* We prove the first part of the statement; the proof of the second part is analogous. Assume that $G$ is solvable, since both $G_1$ and $G_2$ are epimorphic images of $G$, they are solvable and their derived length is at most that of $G$. Hence, the same holds for $G_1 \times G_2$. Conversely, if $G_1 \times G_2$ is solvable, then so is the subgroup $G$ and it is clear that the derived length of $G$ is at most that of $G_1 \times G_2$. □

**Corollary 3.1.19.** *Let $A$ be a weakly trivial skew brace. Then $(A,\cdot)$ is solvable if and only if $(A,\circ)$ is solvable. In that case, their derived lengths coincide and $A$ is solvable as a skew brace.*

*Proof.* Consider the embedding $\iota : A \to A/A^2 \times A/A^2_{\mathrm{op}}$. Then in particular

$$\iota(A,\cdot) \subseteq (A/A^2,\cdot) \times (A/A^2_{\mathrm{op}},\cdot),$$

and

$$\iota(A,\circ) \subseteq (A/A^2,\circ) \times (A/A^2_{\mathrm{op}},\circ),$$

are subdirect products of groups. As $(A/A^2,\cdot) \times (A/A^2_{\mathrm{op}},\cdot) \cong (A/A^2,\circ) \times (A/A^2_{\mathrm{op}},\circ)$, the first part of the statement follows from Lemma 3.1.18. Now, if $A$ has a solvable additive subgroup, so does $A/A^2_{\mathrm{op}}$. In particular, $A/A^2_{\mathrm{op}}$ is solvable. As $A/A^2$ is trivial, hence solvable, we conclude that $A/A^2 \times A/A^2_{\mathrm{op}}$, and therefore also $A$, is solvable. □

The proof of Corollary 3.1.19 can easily be adapted to prove the following corollary.

**Corollary 3.1.20.** *Let $A$ be a weakly trivial skew brace. Then $(A,\cdot)$ is nilpotent if and only if $(A,\circ)$ is nilpotent. In that case, their nilpotency classes coincide and the skew brace $A$ is left and right nilpotent.*

**Proposition 3.1.21.** *Let $A$ be a weakly trivial skew brace. Then the following are equivalent:*

1. *$A$ is left nilpotent.*
2. *$A$ is right nilpotent.*
3. *$A$ is strongly nilpotent.*

*Proof.* For any skew brace, 3 holds whenever 1 and 2 hold by Theorem 1.1.30. Therefore, only the equivalence of 1 and 2 has to be proved.

Assume that $A$ is left nilpotent. Then the almost trivial skew brace $A/A^2_{\mathrm{op}}$ is left nilpotent, hence right nilpotent. As $A/A^2$ is trivial, so right nilpotent, it follows that $A/A^2 \times A/A^2_{\mathrm{op}}$, and therefore also its skew subbrace $A$, is right nilpotent. The same argument can be used to show that right nilpotency implies left nilpotency. □

## 3.2 Two-sided skew braces

We start this section by proving our main results, Theorem 3.2.3 and Corollary 3.2.4, for which we first need a lemma.

**Lemma 3.2.1.** *Let $A$ be a two-sided skew brace. Then $A^2$ and $A^2_{\mathrm{op}}$ centralize one another in $(A, \cdot)$.*

*Proof.* Let $a, b, c, d \in A$. Using consequently the fact that $A$ is a left and right skew brace,

$$\begin{aligned}(a \cdot b) \circ (c \cdot d) &= ((a \cdot b) \circ c) \cdot (a \cdot b)^{-1} \cdot ((a \cdot b) \circ d) \\ &= (a \circ c) \cdot c^{-1} \cdot (b \circ c) \cdot b^{-1} \cdot a^{-1} \cdot (a \circ d) \cdot d^{-1} \cdot (b \circ d) \\ &= (a \circ c) \cdot (b *_{\mathrm{op}} c) \cdot (a * d) \cdot (b \circ d).\end{aligned}$$

If we start by using the right skew brace structure, followed by the left one, then we find

$$\begin{aligned}(a \cdot b) \circ (c \cdot d) &= (a \circ (c \cdot d)) \cdot (c \cdot d)^{-1} \cdot (b \circ (c \cdot d)) \\ &= (a \circ c) \cdot a^{-1} \cdot (a \circ d) \cdot c^{-1} \cdot b^{-1} \cdot (b \circ c) \cdot b^{-1} \cdot (b \circ d) \\ &= (a \circ c) \cdot (a * d) \cdot (b *_{\mathrm{op}} c) \cdot (b \circ d).\end{aligned}$$

Comparing both calculations we find that $(b *_{\mathrm{op}} c) \cdot (a * d) = (a * d) \cdot (b *_{\mathrm{op}} c)$, from which the statement follows. □

*Remark* 3.2.2. Although this result is new, a similar argument is used in [123, Lemma 4.5] to prove that the additive group of $(A * Z(A, \circ)) \cdot (Z(A, \circ) * A)$ is abelian.

**Theorem 3.2.3.** *Let $A$ be a two-sided skew brace. Then $A^2 \cap A^2_{\mathrm{op}}$ is contained in $Z(A', \cdot)$. In particular, $A^2 \cap A^2_{\mathrm{op}}$ is a two-sided brace.*

*Proof.* Using Lemma 3.2.1 we find that $A^2 \cap A^2_{\mathrm{op}}$ is in the center of both $(A^2, \cdot)$ and $(A^2_{\mathrm{op}}, \cdot)$, so it is contained in the center of $(A', \cdot)$. In particular, the commutativity of $(A^2 \cap A^2_{\mathrm{op}}, \cdot)$ follows. □

**Corollary 3.2.4.** *Every two-sided skew brace is the extension of a weakly trivial skew brace by a two-sided left brace.*

*Proof.* It suffices to note that the ideal $A^2 \cap A^2_{\mathrm{op}}$ is a two-sided brace by Theorem 3.2.3 and $A/(A^2 \cap A^2_{\mathrm{op}})$ is a weakly trivial skew brace by Proposition 3.1.7. □

On the other hand, it is not generally true that any extension of a weakly trivial skew brace by a two-sided brace is a two-sided skew brace, as we now demonstrate.

**Example 3.2.5.** Let $A$ be the semidirect product $\mathrm{Triv}(C_3) \rtimes \mathrm{Triv}(C_2)$, where $\mathrm{Triv}(C_2)$ acts non-trivially. Then $A$ is an extension of the weakly trivial skew brace $\mathrm{Triv}(C_2)$ by the two-sided brace $\mathrm{Triv}(C_3)$. However, $\{0\} \times C_2$ is a characteristic subgroup of $(A, \cdot) \cong C_3 \times C_2$ but not a normal subgroup of $(A, \circ) \cong C_3 \ltimes C_2$. It follows that $A$ can not be two-sided, as this would contradict Corollary 1.1.16.

**Definition 3.2.6.** A skew brace $A$ is *simple* if the only ideals are $\{0\}$ and $A$.

We can now extend [123, Corollary 4.2], where a similar result is obtained under the assumption that the additive group is solvable.

**Theorem 3.2.7.** *Let $A$ be a simple two-sided skew brace. Then one of the following holds:*

1. $A \cong \mathrm{Triv}(G)$ *for a simple group $G$.*
2. $A \cong \mathrm{opTriv}(G)$ *for a simple group $G$.*
3. *$A$ is a simple two-sided brace.*

*Proof.* Let $A$ be a simple two-sided skew brace. If $A^2 = \{0\}$, this means that $A = \mathrm{Triv}(G)$ for some group $G$. In that case, the ideals of $A$ are precisely the normal subgroups of $G$, so we conclude that $G$ is simple. If $A^2_{\mathrm{op}} = \{0\}$ then the same reasoning yields that $A \cong \mathrm{opTriv}(G)$ for some simple group $G$. The only case that remains is the one where $A^2 = A^2_{\mathrm{op}} = A$. By Lemma 3.2.1, this implies that $(A, \cdot)$ is abelian. Hence, $A$ is a simple two-sided brace. □

**Corollary 3.2.8.** *Let $A$ be a finite simple two-sided skew brace. Then either $A \cong \mathrm{Triv}(G)$ or $A \cong \mathrm{opTriv}(G)$ for some finite simple group $G$.*

*Proof.* It is well-known that if $A$ is a finite two-sided brace, then $A$ is strongly nilpotent and thus $A^2 \neq A$. If furthermore $A$ is simple, then this implies that $A \cong \mathrm{Triv}(G)$ for some abelian group $G$. If we combine this observation with Theorem 3.2.7, the statement follows. □

*Remark* 3.2.9. Note that there exist simple non-trivial Jacobson radical rings, and therefore also simple non-trivial two-sided braces. The first such example was constructed in [139].

We now prove a refinement of [123, Theorem 4.6], where nilpotency instead of solvability of the multiplicative group was assumed and the upper bound was $2n$.

**Theorem 3.2.10.** *Let $A$ be a two-sided skew brace. If $(A, \circ)$ is solvable of derived length $n$, then $(A, \cdot)$ is solvable of derived length at most $n + 1$.*

*Proof.* By Proposition 3.1.7 we find that $A/(A^2 \cap A^2_{\mathrm{op}})$ is weakly trivial. Because $(A/(A^2 \cap A^2_{\mathrm{op}}), \circ)$ has derived length at most $n$, it follows from Corollary 3.1.19 that $(A/(A^2 \cap A^2_{\mathrm{op}}), \cdot)$ has derived length at most $n$. We also know that $(A^2 \cap A^2_{\mathrm{op}}, \cdot)$ is abelian by Theorem 3.2.3, from which we conclude that $(A, \cdot)$ has derived length at most $n + 1$. □

**Lemma 3.2.11.** *Let $A$ be a two-sided skew brace. If $(A, \circ)$ is nilpotent of class $n$, then $(A', \cdot)$ is nilpotent of class at most $n + 1$.*

*Proof.* As $A'/(A^2 \cap A^2_{\mathrm{op}})$ is weakly trivial and $(A'/(A^2 \cap A^2_{\mathrm{op}}), \circ)$ is nilpotent of class at most $n$, also $(A'/(A^2 \cap A^2_{\mathrm{op}}), \cdot)$ is nilpotent of class at most $n$ by Corollary 3.1.19. By Theorem 3.2.3, we have $A^2 \cap A^2_{\mathrm{op}} \subseteq Z(A', \cdot)$, so we conclude that $(A', \cdot)$ is nilpotent of class at most $n+1$. □

**Theorem 3.2.12.** *Let $A$ be a two-sided skew brace with nilpotent multiplicative group. Then its additive group is abelian-by-nilpotent and nilpotent-by-abelian.*

*Proof.* As $(A/A', \cdot)$ is abelian, the first claim follows by Lemma 3.2.11. For the second claim, recall from Theorem 3.2.3 that $(A^2 \cap A^2_{\mathrm{op}}, \cdot)$ is abelian. It follows from the assumption on $(A, \circ)$, together with Proposition 3.1.7 and Corollary 3.1.20, that $(A/(A^2 \cap A^2_{\mathrm{op}}), \cdot)$ is nilpotent. □

Recall that a group satisfies the *ascending chain condition (ACC) on subgroups* if there exists no infinite strictly ascending chain of subgroups. The following proposition is a reformulation of the main result of [168].

**Proposition 3.2.13.** *Let $A$ be a two-sided brace. Then the following are equivalent:*

1. *$(A, \cdot)$ satisfies the ACC on subgroups,*
2. *$(A, \circ)$ satisfies the ACC on subgroups.*

*In this case, $A$ is strongly nilpotent and $(A, \circ)$ is nilpotent.*

We now generalize the first part of the previous proposition to two-sided skew braces. A generalization of the second part is given at the end of this section in Theorem 3.2.24.

**Theorem 3.2.14.** *Let $A$ be a two-sided skew brace. Then the following are equivalent:*

1. *$(A, \cdot)$ satisfies the ACC on subgroups,*
2. *$(A, \circ)$ satisfies the ACC on subgroups.*

*Proof.* Throughout the proof we freely use the fact that the ACC on subgroups is preserved under taking subgroups, and forming quotients or extensions; see for example [130, 3.1.7] for a proof of the latter.

We first prove the statement for weakly trivial skew braces. Let $A$ be a weakly trivial skew brace such that $(A, \cdot)$ satisfies the ACC on subgroups. Then so do $(A/A^2, \cdot)$ and $(A/A^2_{\mathrm{op}}, \cdot)$, hence also $(A/A^2, \circ)$ and $(A/A^2_{\mathrm{op}}, \circ)$. As $A$ embeds into $A/A^2 \times A/A^2_{\mathrm{op}}$, we find that $(A, \circ)$ satisfies the ACC on subgroups. The other implication is proved in a similar way.

Next, let $A$ be any two-sided skew brace such that $(A, \cdot)$ satisfies the ACC on subgroups. Then both $(A/(A^2 \cap A^2_{\mathrm{op}}), \cdot)$ and $(A^2 \cap A^2_{\mathrm{op}}, \cdot)$ satisfy the ACC on subgroups. As $A/(A^2 \cap A^2_{\mathrm{op}})$ is weakly trivial and $A^2 \cap A^2_{\mathrm{op}}$ is a two-sided brace, we find that $(A/(A^2 \cap A^2_{\mathrm{op}}), \circ)$ and $(A^2 \cap A^2_{\mathrm{op}}, \circ)$ satisfy the ACC on subgroups. It follows that $(A, \circ)$ satisfies the ACC on subgroups. The other implication is proved similarly. □

It is natural to ask if Theorem 3.2.14 can be generalized in the following way.

*Question* 3.2.15. Let $A$ be a two-sided skew brace that satisfies the ACC on skew subbraces. Does this imply that the equivalent conditions of Theorem 3.2.14 are satisfied?

For weakly trivial skew braces, this question can easily be answered affirmatively. The question therefore remains whether the same is true for all two-sided braces.

Similarly, the question arises whether we can replace the ACC on subgroups by the assumption that they are finitely generated. It is generally not true that if $(A, \cdot)$ is finitely generated then $(A, \circ)$ is finitely generated, as the following example shows.

**Example 3.2.16.** Consider the wreath product $G = C_2 \wr \mathbb{Z}$, also known as the lamplighter group, which is finitely generated but does not satisfy the ACC on subgroups since it contains the group $H = \bigoplus_{i\in\mathbb{Z}} C_2$. By the construction in Example 2.2.6 we find a skew brace $A$ with multiplicative group $H \times \mathbb{Z}$ and additive group $G$. The group $H \times \mathbb{Z}$ is abelian, so the obtained skew brace is clearly two-sided. However, $G$ is finitely generated while $H \times \mathbb{Z}$ is not.

On the other hand, it is not even known whether there exist two-sided braces with a finitely generated multiplicative group and a non-finitely generated additive group. See [157, Question 4.1] for a short discussion of an equivalent question.

**Theorem 3.2.17.** *Let $A$ be a two-sided skew brace that satisfies the equivalent conditions of Theorem 3.2.14. Then $(A, \cdot)$ is solvable if and only if $(A, \circ)$ is solvable. In this case, $A$ is a solvable skew brace.*

*Proof.* Similar to the proof of Lemma 3.2.11, it is sufficient to prove the statement for weakly trivial skew braces and two-sided braces. For weakly trivial skew braces, this was proved in Corollary 3.1.19. For two-sided braces, the additive group is of course solvable, and it follows from Proposition 3.2.13 that both the brace and the multiplicative group are solvable. □

*Remark* 3.2.18. We can not drop the condition of Theorem 3.2.17. An example of a two-sided brace whose additive group is not finitely generated and whose multiplicative group is non-solvable is given in [123, Example 3.2].

Our next aim is to prove that, as for two-sided braces, there is no distinction between left and right nilpotency for two-sided skew braces whose additive group is nilpotent.

**Lemma 3.2.19.** *Let $A$ be a two-sided skew brace. Then for all $a, b \in A$ and $c \in Z(A, \cdot)$, we have $a*c, c*a \in Z(A, \cdot)$ and*

$$c * (a \cdot b) = (c * a) \cdot (c * b),$$
$$(a \cdot b) * c = (a * c) \cdot (b * c).$$

*Proof.* As $Z(A, \cdot)$ is characteristic in $(A, \cdot)$, it is an ideal of $A$ by Corollary 1.1.16. This implies the first part of the statement. The second part follows from Lemma 1.1.18. □

**Lemma 3.2.20.** *Let $A$ be a two-sided skew brace. Then for all $a, b \in A$ and $c \in Z(A, \cdot)$, we have that $(a * b) * c = a * (b * c)$.*

*Proof.* Let $a, b \in A$, $c \in Z(A, \cdot)$. Using Lemma 3.2.19 and Lemma 1.1.18 we find

$$\begin{aligned}(a * b) * c &= (a^{-1} \cdot (a \circ b) \cdot b^{-1}) * c \\ &= (a * c)^{-1} \cdot ((a \circ b) * c) \cdot (b * c)^{-1} \\ &= (a * c)^{-1} \cdot (a * (b * c)) \cdot (b * c) \cdot (a * c) \cdot (b * c)^{-1} \\ &= a * (b * c).\end{aligned}$$

□

**Lemma 3.2.21.** *Let $A$ be a two-sided skew brace and $X, Y, Z$ subsets of $A$ with $X \subseteq Z(A, \cdot)$. Then $(X * Y) * Z = X * (Y * Z)$.*

*Proof.* By definition, $Y * Z$ consists of all elements of the form $(b_1 * c_1)^{\epsilon_1} \cdot \ldots \cdot (b_n * c_n)^{\epsilon_n}$ with $n \geq 1$, $\epsilon_i \in \{-1, 1\}$, $b_i \in Y$, $c_i \in Z$. Therefore, $X * (Y * Z)$ is the additive subgroup generated by

$$\{a * ((b_1 * c_1)^{\epsilon_1} \cdot \ldots \cdot (b_n * c_n)^{\epsilon_n}) \mid n \geq 1, \epsilon_i \in \{-1, 1\}, a \in X, b_i \in Y, c_i \in Z\}.$$

Using Lemma 3.2.19 we find that

$$a * ((b_1 * c_1)^{\epsilon_1} \cdot \ldots \cdot (b_n * c_n)^{\epsilon_n}) = (a * (b_1 * c_1))^{\epsilon_1} \cdot \ldots \cdot (a * (b_n * c_n))^{\epsilon_n},$$

so $X * (Y * Z)$ is the additive subgroup generated by

$$\{(a * (b * c) \mid a \in X, b \in Y, c \in Z\}. \tag{3.1}$$

A similar argument shows that $(X * Y) * Z$ is the additive subgroup generated by

$$\{(a * b) * c \mid a \in X, b \in Y, c \in Z\}. \tag{3.2}$$

It follows from Lemma 3.2.20 that (3.1) and (3.2) are the same set. □

**Lemma 3.2.22.** *Let $A$ be a two-sided skew brace and $m \geq 1$ such that $A^{(m)} \subseteq Z(A, \cdot)$. Then for all $k \geq 1$,*

$$A^{(m+k)} = A^{(m)} * A^{(k)}, \tag{3.3}$$

$$A^{(mk)} = (A^{(m)})^{(k)}. \tag{3.4}$$

*Proof.* We first prove (3.3) by induction on $k$. For $k = 1$ this is true by definition. For $k > 1$ we use the induction hypothesis and Lemma 3.2.21 to find

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

Next, we prove (3.4) by induction on $k$. For $k = 1$ this is trivial. We can use the induction hypothesis and (3.3) to find that also for $k > 1$,

$$A^{(mk)} = A^{(m(k-1)+m)} = A^{(m(k-1))} * A^{(m)} = (A^{(m)})^{(k-1)} * A^{(m)} = (A^{(m)})^{(k)}.$$ □

**Theorem 3.2.23.** *Let $A$ be a two-sided skew brace with $(A, \cdot)$ nilpotent. Then the following properties are equivalent:*

1. *$A$ is left nilpotent.*
2. *$A$ is right nilpotent.*
3. *$A$ is strongly nilpotent.*

*Proof.* Because of Theorem 1.1.30, only the equivalence of 1 and 2 has to be proved. We prove the implication from 1 to 2 through induction on the nilpotency class $n$ of $(A, \cdot)$. If $n = 1$, then $A$ is a two-sided brace, so in particular, left and right nilpotency coincide. Now assume that the claim is true for $n - 1$ and let $A$ be a two-sided skew brace such that $(A, \cdot)$ has nilpotency class $n$. Then $A/Z(A, \cdot)$ is still left nilpotent and its additive group has nilpotency class $n - 1$, so it is right nilpotent. Let $m$ be such that $A^{(m)} \subseteq Z(A, \cdot)$. From the assumption that $A$ is left nilpotent, we find that, in particular, the subbrace $Z(A, \cdot)$ is left, so also right, nilpotent. Let $k$ be such that $Z(A, \cdot)^{(k)} = \{0\}$. By Lemma 3.2.22 it follows that $A^{(mk)} = (A^{(m)})^{(k)} \subseteq Z(A, \cdot)^{(k)} = \{0\}$, so $A$ is right nilpotent.

A similar argument proves the implication from 2 to 1. □

**Theorem 3.2.24.** *Let $A$ be a two-sided skew brace that satisfies the equivalent conditions of Theorem 3.2.14. If $(A, \cdot)$ is nilpotent, then $(A, \circ)$ is nilpotent and $A$ is a strongly nilpotent skew brace.*

*Proof.* We will prove by induction on the nilpotency class $n$ of $(A, \cdot)$ that $A$ is right nilpotent. It then follows by Theorem 3.2.23 that $A$ is strongly nilpotent and by Proposition 1.1.25 that the group $(A, \circ)$ is nilpotent. For $n = 1$, the statement follows directly from Proposition 3.2.13. For $n > 1$, we know that $(A, \cdot)/Z(A, \cdot)$ has nilpotency class $n - 1$, so by the induction hypothesis there exists some $m$ such that $A^{(m)} \subseteq Z(A, \cdot)$. From the case $n = 1$, we know that $Z(A, \cdot)$ is right nilpotent hence $Z(A, \cdot)^{(k)} = \{0\}$ for an appropriate choice of $k$. It follows by Lemma 3.2.22 that

$$A^{(mk)} = (A^{(m)})^{(k)} \subseteq Z(A, \cdot)^{(k)} = \{0\},$$

so $A$ is right nilpotent. □

## 3.3 Prime and semiprime two-sided skew braces

In [107, 149], the following notions are introduced.

**Definition 3.3.1.** Let $A$ be a skew brace.

- $A$ is *prime* if $I * J \neq \{0\}$ for any non-zero ideals $I$ and $J$.
- $A$ is *strongly prime* if every $*$-product of any number of non-zero ideals is non-zero.
- $A$ is *semiprime* if $I * I \neq \{0\}$ for any non-zero ideal $I$.
- $A$ is *strongly semiprime* if every $*$-product of any number of copies of a non-zero ideal $I$ is non-zero.

For two-sided braces, both variations of (semi)primeness correspond with the usual notions for rings. At first sight, it is not clear whether every prime, respectively semiprime, skew brace is a strongly prime, respectively strongly semiprime, skew brace. In [16, Section 6], Ballester-Bolinches, Esteban-Romero, Jiménez-Seral and Pérez-Calabuig construct a brace $A$ of size 32 with a unique non-trivial ideal $I$. The ideal $I$ has size 16 and is non-trivial but $(I * I) * (I * I) = \{0\}$. Therefore, $A$ is prime but not strongly semiprime. In this section, we prove that both variations do coincide for two-sided skew braces.

**Lemma 3.3.2.** *Let $A$ be a two-sided skew brace and $X, Y$ subsets of $A$ which are normal in $(A, \circ)$. Then $X * Y$ is normal in $(A, \circ)$.*

*Proof.* Using Proposition 1.1.15 we find for arbitrary $a \in A$, $x \in X$, $y \in Y$,

$$a \circ (x * y) \circ \overline{a} = (a \circ x \circ \overline{a}) * (a \circ y \circ \overline{a}),$$

from which we conclude that $\{x * y \mid x \in X, y \in Y\}$ is a normal subset of $(A, \circ)$. Another application of Proposition 1.1.15 then implies that $X * Y$ is normal in $(A, \circ)$. □

**Lemma 3.3.3.** *Let $A$ be a skew left brace, $J$ a left ideal of $A$ and $X$ a normal subset of $(A, \circ)$. Then $X * J$ is a left ideal of $A$.*

*Proof.* This follows from the fact that for all $a, b, c \in A$ we have the equality

$$\lambda_a(b * c) = \lambda_a(\lambda_b(c) - c) = \lambda_{a \circ b \circ \overline{a}} \lambda_a(c) - \lambda_a(c) = (a \circ b \circ \overline{a}) * \lambda_a(c).$$ □

**Lemma 3.3.4.** *Let $A$ be a two-sided skew brace, and $I$ and $J$ ideals. If $J \cap A^2_{\mathrm{op}} = \{0\}$ or $J \subseteq A^2_{\mathrm{op}}$, then $I * J$ is an ideal of $A$.*

*Proof.* It follows from Lemma 3.3.2 and Lemma 3.3.3 that $I * J$ is a left ideal which is moreover normal in $(A, \circ)$. Therefore, it remains to show that $I * J$ is normal in $(A, \cdot)$. We treat the two cases separately.

Assume $J \cap A^2_{\mathrm{op}} = \{0\}$, so in particular $I *_{\mathrm{op}} J = \{0\}$. Then $x \circ y = y \cdot x$ or equivalently $x * y = x^{-1} \cdot y \cdot x \cdot y^{-1}$ for all $x \in I$, $y \in J$. We find that $I * J$ is in fact the additive commutator of the subgroups $(I, \cdot)$ and $(J, \cdot)$. As these subgroups are normal in $(A, \cdot)$, also their commutator is normal in $(A, \cdot)$.

Next, assume that $J \subseteq A^2_{\mathrm{op}}$ instead. Since $I * J$ is the additive group generated by the elements $x * y$, where $x \in I$, $y \in J$, it is sufficient to prove that $a^{-1} \cdot (x * y) \cdot a \in I * J$ for all $a \in A$. From Lemma 1.1.18 we find

$$0 = x * (a \cdot a^{-1}) = x * a \cdot a \cdot (x * (a^{-1})) \cdot a^{-1},$$

hence $x * (a^{-1}) = a^{-1} \cdot (x * a)^{-1} \cdot a$. Since $y, x * y \in A^2_{\mathrm{op}}$ and $x * a \in A^2$, it follows from Lemma 3.2.1 that $y$ and $x * y$ commute with $x * a$ with in the group $(A, \cdot)$. In combination with our prior observation and Lemma 1.1.18 we find

$$\begin{aligned} x * (a^{-1} \cdot y \cdot a) &= (x * (a^{-1})) \cdot a^{-1} \cdot (x * (y \cdot a)) \cdot a \\ &= a^{-1} \cdot (x * a)^{-1} \cdot (x * y) \cdot y \cdot (x * a) \cdot y^{-1} \cdot a \\ &= a^{-1} \cdot (x * y) \cdot a. \end{aligned}$$

□

**Theorem 3.3.5.** *Let $A$ be a two-sided skew brace. Then $A$ is semiprime if and only if it is strongly semiprime.*

*Proof.* It suffices to show the implication from left to right; we do so by contraposition. Assume that $A$ contains a non-zero ideal $I$ such that there exists a $*$-product of $n$ copies of $I$ which is zero. As a consequence of [107, Lemma 6.11] there exists some $n \geq 2$ such that $I_{(n)} = \{0\}$ where we define inductively $I_{(1)} = I$ and $I_{(k+1)} = I_{(k)} * I_{(k)}$ for $k \geq 1$.

If $I \cap A^2_{\mathrm{op}} = \{0\}$, then Lemma 3.3.4 implies that $I_k$ is an ideal for all $k \geq 1$, so in particular there exists some $k$ such that the ideal $I_k$ is non-zero and $I_k * I_k = \{0\}$. It follows that $A$ is not semiprime.

If instead $J = I \cap A^2_{\mathrm{op}} \neq \{0\}$, then $J_{(n)} \subseteq I_{(n)} = \{0\}$. Since it follows from Lemma 3.3.4 that $J_k$ is an ideal for each $k \geq 1$, we once again conclude that $A$ is not semiprime. □

**Theorem 3.3.6.** *Let $A$ be a two-sided skew brace. Then $A$ is prime if and only if it is strongly prime.*

*Proof.* We can restrict to proving the implication from left to right. Assume that $A$ is prime. If there exists a non-zero ideal $I$ such that $I \cap A^2_{\mathrm{op}} = \{0\}$, then $I * A^2_{\mathrm{op}} \subseteq I \cap A^2_{\mathrm{op}} = \{0\}$. So either $A^2_{\mathrm{op}} = \{0\}$ or all ideals intersect $A^2_{\mathrm{op}}$ non-trivially.

Assume that there exists a $*$-product $P$ of non-zero ideals of $A$ which is zero. If $A^2_{\mathrm{op}} = \{0\}$, so $A$ is almost trivial, then a $*$-product of two ideals is once again an ideal; this is easily seen directly or also follows from Lemma 3.3.4. In particular, at some point in $P$ the $*$-product of two non-zero ideals gives $\{0\}$ and therefore $A$ is not prime. If instead all ideals intersect $A^2_{\mathrm{op}}$ non-trivially, we can replace all the ideals appearing in $P$ by their intersection with $A^2_{\mathrm{op}}$ to obtain a new product $P'$ which is also zero. But from Lemma 3.3.4 we find that every $*$-product in $P'$ gives an ideal, and therefore we find a $*$-product of two non-zero ideals in $P'$ which is zero. □

Chapter 4

# Skew braces and the Yang–Baxter equation

Since (skew) braces were introduced precisely in order to provide an algebraic framework to study set-theoretical solutions of the Yang–Baxter equation, it is only natural that a major emphasis of current research is on the interplay between their respective properties. It is important to note that this question is ambiguous since there exist multiple ways to relate a skew brace to a solution and vice versa. Recall that starting from a solution $(X, r)$, one can construct its associated structure skew brace $G(X, r)$, or one can also look at the permutation skew brace $\mathcal{G}(X, r)$. Moreover, the image of the canonical map $X \to G(X, r)$ provides a cycle base of $G(X, r)$, and the same holds for $\mathcal{G}(X, r)$. The structure skew brace retains strictly more information about $(X, r)$ than the permutation skew brace does. Indeed, abelianity of the group $(G(X, r), \cdot)$ corresponds to involutivity of $(X, r)$, while this information is not always recoverable from $\mathcal{G}(X, r)$. Also, the results in [14, 64, 115] show that solely from the structure group $(G(X, r), \circ)$ of an involutive solution $(X, r)$ one can recover whether $(X, r)$ has finite multipermutation level. One equivalent characterization is that $(X, r)$ has finite multipermutation level if and only if $G(X, r)$ is poly-$\mathbb{Z}$. From a more practical point of view, however, it is often desirable to study $\mathcal{G}(X, r)$. One motivation might be that $\mathcal{G}(X, r)$ is finite whenever $(X, r)$ is finite. Another possible reason is that the class of skew braces that are isomorphic to a structure skew brace is quite scarce. For example, if a structure skew brace has an abelian additive group, then it is automatically free abelian. On the other hand, every skew brace appears as the permutation skew brace of a solution [11]. Conversely, given a skew brace $(A, \cdot, \circ)$ one can always consider the solution $(A, r_A)$ as described in Proposition 1.2.17, although this is often not the most desirable since for example $(A, r_A)$ is indecomposable only if $|A| = 1$. One gets more interesting behavior when restricting the solution $(A, r_A)$ to a cycle base $X \subseteq A$, but still only injective solutions can be obtained in this way. At last, the most general, but less straightforward way of obtaining solutions is by the construction given by Cedó, Jespers and Bachiller for braces [12] and extended by Bachiller to skew braces [11]. Recall that a specialized case of this construction was stated in Proposition 1.2.24. Their construction allows to obtain, for a given skew brace $(A, \cdot, \circ)$ and a cycle base $Y$, all solutions $(X, r)$ such that $\mathcal{G}(X, r) \cong (A, \cdot, \circ)$ and such that the cycle base given by the image of the canonical map $(X, r) \to \mathcal{G}(X, r)$ corresponds to $Y$ under this isomorphism. Moreover, given two solutions constructed from the same skew brace (with possibly different cycle bases), one has precise information on their isomorphisms, see also Proposition 1.2.25.

This chapter consists of four sections that each treat a different aspect of the interplay between solutions and skew braces: the multipermutation level, the relation between indecomposability and generators, the interplay between solutions and bi-skew braces, and automorphisms.

The property of having a finite multipermutation level behaves well with respect to all of the previous

connections between skew braces and solutions. This follows directly from results by Gateva-Ivanova and Cameron for the involutive case [78] and Cédo, Jespers, Kubat, Van Antwerpen and Verwimp for the general case [49]. Moreover, for $(X, r)$ an injective multipermutation solution, the multipermutation level of the structure skew brace $G(X, r)$ is precisely that of $(X, r)$. More generally,

$$\mathrm{mpl}(X, r) - 1 \leq \mathrm{mpl}(G(X, r) \leq \mathrm{mpl}(X, r).$$

Similarly, since trivially

$$\mathrm{mpl}(G(X, r)) - 1 \leq \mathrm{mpl}(\mathcal{G}(X, r)) \leq \mathrm{mpl}(G(X, r)),$$

one finds bounds relating the multipermutation level of $(X, r)$ and $\mathcal{G}(X, r)$. One can easily provide examples to show that these bounds cannot be made into a strict equality. In Theorem 4.1.10 we show that the multipermutation level of $\mathcal{G}(X, r)$ does accurately predict another numerical invariant of $(X, r)$, which is a slight variation of the multipermutation level. Here, instead of measuring how many times one has to retract a solution in order to get the one-element solutions, we measure how many retractions are necessary to get a trivial solution.

Starting from an indecomposable solution $(X, r)$, the induced cycle bases of $G(X, r)$ and $\mathcal{G}(X, r)$ are transitive cycle bases. Also, for the converse construction by Bachiller, Cédo and Jespers one needs a transitive cycle base in order to construct an indecomposable solution. From the work of Agata and Alicja Smoktunowicz [150] and Rump [136], it follows that a multipermutation brace admits a transitive cycle base if and only if it is one-generated as a brace. This does not hold without the assumption on the multipermutation level, as demonstrated in [136, Section 5]. In Proposition 4.2.3 we prove that a skew brace admits a transitive cycle base if and only if it is one-generated as a strong left ideal, where we do not require the skew brace to have finite multipermutation level. We then further obtain results on the impact of different types of nilpotency on how different notions of generating sets coincide in Theorems 4.2.5 and 4.2.9 and Proposition 4.2.13.

Bi-skew braces were introduced in the context of Hopf–Galois theory [61], but the question naturally arises whether this corresponds to a property of solutions. This question, from multiple points of view, is the main topic of Section 4.3. In Proposition 4.3.2 we characterize when a skew brace $(A, \cdot, \circ)$ is a bi-skew brace using only the solution $(A, r_A)$. In the other direction, in Theorem 4.3.4 we provide a precise criterion for when $G(X, r)$ is a bi-skew brace when $(X, r)$ is an injective solution. However, in Example 4.3.3 we show that given a bi-skew brace $(A, \cdot, \circ)$ there is no direct relation between the solutions $(A, r_A)$ and $(A, r_{A_\leftrightarrow})$.

In the literature, not many general results are known about the automorphism group $\mathrm{Aut}(X, r)$ of a solution $(X, r)$. The most prominent results were obtained by Jedlička, Pilitowska and Zamojska-Dzienio in [90] and Jedlička and Pilitowska in [88] in the case of indecomposable involutive solutions of multipermutation level 2. For such solutions $(X, r)$ we know that their automorphism group acts regularly on $X$ and if moreover the permutation group $\mathcal{G}(X, r)$ is abelian, then so is $\mathrm{Aut}(X, r)$. In [90], Jedlička, Pilitowska and Zamojska-Dzienio also obtained intriguing results on homomorphisms and endomorphisms of indecomposable involutive solutions of multipermutation level 2. We start the last section of this chapter by proving Theorem 4.4.1, which states that an indecomposable multipermutation solution contains no non-trivial subsolutions. This then allows us to extend the earlier-mentioned results on endomorphisms and homomorphisms to arbitrary permutation levels and without restrictions on the permutation group. At last, we give a first attempt at a systematic study of the automorphism group of indecomposable involutive solutions. From the earlier mentioned results by Bachiller, Cédo and Jespers we deduce an explicit description of the automorphism group of such solutions $(X, r)$ in terms of automorphisms of $\mathcal{G}(X, r)$ that map its canonical transitive cycle base to itself. To any brace $A$ with transitive cycle base $Y$ and $x \in Y$ we associate a group $S_A(x)$, which coincides with the automorphism group of the uniconnected solution arising

from the brace $A$ and the element $x$. In Proposition 4.4.8 we prove that the automorphism group of any indecomposable involutive solution $(X, r)$ obtained starting from $A$ and $x$ through Proposition 1.2.24 is a quotient of a subgroup of $S_A(x)$. We then further specialize to solutions that have multipermutation 2 or whose permutation group is cyclic and obtain our main results which relate $\mathrm{Aut}(X, r)$ to the additive group of the permutation brace $\mathcal{G}(X, r)$, this is achieved in Theorems 4.4.14 and 4.4.23.

All results in this chapter for which no external reference is given are novel. Those in Sections 4.1, 4.2 and 4.4 were obtained in collaboration with Marco Castelli and appear in the preprint [45]. One should note that the contents of Section 4.4 differ from how they appear in [45, Section 6] since, in the meantime, improved results have been obtained. The results in Section 4.3 were obtained in collaboration with Lorenzo Stefanello and have been published in [154].

## 4.1 A variation of the multipermutation level

**Definition 4.1.1.** Let $(X, r)$ be a multipermutation solution. We define $\mathrm{mpl}'(X, r)$ as the smallest $n \geq 1$ such that $\mathrm{Ret}^n(X, r)$ is a trivial solution, possibly of size $> 1$.

If $(X, r)$ is a multipermutation solution, then $\mathrm{Ret}^{\mathrm{mpl}(X,r)}(X, r)$ has size 1 and is therefore trivial. Also note that any solution $(X, r)$ for which there exists some $n$ such that $\mathrm{Ret}^n(X, r)$ is a trivial solution, is a multipermutation solution as then $\mathrm{Ret}^{n+1}(X, r)$ has size 1. This proves the following result.

**Lemma 4.1.2.** *Let $(X, r)$ be a multipermutation solution. Then*

$$\mathrm{mpl}'(X, r) \leq \mathrm{mpl}(X, r) \leq \mathrm{mpl}'(X, r) + 1. \tag{4.1}$$

**Proposition 4.1.3.** *Let $(X, r)$ be an indecomposable multipermutation solution. Then $\mathrm{mpl}'(X, r)$ and $\mathrm{mpl}(X, r)$ are equal.*

*Proof.* Let $n$ be such that $\mathrm{Ret}^n(X, r)$ is a trivial solution. As indecomposability is preserved under retraction, $\mathrm{Ret}^n(X, r)$ is also indecomposable and thus $|\mathrm{Ret}^n(X, r)| = 1$. □

**Proposition 4.1.4.** *Let $(X, r)$ be a multipermutation solution with $|X| > 1$ and such that for every $x \in X$, there exist $y, y' \in X$ such that $\sigma_y(x) = x$ and $\tau_{y'}(x) = x$. Then $\mathrm{mpl}(X, r) = \mathrm{mpl}'(X, r) + 1$.*

*Proof.* Let $n = \mathrm{mpl}(X, r)$. As $|X| > 1$, we know that $n > 1$, hence $\mathrm{Ret}^{n-1}(X, r)$ is well-defined and must be a permutation solution on a set of size more than 1. The condition on $(X, r)$ is preserved under retractions, and a permutation solution satisfying this condition is necessarily trivial. It follows that $\mathrm{Ret}^{n-1}(X, r)$ is a trivial solution and $\mathrm{mpl}'(X, r) \leq n - 1$, and therefore the statement follows in combination with Lemma 4.1.2. □

*Remark* 4.1.5. The condition appearing in Proposition 4.1.4 is a natural generalization of condition $(*)$ appearing in [78, Definition 4.3] for involutive solutions. Note that solutions $(X, r)$ such that $r(x, x) = (x, x)$ for all $x \in X$, the so-called *square-free solutions*, satisfy this condition. Also, for any skew brace $A$, the solution $(A, r_A)$ satisfies the condition since $\sigma_0 = \tau_0 = \mathrm{id}$.

The first part of the following result appears as [49, Proposition 4.8]; for completeness' sake, we give a full proof.

**Lemma 4.1.6.** *Let $f : (X, r) \to (Y, s)$ be a surjective homomorphism of solutions. Then $f$ induces a surjective homomorphism of solutions $\overline{f} : \mathrm{Ret}(X, r) \to \mathrm{Ret}(Y, s)$. If $(X, r)$ is a multipermutation solution, then so is $(Y, s)$ and moreover $\mathrm{mpl}(Y, s) \leq \mathrm{mpl}(X, r)$ and $\mathrm{mpl}'(Y, s) \leq \mathrm{mpl}'(X, r)$.*

*Proof.* Let $f : (X, r) \to (Y, s)$ be a surjective homomorphism of solutions. If $\sigma_x = \sigma_y$ for $x, y \in X$, then also

$$\sigma_{f(x)}(f(z)) = f(\sigma_x(z)) = f(\sigma_y(z)) = \sigma_{f(y)}(f(z)),$$

for all $z \in X$. Since $f$ is surjective, this implies $\sigma_{f(x)} = \sigma_{f(y)}$ and thus $f$ indeed induces a surjective homomorphism of solutions $\overline{f} : \mathrm{Ret}(X, r) \to \mathrm{Ret}(Y, s)$. Repeatedly applying this construction yields surjective maps $\mathrm{Ret}^n(X, r) \to \mathrm{Ret}^n(Y, s)$ for all $n \geq 1$. Since these maps are surjective, we find that if $\mathrm{Ret}^n(X)$ has size 1 then so does $\mathrm{Ret}^n(Y)$, and similarly if $\mathrm{Ret}^n(X)$ is trivial then so is $\mathrm{Ret}^n(Y)$. □

**Corollary 4.1.7.** *Let $(X, r)$ be a multipermutation solution. Then*

$$\mathrm{mpl}(X, r) - 1 \leq \mathrm{mpl}\,\mathrm{Inj}(X, r) \leq \mathrm{mpl}(X, r),$$
$$\mathrm{mpl}'(X, r) - 1 \leq \mathrm{mpl}'\,\mathrm{Inj}(X, r) \leq \mathrm{mpl}'(X, r).$$

*Proof.* If we apply Lemma 4.1.6 to the surjective homomorphisms

$$(X, r) \to \mathrm{Inj}(X, r) \to \mathrm{Ret}(X, r),$$

we obtain

$$\mathrm{mpl}(\mathrm{Ret}(X, r)) \leq \mathrm{mpl}(\mathrm{Inj}(X, r)) \leq \mathrm{mpl}(X, r).$$

It then suffices to note that the inequality $\mathrm{mpl}(X, r) \leq \mathrm{mpl}(\mathrm{Ret}(X, r)) + 1$ holds. The second part of the statement follows analogously. □

**Proposition 4.1.8.** *Let $A$ be a skew brace and $(X, r)$ a cycle base of $A$. Then $\mathcal{G}(X, r) \cong \mathrm{Ret}(A)$.*

*Proof.* The universal property of $G(X, r)$, see Theorem 1.2.21, yields a surjective skew brace homomorphism

$$f : G(X, r) \to A,$$

which is injective on the set of generators $X$. We claim that $f^{-1}(\mathrm{Soc}(A)) = \Gamma$, with $\Gamma$ the kernel of the canonical skew brace homomorphism $\pi : G(X, r) \to \mathcal{G}(X, r)$, from which the statement then follows. Since $(X, r)$ is injective, we find $\Gamma = \mathrm{Soc}(G(X, r))$. From the surjectivity of $f$ we get $f(\mathrm{Soc}(G(X, r))) \subseteq \mathrm{Soc}(A)$ and thus $\Gamma \subseteq f^{-1}(\mathrm{Soc}(A))$. Now to prove the inverse inclusion, let $g \in \mathcal{G}(X, r) \setminus \mathrm{Soc}(G(X, r))$. As $X$ is a cycle base of $G(X, r)$ there exist some $x, y \in X$, $x \neq y$, such that $\theta_{(g,0)}(x) = y$ or $\theta_{(0,g)}(x) = y$. As $f(x) \neq f(y)$, this implies that $f(g) \notin \mathrm{Soc}(A)$ and this proves the remaining inclusion. □

**Corollary 4.1.9.** *Let $(X, r)$ be a solution. Then $\mathcal{G}(\mathrm{Ret}(X, r)) \cong \mathrm{Ret}(\mathcal{G}(X, r))$.*

*Proof.* Let $(X, r)$ be a solution, then we know that the canonical image of $X$ in $\mathcal{G}(X, r)$ is a cycle base isomorphic to $\mathrm{Ret}(X, r)$. Proposition 4.1.8 now yields that $\mathcal{G}(\mathrm{Ret}(X, r)) \cong \mathrm{Ret}(\mathcal{G}(X, r))$. □

We now obtain the main result of this section.

**Theorem 4.1.10.** *Let $(X, r)$ be a multipermutation solution. Then $\mathrm{mpl}'(X, r)$ equals $\mathrm{mpl}(\mathcal{G}(X, r))$.*

*Proof.* From Corollary 4.1.9, we find that in general $\mathcal{G}(\mathrm{Ret}^n(X, r)) \cong \mathrm{Ret}^n(\mathcal{G}(X, r))$ for all $n \geq 0$. Note that a solution is trivial if and only if its permutation skew brace is the zero brace, from which the equality follows. □

As the multipermutation level of a solution $(X, r)$ can vary between $\mathrm{mpl}'(X, r)$ and $\mathrm{mpl}'(X, r) + 1$, there is no general way to express $\mathrm{mpl}(\mathcal{G}(X, r))$ directly in terms of $\mathrm{mpl}(X, r)$. This shows the main advantage of $\mathrm{mpl}'(X, r)$ over $\mathrm{mpl}(X, r)$. If $(X, r)$ is indecomposable, we obtain the following result from Proposition 4.1.3.

**Corollary 4.1.11.** *Let $(X, r)$ be an indecomposable multipermutation solution. Then $\mathrm{mpl}(X, r)$ equals $\mathrm{mpl}(\mathcal{G}(X, r))$.*

**Theorem 4.1.12.** *Let $(X, r)$ be a multipermutation solution with $|X| > 1$. Then*

$$\mathrm{mpl}(G(X, r)) - 1 \leq \mathrm{mpl}'(X, r) \leq \mathrm{mpl}(G(X, r))$$

*If moreover $(X, r)$ is injective, then $\mathrm{mpl}'(X, r) + 1 = \mathrm{mpl}(G(X, r))$.*

*Proof.* If $(X, r)$ is injective, then $\mathcal{G}(X, r) = \mathrm{Ret}(G(X, r))$, hence the second part of the statement follows from Theorem 4.1.10. The first part now follows from Corollary 4.1.7 and the fact that $G(X, r) = G(\mathrm{Inj}(X, r))$. □

As a consequence, we find the following generalization of [49, Corollary 4.16] and [78, Theorem 5.15].

**Corollary 4.1.13.** *Let $(X, r)$ be an injective multipermutation solution. Then*

$$\mathrm{mpl}(G(X, r)) - 1 \leq \mathrm{mpl}(X, r) \leq \mathrm{mpl}(G(X, r)).$$

*If moreover, $(X, r)$ satisfies the condition of Proposition 4.1.4 then $\mathrm{mpl}(X, r) = \mathrm{mpl}(G(X, r))$.*

*Proof.* The first part is a direct consequence of Lemma 4.1.2 and Theorem 4.1.12. The second part follows from Proposition 4.1.4 and Theorem 4.1.12. □

## 4.2 Cycle bases and generators of skew braces

Let a skew brace $A$ be given. We start by showing that the existence of a transitive cycle base, or more generally, the minimal number of orbits in a cycle base, can be studied in terms of generators of strong left ideals.

**Definition 4.2.1.** Let $A$ be a skew brace. For a set $X \subseteq A$, the skew subbrace (respectively strong left ideal or ideal) of $A$ generated by $X$ is the smallest skew subbrace (respectively strong left ideal or ideal) of $A$ containing $X$. If $A$ has a singleton generating set as a skew brace (respectively strong left ideal or ideal), then we say that $A$ is *one-generated* as a skew brace (respectively strong left ideal or ideal).

Recall that the $\theta$-action of a skew brace was defined in Lemma 1.2.32.

**Lemma 4.2.2.** *Let $A$ be a skew brace and $X \subseteq A$. The strong left ideal generated by $X$, denoted by $I_{sl}(X)$, is the subgroup of $(A, \cdot)$ generated by*

$$S = \{\theta_{(a,b)}(x) \mid x \in X, a, b \in A\}.$$

*Proof.* As a direct consequence of the definition of $\theta$, a subgroup of $(A, \cdot)$ is a strong left ideal if and only if it is invariant under the $\theta$-action. It then follows that $S$ is contained in any strong left ideal containing $X$. Since $\theta$ acts by additive automorphisms, the subgroup of $(A, \cdot)$ generated by $S$ is invariant under the $\theta$-action hence it is a strong left ideal. □

From Lemma 4.2.2 we immediately obtain the following result, which lets us translate the question "What is the minimal number of orbits contained in a cycle base of $A$?" to "What is the minimal number of elements that generate $A$ as a strong left ideal?"

**Proposition 4.2.3.** *Let $A$ be a non-zero skew brace. If $X$ is a cycle base of $A$ and $Y$ is a set of representatives of the orbits in $X$, then $Y$ generates $A$ as a strong left ideal. Conversely, if $Y \subseteq A$ generates $A$ as a strong left ideal, then the union of the orbits of elements in $Y$ forms a cycle base of $A$.*

**Corollary 4.2.4.** *Let $A$ be a skew brace. If $X$ is a transitive cycle base of $A$, then every element of $X$ generates $A$ as a strong left ideal.*

Motivated by the above, in the remainder of this section, we study the relation between the generators of $A$ as a skew brace, strong left ideal and ideal. Inspired by results in [136, 145] we first consider multipermutation skew braces. Later, also left nilpotency or annihilator nilpotency appear as a natural assumption. This first result extends [145, Theorem 5.4] and [136, Proposition 10].

**Theorem 4.2.5.** *Let $A$ be a multipermutation skew brace. If $X$ generates $A$ as a strong left ideal, then $X$ generates $A$ as a skew brace.*

*Proof.* We will prove this claim by induction on the multipermutation level of $A$. If $A$ is a trivial brace, then the claim clearly holds. Now assume that $A$ is not a trivial brace and let $A(X)$ denote the skew subbrace of $A$ generated by $X$. The induction hypothesis implies that $A = A(X) \cdot \mathrm{Soc}(A)$. As $X$ generates $A$ as a strong left ideal, we know that $A = I_{sl}(X)$ with $I_{sl}(X)$ as in Lemma 4.2.2. For any $a, b \in A$, we can write $a = a_1 \cdot a_2$ and $b = b_1 \cdot b_2$ with $a_1, b_1 \in A(X)$ and $a_2, b_2 \in \mathrm{Soc}(A)$. This then implies that $\theta_{(a,b)}(x) = \theta_{(a_1,b_1)}(x) \in A(X)$ for all $x \in X$ and therefore $A = I_{sl}(X) \subseteq A(X)$. □

**Corollary 4.2.6.** *Let $A$ be a multipermutation skew brace. The following are equivalent:*

1. *$A$ is one-generated as a skew brace,*

2. *$A$ is one-generated as a strong left ideal.*

*In particular, if $x \in A$ generates $A$ as a strong left ideal, then it generates $A$ as a skew brace.*

Next, we study the relation between sets that generate a skew brace as an ideal and as a strong left ideal. The following result by Jespers, Kubat, Van Antwerpen and Verwimp [91] gives a nice way to determine the minimal number of generators as an ideal, for a large class of skew braces. For a skew brace $A$, we let $\omega(A)$ be the minimal (possibly infinite) number of generators of $A$ as an ideal. A skew brace satisfies the *descending chain condition (DCC)* on ideals if there exists no infinite strictly descending chain of ideals.

**Theorem 4.2.7.** *Let $A$ be a skew brace with $\omega(A) < \infty$ and satisfying the DCC on ideals. Then*

$$\omega(A) = \omega(A/A^2) = \omega(A/A').$$

The following example shows that, in general, it is not true that if a skew brace is one-generated as an ideal, then it is also one-generated as a strong left ideal. If we want such a result to hold, we thus need to impose extra conditions on $A$.

**Example 4.2.8.** Let $A = \mathrm{Triv}(\mathbb{Z}/p \times \mathbb{Z}/p)$ and $B = \mathrm{Triv}(\mathbb{Z}/2)$ for some odd prime $p$ and consider the semidirect product $C = A \rtimes B$, where $A$ acts by inversion. Explicitly,

$$\begin{aligned}(n,m,l) + (n',m',l') &= (n+n', m+m', l+l')\\ (n,m,l) \circ (n',m',l') &= (n+(-1)^l n', m+(-1)^l m', l+l')\\ \lambda_{(n,m,l)}(n',m',l') &= ((-1)^l n', (-1)^l m', l').\end{aligned}$$

Then we find that $C^2 = C' = A$ and thus $(C/C', +) \cong \mathbb{Z}/2$ is cyclic, from which it follows that $\omega(A) = 1$ by Theorem 4.2.7. We claim that $C$ is not one-generated as a strong left ideal. If it were, then the image of this generator should generate $C/C^2$, hence it is of the form $(1, l, m)$, with $l, m \in \mathbb{Z}/p$. However, for any choice of $l, m \in \mathbb{Z}/p$, the set $\{(n, rm, rl) \mid n \in \mathbb{Z}/2, r \in \mathbb{Z}/p\}$ is a strong left ideal which contains $(1, l, m)$ and which has index $p$. Thus $C$ is not one-generated as a strong left ideal.

**Theorem 4.2.9.** *Let $A$ be a left nilpotent skew brace and $X$ a subset of $A$. If the image of $X$ in $A/A^2$ generates $A/A^2$ as a strong left ideal, then $X$ generates $A$ as a strong left ideal.*

*Proof.* Let $I = I_{sl}(X)$ denote the strong left ideal of $A$ generated by $X$. By induction on $n$, we will prove that $I \cdot A^n = A$, which then implies the statement. As the natural image of $X$ in $A/A^2$ generates $A/A^2$ as a strong left ideal, we find that $I \cdot A^2 = A$. Now let $n \geq 2$ and assume that $I \cdot A^n = A$. Recall from Lemma 1.1.18 that for all $a, b, c \in A$ we have that $a * (b \cdot c) = (a * b) \cdot b \cdot (a * c) \cdot b^{-1}$, so we find

$$A^2 = A * (I \cdot A^n) = A * (A^n \cdot I) \subseteq A^{n+1} \cdot I.$$

We know already that $I \cdot A^2 = A$, thus $A \subseteq I \cdot A^{n+1}$. □

**Corollary 4.2.10.** *Let $A$ be a left nilpotent skew brace of finite weight satisfying the DCC on ideals. The minimal number of generators of $A$ as a strong left ideal coincides with $\omega(A)$.*

*Proof.* It suffices to prove that $A$ is generated as a strong left ideal by $\omega(A)$ elements. From Theorem 4.2.7 we know that $\omega(A) = \omega(A/A^2)$. As every strong left ideal in $A/A^2$ is an ideal, $\omega(A/A^2)$ is also the minimal numbers of generators of $A/A^2$ as a strong left ideal and by Theorem 4.2.9 we thus obtain a generating set of size $\omega(A)$ which generates $A$ as a strong left ideal. □

**Corollary 4.2.11.** *Let $A$ be a left nilpotent skew brace such that $A$ satisfies the DCC on ideals. Then the following are equivalent:*

1. *$A$ is one-generated as a strong left ideal,*
2. *$A$ is one-generated as an ideal,*
3. *$(A/A', +)$ is cyclic.*

*Proof.* The equivalence of 1 and 2 is clear from Corollary 4.2.10. The equivalence of 2 and 3 follows from Theorem 4.2.7. □

**Lemma 4.2.12.** *Let $A$ be a skew brace such that $(A/A', +)$ is cyclic and $(A, +)$ or $(A, \circ)$ is nilpotent. Then $A^2 = A'$.*

*Proof.* Under the imposed conditions, the group $(A/A^2, \cdot) = (A/A^2, \circ)$ is nilpotent. Also, its abelianization is isomorphic to $(A/A', \cdot)$, hence it is cyclic. It is a well-known result in group theory that this implies that $(A^2, \cdot)$ itself is cyclic. In particular, $A/A^2$ is a trivial brace, hence $A' \subseteq A^2$. □

**Proposition 4.2.13.** *Let $A$ be an annihilator nilpotent skew brace that satisfies the DCC on ideals. Then the following are equivalent:*

1. *$A$ is one-generated as a skew brace,*
2. *$A$ is one-generated as a strong left ideal,*
3. *$A$ is one-generated as an ideal,*
4. *$(A/A^2, \cdot)$ is cyclic.*

*In this case, the following are equivalent for an element $x \in X$:*

1. *$x$ generates $A$ as a skew brace,*
2. *$x$ generates $A$ as a strong left ideal,*
3. *$x$ generates $A$ as an ideal,*
4. *$x + A^2$ generates $(A/A^2, \cdot)$.*

*Proof.* The first part is a consequence of Corollary 4.2.6, Corollary 4.2.11 and Lemma 4.2.12.
The second part now follows if we also take into account Theorem 4.2.9. □

The first part of Proposition 4.2.13 generalizes [137, Corollary 1]. In the same paper, in Proposition 5, Rump showed that for one-generated braces with an abelian multiplicative group, the transitive cycle bases are precisely the cosets of $A^2$ that generate $A/A^2$. Since a finite brace with an abelian multiplicative group is, in particular, annihilator nilpotent, one might expect that a similar result holds for this class. The following example shows that even skew braces that are very similar to this class, namely annihilator nilpotent braces and annihilator nilpotent skew braces with an abelian permutation group, do not exhibit a similar feature.

**Example 4.2.14.** Let $(A, +) = (\mathbb{Z}/p)^n$, for $p$ a prime and $n < p$ and let $\phi \in \mathrm{Aut}(A, +)$ be the automorphism given by the Jordan normal block of size $n$, where we consider $(\mathbb{Z}/p)^n$ as column vectors. Let $\lambda : (A, +) \to \mathrm{Aut}(A, +)$ be given by $(a_1, \ldots, a_n) \mapsto \phi^{a_n}$. In particular, we find that

$$\ker \lambda = (\mathbb{Z}/p)^{n-1} \times \{0\} = \{\phi(a) - a \mid a \in A\}.$$

From Theorem 2.4.5 we find a bi-skew brace $(A, +, \circ)$ where $a \circ b = a + \lambda_a(b)$. A direct verification shows that $(A, \circ)$ is abelian if and only if $n = 2$. Note that $A$ is right nilpotent of class 2 since it is a bi-skew brace. It is left nilpotent by Theorem 1.1.24 as it is of prime power size, hence $A$ is annihilator nilpotent. As $(A, \circ)/\ker \lambda$ is cyclic of order $p$, we see that all transitive cycle bases have size $p$. Because $|A^2| = p^{n-1}$, the transitive cycle bases are cosets of $A^2$ if and only if $n = 2$, in this case $(A, \circ)$ is abelian.

**Example 4.2.15.** For any choice of a prime $p$ and $n < p$, the skew brace $(A, +, \circ)$ from Example 4.2.14 is a bi-skew brace, so we can also consider the skew brace $(A, \circ, +)$, which is still annihilator nilpotent. Now its multiplicative group is always abelian and its additive group is abelian if and only if $n = 2$. As the $\lambda$-map of an element $a \in A$ in this skew brace is given by $\lambda_a^{-1}$ and $(A, \circ, +)^2 = (A, +, \circ)^2$, we have the same conclusion as in the previous case: it is only true that the transitive cycle bases of $(A, \circ, +)$ are cosets of $(A, \circ, +)^2$ if $n = 2$. In this case, $A$ is a brace.

## 4.3 Bi-skew braces and solutions of the Yang–Baxter equation

**Proposition 4.3.1.** *Let $A$ be a skew brace. Then $A$ is a bi-skew brace if and only if for all $a, b \in A$,*

$$\lambda_{\lambda_a^{\mathrm{op}}(b)} = \lambda_b. \tag{4.2}$$

*Proof.* If $A$ is a bi-skew brace, then the assertion follows from Theorem 1.1.34. For the other implication, suppose that (4.2) holds. For all $a, b \in A$, we have

$$\lambda_{a\cdot b} = \lambda_{b\circ\lambda_{\overline{b}}^{\mathrm{op}}(a)} = \lambda_b\lambda_{\lambda_{\overline{b}}^{\mathrm{op}}(a)} = \lambda_b\lambda_a.$$

Hence, again by Theorem 1.1.34, $A$ is a bi-skew brace. □

The following is a straightforward corollary. Recall that for a skew brace $A$, we always have a natural solution $(A, r_A)$ as described in Proposition 1.2.17 and the solution associated to $A_{\mathrm{op}}$ is the inverse of that of $A$, see Example 1.2.20.

**Proposition 4.3.2.** *Let $A$ be a skew brace. Then $A$ is a bi-skew brace if and only if its associated solution $(A, r_A)$ satisfies, for all $x, y \in A$,*

$$\sigma_{\hat{\sigma}_x(y)} = \sigma_y.$$

As a result, the information whether $A$ is a bi-skew brace is not lost when one only considers its associated solution. Next, it is natural to ask whether, if we know that $A$ is a bi-skew brace, it is possible to recover the associated solution of $A_{\leftrightarrow}$ from the associated solution of $A$. The following example shows that this is, in general, not possible, as we construct non-isomorphic bi-skew braces $A$ and $B$ such that the associated solutions are isomorphic, but the solutions associated to $A_{\leftrightarrow}$ and $B_{\leftrightarrow}$ are not isomorphic.

**Example 4.3.3.** Let $(G, \cdot) = C_2 \times C_8$, with $C_2 = \langle x \rangle$, and let $\alpha\colon C_2 \to \mathrm{Aut}(G)$ be the group homomorphism mapping $x$ to the inversion automorphism of $G$. Then, as in Example 2.2.6 we find a bi-skew brace $A = \mathrm{Triv}(G) \rtimes \mathrm{Triv}(C_2)$, whose associated solutions are as follows:

$$\begin{aligned} r_A((g, x^i), (h, x^j)) &= ((\alpha_x^i(h), x^j), (\alpha_x^j(g), x^i)), \\ r_{A_\leftrightarrow}((g, x^i), (h, x^j)) &= ((\alpha_x^i(h), x^j), (g \cdot h \cdot \alpha_x^i(h^{-1}), x^i)). \end{aligned}$$

In particular, $\tau_{\leftrightarrow,(h,x^j)}(g, 1) = (g, 1)$ and $\tau_{\leftrightarrow,(h,x^j)}(g, x) = (g \cdot h^2, x)$. Here $\tau_{\leftrightarrow}$ is the usual $\tau$-map associated with the solution $(A, r_{A_\leftrightarrow})$. Note that if $h \in G$ is an element of order 8, then $\tau_{\leftrightarrow,(h,x^j)}$ has order 4.

Now take $(H, \cdot) = C_2^4$, and let $\beta\colon C_2 \to \mathrm{Aut}(H)$, where still $C_2 = \langle x \rangle$, be the map which sends $x$ to the automorphism interchanging the first two and the last two coordinates of $H$. In the same way as before, we then obtain a bi-skew brace $B = \mathrm{Triv}(H) \rtimes \mathrm{Triv}(C_2)$, and two associated solutions:

$$\begin{aligned} r_B((g, x^i), (h, x^j)) &= ((\beta_x^i(h), x^j), (\beta_x^j(g), x^i)), \\ r_{B_\leftrightarrow}((g, x^i), (h, x^j)) &= ((\beta_x^i(h), x^j, ), (g \cdot h \cdot \beta_x^i(h), x^i)). \end{aligned}$$

In this case once again, we find that $\tau_{\leftrightarrow,(h,x^j)}(g, 1) = (g, 1)$ and $\tau_{\leftrightarrow,(h,x^j)}(g, x) = (g \cdot h \cdot \beta_x^i(h), x)$. Since $h \cdot \beta_x^i(h)$ has either order 1 or 2, it follows that all $\tau$-maps associated to $r_{B_\leftrightarrow}$ have either order one or two. Therefore, $r_{A_\leftrightarrow}$ can not be isomorphic to $r_{B_\leftrightarrow}$.

On the other hand, the cycle structures of $\alpha_x$ and $\beta_x$ are the same; they are both of order two and fix four points. Therefore, there exists a bijection $\theta\colon G \to H$ such that $\theta\alpha_x = \beta_x\theta$, and in particular the bijection

$$C_2 \times G \to C_2 \times H, \quad (x^i, g) \mapsto (x^i, \theta(g))$$

gives an isomorphism between the solutions $r_A$ and $r_B$.

We now deal with the inverse situation, where we start with a given solution and ask whether the skew brace on the structure group is a bi-skew brace.

**Theorem 4.3.4.** *Let $(X, r)$ be an injective solution. Then $G(X, r)$ is a bi-skew brace if and only if $\sigma_{\hat{\sigma}_x(y)} = \sigma_y$ for all $x, y \in X$.*

*Proof.* The implication from left to right is a consequence of Proposition 4.3.2 and the fact that $(X, r)$ is injective.

Now assume that for all $x, y \in X$, we have that $\sigma_{\hat{\sigma}_x(y)} = \sigma_y$. This means that $\lambda_{\lambda^{\mathrm{op}}_x(y)} = \lambda_y$ where $x, y$ are now considered as the generators of $G(X, r)$ and $\lambda$ and $\lambda^{\mathrm{op}}$ are the $\lambda$-maps associated to $G(X, r)$ and $G(X, r)_{\mathrm{op}}$ respectively. In particular, as $X$ generates the multiplicative group $(G(X, r), \circ)$, it follows that $\lambda_{\lambda^{\mathrm{op}}_g(y)} = \lambda_y$ for all $g \in G(X, r)$.

For a word $w = x_1^{\epsilon_1} \cdot \ldots \cdot x_n^{\epsilon_n}$ with $x_i \in X$ and $\epsilon_i \in \{-1, 1\}$, we will prove that

$$\lambda_w = \lambda_{x_n}^{\epsilon_n} \ldots \lambda_{x_1}^{\epsilon_1}.$$

As $(G(X, r), \cdot)$ is generated by $X$, this then proves that

$$\lambda \colon (G(X, r), \cdot) \to \mathrm{Aut}(G(X, r), \cdot)$$

is a group antihomomorphism, and therefore $G(X, r)$ is a bi-skew brace. We will 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 $\lambda_{x^{-1}} = \lambda_x^{-1}$ for all $x \in X$. For this, we note that there is the equality

$$\lambda_a^{\mathrm{op}}(\overline{a}) = (a \circ \overline{a}) \cdot a^{-1} = a^{-1},$$

or equivalently, $\overline{(\lambda_a^{\mathrm{op}})^{-1}(a^{-1})} = a$, so substituting $a$ by $x^{-1}$ we find $\overline{(\lambda_{x^{-1}}^{\mathrm{op}})^{-1}(x)} = x^{-1}$, thus

$$\lambda_{x^{-1}} = \lambda_{\overline{(\lambda_{x^{-1}}^{\mathrm{op}})^{-1}(x)}} = \lambda^{-1}_{(\lambda_{x^{-1}}^{\mathrm{op}})^{-1}(x)} = \lambda_x^{-1}.$$

Now assume that the statement holds for words of length $n - 1$, and let $w = x_1^{\epsilon_1} \cdot \ldots \cdot x_n^{\epsilon_n}$ be a word of length $n$. If we write $v = x_2^{\epsilon_2} \cdot \ldots \cdot x_n^{\epsilon_n}$, then

$$\begin{aligned}
\lambda_w &= \lambda_{v \circ \lambda_v^{\mathrm{op}}(x_1^{\epsilon_1})} \\
&= \lambda_v \lambda_{\lambda_v^{\mathrm{op}}(x_1^{\epsilon_1})} \\
&= \lambda_{x_n}^{\epsilon_n} \ldots \lambda_{x_2}^{\epsilon_2} \lambda^{\epsilon_1}_{\lambda_v^{\mathrm{op}}(x_1)} \\
&= \lambda_{x_n}^{\epsilon_n} \ldots \lambda_{x_2}^{\epsilon_2} \lambda_{x_1}^{\epsilon_1}.
\end{aligned}$$

□

**Corollary 4.3.5.** *Let $(X, r)$ be a solution such that $\sigma_{\hat{\sigma}_x(y)} = \sigma_y$ for all $x, y \in X$. Then $G(X, r)$ is a bi-skew brace.*

*Proof.* As $\mathrm{Inj}(X, r)$ is a homomorphic image of $(X, r)$, it follows that $\mathrm{Inj}(X, r)$ still has the property that $\sigma_{\hat{\sigma}_x(y)} = \sigma_y$ for all $x, y \in \mathrm{Inj}(X, r)$. Because $G(X, r)$ and $G(\mathrm{Inj}(X, r))$ are isomorphic skew braces, the result follows from Theorem 4.3.4. □

Recall from Theorem 2.2.1 that a brace $A$ is $\lambda$-homomorphic (or equivalently, a bi-skew brace) if and only if it is right nilpotent of class at most 2. The latter is in turn equivalent to $\mathrm{mpl}(A) \leq 2$.

**Proposition 4.3.6.** *Let $(X, r)$ be an involutive solution. Then*

1. *$G(X,r)$ is a bi-skew brace if and only if* $\mathrm{mpl}'(X,r) \leq 1$,

2. *$\mathcal{G}(X,r)$ is a bi-skew brace if and only if* $\mathrm{mpl}'(X,r) \leq 2$.

*Proof.* We know that a brace $A$ is a bi-skew brace if and only if it is multipermutation of level at most 2. The statement then follows when combined with Theorem 4.1.10 and the fact that $\mathrm{mpl}(G(X,r)) = \mathrm{mpl}(\mathcal{G}(X,r)) + 1$. □

## 4.4 Automorphisms of solutions

### 4.4.1 Multipermutation solutions

**Theorem 4.4.1.** *Let $(X,r)$ be an indecomposable solution of finite multipermutation level. Then $(X,r)$ contains no non-trivial subsolutions.*

*Proof.* Let us prove this by induction on the multipermutation level of the solutions. If $(X,r)$ is an indecomposable permutation solution, then $r(x,y) = (\sigma(y), \tau(x))$ for permutations $\sigma, \tau \in \mathbb{S}_X$ such that $\langle \sigma, \tau \rangle$ acts transitively on $X$. For such solutions, the statement clearly holds. Now assume that the statement holds for all indecomposable solutions of multipermutation level at most $n$ and let $(X,r)$ be an indecomposable solution of multipermutation level $n+1$. Let $Y \subseteq X$ be a subsolution and let $Y'$ be the image of $Y$ under the canonical surjection $(X,r) \to \mathrm{Ret}(X,r)$. By the induction hypothesis, $Y'$ is the whole set $\mathrm{Ret}(X,r)$, which means that for any $x \in X$ there exists some $y \in Y$ such that $\sigma_x = \sigma_y$ and $\tau_x = \tau_y$. In particular,

$$\langle \sigma_x, \tau_x \mid x \in X \rangle = \langle \sigma_y, \tau_y \mid y \in Y \rangle,$$

from which we deduce that $Y = X$. □

The following example shows that the hypothesis on the multipermutation level can not be dropped.

**Example 4.4.2.** Let $X = \{1,2,3,4\}$ and let $r$ be the involutive solution given by

$$\sigma_1 = (3\ 4), \quad \sigma_2 = (1\ 3\ 2\ 4), \quad \sigma_3 = (1\ 4\ 2\ 3), \quad \sigma_4 = (1\ 2),$$

for all $x, y \in X$. Then, the set $\{1\}$ is a subsolution of $X$.

The following corollary extends [90, Proposition 5.1], where the statement was proved for indecomposable involutive solutions with an abelian permutation group and multipermutation level 2.

**Corollary 4.4.3.** *Let $(X,r)$ be an indecomposable multipermutation solution. Then every endomorphism of $(X,r)$ is surjective. In particular, if $|X| < \infty$ then every endomorphism of $(X,r)$ is an automorphism.*

*Proof.* It suffices to note that the image under an endomorphism of $X$ is a subsolution of $X$. □

The following lemma extends [88, Corollary 3.11], where the statement was proved for indecomposable involutive solutions of multipermutation level 2.

**Lemma 4.4.4.** *Let $f, g : (X,r) \to (Y,s)$ be homomorphisms of solutions such that $f(x) = g(x)$ for some $x \in X$. If $(X,r)$ is indecomposable and has finite multipermutation level, then $f = g$.*

*Proof.* It suffices to prove that $E = \{y \in X \mid f(y) = g(y)\}$ is a subsolution of $(X, r)$, since Theorem 4.4.1 then implies that $\phi = \psi$. To see this, note that if $y, y' \in E$, then

$$f(\sigma_y(y')) = \sigma_{f(y)} f(y') = \sigma_{g(y)} g(y') = g(\sigma_y(y')),$$

and in a similar way we also find the equalities $f(\tau_y(y')) = g(\tau_y(y'))$, $f(\hat{\sigma}_y(y')) = g(\hat{\sigma}_y(y'))$ and $f(\hat{\tau}_y(y')) = g(\hat{\tau}_y(y'))$. □

**Corollary 4.4.5.** *Let $(X, r)$ be an indecomposable multipermutation solution, then $\mathrm{Aut}(X, r)$ acts freely on $X$. In particular, $|\mathrm{Aut}(X, r)| \leq |X|$.*

*Proof.* Assume that $\phi(x) = \psi(x)$ for $\phi, \psi \in \mathrm{Aut}(X, r)$ and $x \in X$. Then it follows from Lemma 4.4.4 that $\phi = \psi$. □

### 4.4.2 Studying automorphisms of solutions through their permutation brace

We start by recording the following fact, which follows directly from Proposition 1.2.25.

**Proposition 4.4.6.** *Let $A$ be a brace, let $(x, K)$ be a pair satisfying the conditions of Proposition 1.2.24 and let $(X, r)$ be the associated indecomposable solution. If $z \in A$ and $\psi$ is an automorphism of $A$ such that $\psi(x) = \lambda_z(x)$ and $\psi(K) = z \circ K \circ \overline{z}$, then*

$$F : (X, r) \to (X, r) : a \circ K \mapsto \psi(a) \circ z \circ K,$$

*is an automorphism of the solution $(X, r)$. Moreover, every automorphism of $(X, r)$ is of this form.*

Alternatively, using Proposition 1.2.24, we can formulate the same statement with the focus instead shifted towards the solution.

**Proposition 4.4.7.** *Let $(X, r)$ be an indecomposable involutive solution and let $x \in X$. If $\tau \in \mathcal{G}(X, r)$ and $\psi \in \mathrm{Aut}(\mathcal{G}(X, r))$ such that $\psi(\sigma_x) = \lambda_\tau(\sigma_x)$ and*

$$\psi(\mathrm{Stab}_{\mathcal{G}(X,r)}(x)) = \tau \circ \mathrm{Stab}_{\mathcal{G}(X,r)}(x) \circ \overline{\tau},$$

*then the map*

$$F : X \to X : \sigma(x) \mapsto \psi(\sigma)(\tau(x)),$$

*is an automorphism of $(X, r)$. Moreover, every automorphism of $(X, r)$ is of this form.*

Let $A$ be a brace, $x \in A$ and $K$ a subgroup of $(A, \circ)$ satisfying the conditions of Proposition 1.2.24. Then Proposition 4.4.6 gives a solid motivation to study the subgroup

$$S_A(x, K) = \{\mathcal{R}_z^\circ \circ \psi \mid \psi \in \mathrm{Aut}(A, +, \circ), z \in A, \psi(x) = \lambda_z(x), \psi(K) = z \circ K \circ \overline{z}\},$$

of $\mathbb{S}_A$, where $\mathcal{R}_z^\circ$ denotes the right translation by $z \in A$ in $(A, \circ)$. Indeed, if we denote the associated indecomposable solution by $(X, r)$, then we have the following surjective group homomorphism:

$$h : S_A(x, K) \to \mathrm{Aut}(X, r) : \mathcal{R}_z^\circ \psi \mapsto (a \circ K \mapsto \mathcal{R}_z^\circ \psi(a) \circ K).$$

Let $\mathcal{R}_z^\circ \psi \in S_A(x, K)$ be contained in the kernel of $h$, then in particular $K = \mathcal{R}_z^\circ(\psi(0)) \circ K = z \circ K$ hence $z \in K$. This implies $\psi(x) = \lambda_z(x) = x$. For an arbitrary $a \in A$ we then find $\mathcal{R}_z^\circ(\psi(a)) \circ K = \psi(a) \circ K$,

which implies that $\psi(a) \circ \overline{a} \in K$. Conversely, let $z \in K$ and $\psi \in \mathrm{Aut}(A, +, \circ)$ such that $\psi(x) = x$ and $\psi(a) \circ \overline{a} \in K$ for all $a \in A$. Then clearly $\psi(K) = K$ and for any $a \in A$ we find $\mathcal{R}^\circ_z(\psi(a)) \circ K = a \circ K$. We conclude that

$$\ker h = \{\mathcal{R}^\circ_z \psi \mid z \in K, \psi(x) = x, \psi(a) \circ \overline{a} \in K \text{ for all } a \in A\}. \tag{4.3}$$

Note that in particular we always have $\mathcal{R}^\circ(K) \subseteq \ker h$. If $K = \{0\}$, which corresponds to the case that $(A, \circ)$ acts regularly on the associated solution, then clearly $\ker h$ is trivial. If $A$ is multipermutation, then $x$ must generate $A$ as a brace by Corollary 4.2.6, so the only $\psi \in \mathrm{Aut}(A, +, \circ)$ such that $\psi(x) = x$ is the identity automorphism. In this case, we find that $\ker h = \mathcal{R}^\circ(K)$. Our findings can be summarized as follows, where the focus is shifted back to the solution itself.

**Proposition 4.4.8.** *Let $(X, r)$ be an indecomposable involutive solution. Then for any $x \in X$ the map*

$$h : S_{\mathcal{G}(X,r)}(\sigma_x, \mathrm{Stab}_{\mathcal{G}(X,r)}(x)) \to \mathrm{Aut}(X, r) : \mathcal{R}^\circ_\tau \psi \mapsto (\sigma(x) \mapsto \psi(\sigma)(\tau(x))),$$

*is a surjective group homomorphism. If $\mathcal{G}(X, r)$ acts regularly on $X$, then $h$ is an isomorphism. If $(X, r)$ has finite multipermutation level, then* $\ker h = \mathcal{R}^\circ(\mathrm{Stab}_{\mathcal{G}(X,r)}(x))$.

*Remark* 4.4.9. Note that the equality $\ker h = \mathcal{R}^\circ(\mathrm{Stab}_{\mathcal{G}(X,r)}(x))$ in Proposition 4.4.8 more generally holds whenever $\sigma_x$ generates $\mathcal{G}(X, r)$ as a brace. In particular, this is the case when $\sigma_x$ generates the additive or multiplicative group of $\mathcal{G}(X, r)$.

By definition, $S_A(x, K)$ is a subgroup of $S_A(x, \{0\})$, we will denote the latter simply by $S_A(x) := S_A(x, \{0\})$. Let us approach the above discussion from a different point of view. Let

$$\tilde{p} : (X, r) \to (Y, s),$$

be a universal covering of indecomposable solutions such that $(X, r)$ is uniconnected. Let $\phi$ be an automorphism of $(Y, s)$, then since $\tilde{p}$ is a universal covering and also $\phi^{-1}\tilde{p}$ is a covering, we find that $\tilde{p}$ factors through $\phi^{-1}\tilde{p}$, meaning that there exists a homomorphism $\tilde{\phi} : (X, r) \to (X, r)$ such that the following diagram commutes:

$$\begin{array}{ccc} (X,r) & \overset{\tilde{\phi}}{\dashrightarrow} & (X,r) \\ {\scriptstyle\tilde{p}}\downarrow & & \downarrow{\scriptstyle\tilde{p}} \\ (Y,s) & \xrightarrow[\phi]{} & (Y,s) \end{array}$$

It follows that $\tilde{\phi}$ is also covering, but since $(X, r)$ is uniconnected, it follows that $\tilde{\phi}$ is invertible. We conclude that any automorphism of $(Y, s)$ lifts to an automorphism of $(X, r)$, although this lifting is not expected to be unique. Also, the converse should not hold; not every automorphism of $(X, r)$ yields an automorphism of $(Y, s)$. However, we have a surjective group homomorphism from the subgroup of $\mathrm{Aut}(X, r)$ consisting of all automorphisms that are liftings of automorphisms of $(Y, s)$ to the automorphism group $(X, r)$.

In fact, this situation is precisely the one that was discussed before. Indeed, let $A$ be a brace and $x \in A$ an element contained in a transitive cycle base of $A$. We let $(X, r)$ be the solution arising from the pair $(x, \{0\})$ and $(Y, s)$ the solution arising from $(x, K)$ for any $K$ satisfying the conditions of Proposition 1.2.24. Recall from Proposition 1.2.29 that then the map

$$\tilde{p} : (X, r) \to (Y, s) : a \mapsto a \circ K$$

is a covering and $(X, r)$ is uniconnected. The group $S_A(x)$ is precisely the group of automorphisms of $(X, r)$ and $S_A(x, K)$ is the group of automorphisms of $(X, r)$ that can be obtained by lifting an automorphism of $(Y, s)$. The surjective group homomorphism $h$ is the map that sends any automorphism in $S_A(x, K)$ to the automorphism of $(X, r)$ it was lifted from.

From now on, let $X$ be a transitive cycle base of $A$. We define $\mathrm{Aut}(A, X)$ as the group of all skew brace automorphisms $\psi : A \to A$ such that $\psi(X) \subseteq X$.

**Lemma 4.4.10.** *Let $A$ be a brace with transitive cycle base $X$. Then the following are equivalent for an automorphism $\psi$ of $A$:*

1. *There exists some $x \in X$ such that $\psi(x) \in X$,*
2. *$\psi(X) \subseteq X$,*
3. *$\psi(X) = X$.*

*Proof.* Assume that $\psi(x) \in X$ for some $x \in X$. Recall that $X = \{\lambda_a(y) \mid a \in A\}$ for any $y \in X$. Since $\psi(\lambda_a(x)) = \lambda_{\psi(a)}(\psi(x)) \in X$ for all $a \in A$ we find that $\psi(X) \subseteq X$. Also, since every $y \in X$ is of the form $\lambda_a(\psi(x))$ for some $a \in A$, we find $y = \psi(\lambda_{\psi^{-1}(a)}(x)) \in \psi(X)$ and thus $X \subseteq \psi(X)$. The other implications are trivial. □

**Lemma 4.4.11.** *Let $A$ be a brace, $X$ a transitive cycle base of $A$ and $x \in X$. Then $S_A(x)$ has a normal subgroup isomorphic to the stabilizer of $x$ under the $\lambda$-action, such that its quotient is isomorphic to $\mathrm{Aut}(A, X)$.*

*Proof.* Define

$$\phi : S_A(x) \to \mathrm{Aut}(A, X) : \mathcal{R}_a^\circ \psi \mapsto \psi.$$

By Lemma 4.4.10, this is a well-defined group homomorphism with kernel the right translations contained in $S_A(x)$. Clearly $\mathcal{R}_a^\circ = \mathcal{R}_a^\circ \mathrm{id}_A \in S_A(x)$ if and only if $\lambda_a(x) = x$. Moreover, the definition of $\mathrm{Aut}(A, X)$ ensures that $\phi$ is surjective. □

If $\lambda_a$ is an automorphism of $A$ for some $a \in A$, then it follows automatically that $\lambda_a \in \mathrm{Aut}(A, X)$. Define

$$H(A) = \{a \in A \mid \lambda_a \in \mathrm{Aut}(A, +, \circ)\}.$$

From Lemma 1.1.33 we find that $H(A)$ is precisely the preimage of $\mathrm{Fix}(A/\operatorname{Soc}(A))$ under the surjection $A \to A/\operatorname{Soc}(A)$. Moreover, if $x \in X$, then $\mathcal{R}_a^\circ \lambda_a$ is contained in $S_A(x)$ for all $a \in H(A)$. For all $a, b \in H$, $c \in A$ we find

$$\mathcal{R}_a^\circ \lambda_a \mathcal{R}_b^\circ \lambda_b(c) = \mathcal{R}_a^\circ(\lambda_a(\lambda_b(c) \circ b)) = \lambda_a\lambda_b(c) \circ \lambda_a(b) \circ a = \mathcal{R}_{\lambda_a(b)\circ a}^\circ \lambda_{a\circ b}(c).$$

Since $a, b \in H$ we find that $\lambda_{a\circ b} = \lambda_{\lambda_a(b)\circ a}$. We conclude that

$$\{\mathcal{R}_a^\circ \lambda_a \mid a \in H(A)\}$$

is a subgroup of $S_A(x)$.

**Proposition 4.4.12.** *Let $A$ be a brace. Then $\{\mathcal{R}_a^\circ \lambda_a \mid a \in H(A)\}$ is isomorphic to $(H(A), +)$.*

*Proof.* Consider the map

$$\phi : \{\mathcal{R}_a^\circ \lambda_a \mid a \in H(A)\} \to (H(A), +) : \mathcal{R}_a^\circ \lambda_a \mapsto \overline{a}.$$

It is clear that $\phi$ is a bijection. Using the observation above, we find

$$\begin{aligned}\phi(\mathcal{R}_a^\circ \lambda_a \mathcal{R}_b^\circ \lambda_b) &= \phi(\mathcal{R}^\circ_{\lambda_a(b)\circ a} \lambda_{\lambda_a(b)\circ a}) \\ &= \overline{\lambda_a(b) \circ a} \\ &= \overline{a} \circ \overline{\lambda_a(b)} \\ &= \overline{a} \circ \lambda_a(\overline{b}) \\ &= \overline{a} + \overline{b} \\ &= \phi(\mathcal{R}_a^\circ \lambda_a) + \phi(\mathcal{R}_b^\circ \lambda_b),\end{aligned}$$

from which the statement follows. □

**Lemma 4.4.13.** *Let $A$ be a brace of multipermutation level 2, $X$ a transitive cycle base of $A$ and $x \in X$. Then:*

1. $\mathrm{Aut}(A, X) = \{\lambda_a \mid a \in A\}$.
2. $S_A(x) = \{\mathcal{R}_a^\circ \lambda_a \mid a \in A\}$, *so in particular $S_A(x)$ acts regularly on $A$.*
3. $S_A(x, K) = S_A(x)$ *for any subgroup $K$ of $(A, \circ)$ that stabilizes $x$ under the $\lambda$-action.*
4. $S_A(x) \cong (A, +)$.

*Proof.* Note that, since $H(A) = A$, the map $\lambda_a$ is contained in $\mathrm{Aut}(A, X)$ for all $a \in A$. Because $A$ has finite multipermutation level, we know by Corollary 4.2.6 that $x \in X$ generates $A$ as a brace. By definition, for $\psi \in \mathrm{Aut}(A, X)$ there exists some $a \in A$ such that $\psi(x) = \lambda_a(x)$. Since $x$ generates the brace $A$, it then follows that $\psi = \lambda_a$. This proves the first part of the statement. It then follows that every element in $S_A(x)$ is of the form $\mathcal{R}_b^\circ \lambda_a$ for some $a, b \in A$, but the condition $\lambda_b(x) = \lambda_a(x)$ forces $\lambda_a = \lambda_b$ and thus $\mathcal{R}_b^\circ \lambda_a = \mathcal{R}_b^\circ \lambda_b$. This implies the second part of the statement.

To prove the third part, let $k \in A$ such that $\lambda_k(x) = x$. By a similar reasoning as above, it follows that $\lambda_k = \mathrm{id}_A$ and thus $k \in \mathrm{Soc}(A)$. Therefore, if $K$ is a subgroup of $(A, \circ)$ that fixes $x$ under the $\lambda$-action, then $K \subseteq \mathrm{Soc}(A)$ and thus $\lambda_a(K) = a \circ K \circ \overline{a}$ by the comment in Example 1.1.5.

The last part is now a direct consequence of Proposition 4.4.12. □

The following theorem is an extension of [88, Proposition 5.16].

**Theorem 4.4.14.** *Let $(X, r)$ be an indecomposable involutive solution of multipermutation level 2 and $x \in X$. Then $\mathrm{Aut}(X, r)$ is isomorphic to $(\mathcal{G}(X, r), +)/\mathrm{Stab}_{\mathcal{G}(X,r)}(x)$ and its action on $X$ is regular. In particular, $\mathrm{Aut}(X, r)$ is abelian.*

*Proof.* Let $x \in X$. From Proposition 4.4.8 we know that

$$\mathrm{Aut}(X, r) \cong S_{\mathcal{G}(X,r)}(\sigma_x, \mathrm{Stab}_{\mathcal{G}(X,r)}(x))/\mathcal{R}^\circ(\mathrm{Stab}_{\mathcal{G}(X,r)}(x)).$$

Since $\mathcal{G}(X, r)$ has multipermutation level 2 we get from Lemma 4.4.13 that

$$S_{\mathcal{G}(X,r)}(\sigma_x, \mathrm{Stab}_{\mathcal{G}(X,r)}(x)) = S_{\mathcal{G}(X,r)}(\sigma_x) \cong (\mathcal{G}(X, r), +),$$

where under this isomorphism the subgroup $\mathcal{R}^\circ(\mathrm{Stab}_{\mathcal{G}(X,r)}(x))$ is mapped to $\mathrm{Stab}_{\mathcal{G}(X,r)}(x)$. Also, $S_{\mathcal{G}(X,r)}(\sigma_x)$ acts regularly on $A$, hence $S_{\mathcal{G}(X,r)}(\sigma_x)/\mathcal{R}^\circ(\mathrm{Stab}_{\mathcal{G}(X,r)}(x))$ acts regularly on the cosets $(\mathcal{G}(X,r),\circ)/\mathrm{Stab}_{\mathcal{G}(X,r)}(x)$. □

*Remark* 4.4.15. Let $(X,r)$ be an indecomposable involutive solution of multipermutation level 2 and let $\tilde{p}: (\tilde{X},\tilde{r}) \to (X,r)$ be a universal covering with $(\tilde{X},\tilde{r})$ uniconnected. Then Lemma 4.4.13 and Theorem 4.4.14 learn us that every automorphism of $(\tilde{X},\tilde{r})$ yields an automorphism of $(X,r)$ and the automorphism group of $(\tilde{X},\tilde{r})$ is isomorphic to $(\mathcal{G}(X,r),+)$.

We now turn our attention to braces whose additive group is cyclic, known as *cyclic* braces.

**Lemma 4.4.16.** *Let $A$ be a cyclic brace and $x \in A$. Then $x$ generates $A$ as a left ideal if and only if $x$ generates the group $(A,+)$.*

*Proof.* One implication is trivial. Conversely, we know that the additive subgroup generated by $x$ is equal to $mA$, for some $m \geq 1$. Since $mA$ is a characteristic subgroup of $(A,+)$, it is a left ideal, the left ideal generated by $x$ is contained in $mA$. This forces $m = 1$. □

The following lemma is similar to Lemma 4.4.13.

**Lemma 4.4.17.** *Let $A$ be a cyclic brace, let $X$ be a transitive cycle base of $A$ and $x \in X$. Then*

1. $\mathrm{Aut}(A,X) = \{\lambda_a \mid a \in H(A)\}$.
2. $S_A(x) = \{\mathcal{R}_a^\circ \lambda_a \mid a \in H(A)\}$, *so the orbit of* $0$ *under its action is* $H(A)$.
3. $S_A(x,K) = S_A(x)$ *for any subgroup $K$ of $(A,\circ)$ that stabilizes $x$ under the $\lambda$-action.*
4. $S_A(x) \cong (H(A),+)$.

*Proof.* From Lemma 4.4.16 we know that $x$ generates the group $(A,+)$. Therefore, if $\psi \in \mathrm{Aut}(A,+,\circ)$ and $a \in A$ are such that $\lambda_a(x) = \psi(x)$, then $\psi = \lambda_a$. The first part of the statement now follows since $\lambda_a \in \mathrm{Aut}(A,+,\circ)$ if and only if $a \in H(A)$. It now follows that every element in $S_A(x)$ is of the form $\mathcal{R}_b^\circ \lambda_a$ for some $a,b \in A$, but the condition $\lambda_b(x) = \lambda_a(x)$ forces $\lambda_a = \lambda_b$ and thus $\mathcal{R}_b^\circ \lambda_a = \mathcal{R}_b^\circ \lambda_b$. This implies the second part of the statement.

For the third part, let $k \in A$ such that $\lambda_k(x) = x$. Since $x$ generates $(A,+)$, we find $\lambda_k = \mathrm{id}_A$ and thus $k \in \mathrm{Soc}(A)$. Therefore, if $K$ is a subgroup of $(A,\circ)$ that fixes $x$ under the $\lambda$-action, then $K \subseteq \mathrm{Soc}(A)$ and thus $\lambda_a(K) = a \circ K \circ \overline{a}$ by the remark in Example 1.1.5.

The last part is now a direct consequence of Proposition 4.4.12. □

**Theorem 4.4.18.** *Let $(X,r)$ be an indecomposable involutive solution such that $(\mathcal{G}(X,r),+)$ is cyclic. Then $\mathrm{Aut}(X,r)$ is isomorphic to $(H(\mathcal{G}(X,r)),+)/\mathrm{Stab}_{\mathcal{G}(X,r)}(x)$. In particular, $\mathrm{Aut}(X,r)$ is abelian and $\mathrm{Aut}(X,r)$ acts transitively on $X$ if and only if $\mathrm{mpl}(X,r) \leq 2$.*

*Proof.* Let $x \in X$. From Lemma 4.4.16 we know that $\sigma_x$ generates $(\mathcal{G}(X,r),+)$. From Proposition 4.4.8 and Remark 4.4.9 we get that

$$\mathrm{Aut}(X,r) \cong S_{\mathcal{G}(X,r)}(\sigma_x, \mathrm{Stab}_{\mathcal{G}(X,r)}(x))/\mathcal{R}^\circ(\mathrm{Stab}_{\mathcal{G}(X,r)}(x)).$$

Lemma 4.4.17 implies that

$$S_{\mathcal{G}(X,r)}(\sigma_x, \mathrm{Stab}_{\mathcal{G}(X,r)}(x)) = S_{\mathcal{G}(X,r)}(\sigma_x) \cong (H(\mathcal{G}(X,r)),+),$$

where under this isomorphism the subgroup $\mathcal{R}^\circ(\mathrm{Stab}_{\mathcal{G}(X,r)}(x))$ is mapped to $\mathrm{Stab}_{\mathcal{G}(X,r)}(x)$. Also, the orbit of 0 under the action of $S_{\mathcal{G}(X,r)}(\sigma_x)$ is $H(\mathcal{G}(X,r))$, hence $S_{\mathcal{G}(X,r)}(\sigma_x)/\mathcal{R}^\circ(\mathrm{Stab}_{\mathcal{G}(X,r)}(x))$ acts regularly on the cosets $(\mathcal{G}(X,r),\circ)/\mathrm{Stab}_{\mathcal{G}(X,r)}(x)$ if and only if $H(\mathcal{G}(X,r)) = \mathcal{G}(X,r)$ or equivalent when $\mathcal{G}(X,r)$ is a bi-skew brace, the result now follows from Propositions 4.1.3 and 4.3.6. □

It is non-trivial to determine whether, given a solution $(X,r)$, the additive group $(\mathcal{G}(X,r),+)$ is cyclic. On the other hand, it is directly verified whether the permutation group $(\mathcal{G}(X,r),\circ)$ is cyclic. The following lemma shows that in many cases, if $(\mathcal{G}(X,r),\circ)$ is cyclic, then so is $(\mathcal{G}(X,r),+)$.

**Lemma 4.4.19.** *Let $A$ be a brace such that $(A,\circ)$ is cyclic. Then either $(A,+)$ is cyclic or $A$ is finite and $(A,+)$ is isomorphic to $(\mathbb{Z}/2)^2 \times \mathbb{Z}/n$ with $n$ odd.*

*Proof.* If $A$ is infinite, then the result follows by Corollary 2.3.3. If $A$ is finite, then the result follows directly from [160, Proposition 1.3, Theorem 1.5] or [12, Proposition 5.4]. □

*Remark* 4.4.20. Recall from [132] that up to isomorphism every brace whose additive and multiplicative groups are cyclic is of the form $A = (\mathbb{Z}/n,+,\circ)$ where $a \circ b = a + b + abk$ with $k$ a divisor of $n$ such that every prime divisor of $n$ also divides $k$. For such a brace, we find that $H(A) = \{a \in A \mid k^2 a = 0\}$.

If $(X,r)$ is a finite indecomposable involutive solution with a cyclic permutation group such that the highest power of 2 dividing $|X|$ is not 4, then we can conclude from Lemma 4.4.19 that $(\mathcal{G}(X,r),+)$ is cyclic. In the other case, however, the Sylow 2-subgroup is small, so in particular it is of multipermutation level at most 2. The following lemma allows us to combine the two different cases considered in Lemmas 4.4.13 and 4.4.17 in order to obtain a similar result in the case that the $(\mathcal{G}(X,r),\circ)$ is cyclic.

**Lemma 4.4.21.** *Let $A = A_1 \times A_2$ be a product of finite braces of coprime order, let $X$ be a transitive cycle base of $A$ and $x \in X$. Let $X_i \subseteq A_i$ and $x_i \in A_i$, $i \in \{1,2\}$ be the projection onto $A_i$ of $X$ and $x$ respectively. Then*

1. *$X_i$ is a transitive cycle base of $A_i$,*
2. *$\mathrm{Aut}(A,X) \cong \mathrm{Aut}(A_1,X_1) \times \mathrm{Aut}(A_2,X_2)$,*
3. *$S_A(x) \cong S_{A_1}(x_1) \times S_{A_2}(x_2)$.*

*Proof.* Since for $(a_1,a_2),(b_1,b_2) \in A_1 \times A_2$ we have $\lambda_{(a_1,a_2)}(b_1,b_2) = (\lambda_{a_1}(b_1),\lambda_{a_2}(b_2))$, it follows that $X_i$ is a transitive cycle base of $A_i$. As $|A_1|$ and $|A_2|$ are coprime, the automorphisms of $(A,+)$ are of the form

$$\phi_1 \times \phi_2 : A \to A : (a,b) \mapsto (\phi_1(a),\phi_2(b)),$$

for $\phi_i \in \mathrm{Aut}(A_i,+,\circ)$. From this, the second part of the statement follows directly. Consider the injective map

$$S_{A_1}(x_1) \times S_{A_2}(x_2) \to S_A(x) : (\mathcal{R}^\circ_{a_1}\psi_1, \mathcal{R}^\circ_{a_2}\psi_2) \mapsto \mathcal{R}^\circ_{(a_1,a_2)}(\psi_1 \times \psi_2),$$

which is well-defined since $\lambda_{(a_1,a_2)}(x_1,x_2) = (\psi_1 \times \psi_2)(x_1,x_2)$ if and only if $\lambda_{a_1}(x_1) = \psi_1(x_1)$ and $\lambda_{a_2}(x_2) = \psi_2(x_2)$. It follows from 2 that this map is surjective and it is clear that this is a group homomorphism. □

**Lemma 4.4.22.** *Let $A$ be a brace with $(A,\circ)$ cyclic, let $X$ be a transitive cycle base of $A$ and $x \in X$. Then*

1. *$\mathrm{Aut}(A,X) = \{\lambda_a \mid a \in H(A)\}$,*

2. $S_A(x) = \{\mathcal{R}_a^\circ \lambda_a \mid a \in H(A)\}$, *so the orbit of* $0$ *under its action is* $H(A)$,

3. $S_A(x) \cong (H(A), +)$.

*Proof.* If $(A, +)$ is cyclic, then this follows from Lemma 4.4.17. If $(A, +)$ is not cyclic, then we know that $A$ is finite and $A = A_1 \times A_2$ as braces, where $(A_1, +)$ is cyclic of odd order and $(A_2, +)$ is the Klein group. Note that $\mathrm{mpl}(A_2) \leq 2$. The result then follows by Lemma 4.4.21 combined with Lemmas 4.4.13 and 4.4.17 and the observation that $H(A_1 \times A_2) = H(A_1) \times H(A_2)$. □

In [90, Section 5] all indecomposable involutive solutions with $\mathrm{mpl}(X, r) = 2$ whose automorphism and permutation group are cyclic were determined. In the following, we characterize these in terms of their permutation skew braces, where we remove the assumption on the multipermutation level.

**Theorem 4.4.23.** *Let* $(X, r)$ *be an indecomposable involutive solution with a cyclic permutation group. Then* $\mathrm{Aut}(X, r)$ *is isomorphic to* $(H(\mathcal{G}(X, r)), +)$*, so in particular it is abelian. Furthermore,* $\mathrm{Aut}(X, r)$ *acts transitively on* $X$ *if and only if* $\mathrm{mpl}(X, r) \leq 2$*.*

*Proof.* Let $x \in X$. Note that by Corollary 2.3.3 and the well-known fact that finite Jacobson radical rings are nilpotent, we find that $(\mathcal{G}(X, r), +)$ is multipermutation. From Proposition 4.4.8 we obtain

$$\mathrm{Aut}(X, r) \cong S_{\mathcal{G}(X,r)}(\sigma_x, \mathrm{Stab}_{\mathcal{G}(X,r)}(x))/\mathcal{R}^\circ(\mathrm{Stab}_{\mathcal{G}(X,r)}(x)) \cong S_{\mathcal{G}(X,r)}(\sigma_x),$$

where we used the fact that the stabilizer of $x$ is trivial since $(\mathcal{G}(X, r), \circ)$ is abelian. From Lemma 4.4.22 we find that

$$S_{\mathcal{G}(X,r)}(\sigma_x) \cong (H(\mathcal{G}(X, r)), +),$$

which proves the first part of the statement. The orbit of $0$ under the action of $S_{\mathcal{G}(X,r)}(\sigma_x)$ is $H(\mathcal{G}(X, r))$, and we know that $H(\mathcal{G}(X, r)) = \mathcal{G}(X, r)$ if and only if $\mathcal{G}(X, r)$ is a bi-skew brace. By Propositions 4.1.3 and 4.3.6, the last part of the statement follows. □

**Corollary 4.4.24.** *Let* $(X, r)$ *be a finite indecomposable involutive solution such that its permutation group is cyclic. Then* $\mathrm{Aut}(X, r)$ *is non-cyclic if and only if the Sylow* $2$*-subgroup of* $(\mathcal{G}(X, r), +)$ *is isomorphic to the Klein group. In particular, if the highest power of 2 dividing* $|X|$ *is different from 4, then* $\mathrm{Aut}(X, r)$ *is cyclic.*

*Proof.* This follows directly from Theorem 4.4.23 and Lemma 4.4.19. □

If we restrict to solutions of multipermutation level 2, then we can also obtain a partial dual statement.

**Corollary 4.4.25.** *Let* $(X, r)$ *be a finite indecomposable involutive solution with an abelian non-cyclic permutation group. Suppose moreover that* $\mathrm{mpl}(X, r) = 2$*. If* $\mathrm{Aut}(X, r)$ *is cyclic, then the Sylow* $2$*-subgroup of the permutation group is isomorphic to the Klein group. In particular, if the highest power of 2 dividing* $|X|$ *is different from 4, then* $\mathrm{Aut}(X, r)$ *is non-cyclic.*

*Proof.* If $\mathrm{Aut}(X, r)$ is cyclic then by Theorem 4.4.14 the additive group of $\mathcal{G}(X, r)$ is cyclic. Since $\mathrm{mpl}(X, r) = 2$, we find that $\mathcal{G}(X, r)$ is a bi-skew brace. The statement now follows from Lemma 4.4.19 since $(\mathcal{G}(X, r), \circ, +)$ is a brace with a cyclic multiplicative group and a non-cyclic additive group. □

Chapter 5

# Indecomposable involutive solutions of order $p^2$

In [73, Theorem 2.13], Etingof, Schedler and Soloviev proved that for any prime $p$ there exists, up to isomorphism, only a unique involutive solution given by $(\mathbb{Z}/p, r)$ with

$$r(x, y) = (x + 1, y - 1).$$

Furthermore, Jedlička and Pilitowska [88] have classified all indecomposable involutive solutions of multipermutation level 2 by providing a universal indecomposable involutive solution and describing its epimorphic images through congruences, see also [89, 90]. In particular, this includes all indecomposable cycle sets of order $pq$ that are of finite multipermutation level, where $p, q$ are (not necessarily distinct) primes. In [54], Cedó and Okniński proved that all indecomposable involutive solutions of square-free size are of finite multipermutation level, which implies that the classification of indecomposable involutive solutions of size $pq$ for $p \neq q$ is accomplished through the earlier mentioned results by Jedlička and Pilitowska. Cedó and Okniński [53, Section 5] described a class of simple, thus irretractable, indecomposable solutions of size $p^2$, $p$ a prime. Subsequently, they ask whether all irretractable indecomposable involutive solutions belong to this family.

In this chapter, we explicitly determine all indecomposable involutive solutions of size $p^2$. In order to simplify some of the calculations and notations, we use the language of cycle sets throughout the whole chapter. It is only at the end that we formulate the classification in terms of solutions of the YBE.

This chapter is organized as follows. In Section 5.1 we first include some preliminary results on systems of imprimitivity of group actions and in Section 5.2 we prove auxiliary results on braces, both of which will be extensively used in Sections 5.4 and 5.5. Although our focus is on irretractable solutions, we first give in Corollary 5.3.4 a complete list of retractable indecomposable involutive solutions of size $p^2$. These solutions have been described by Jedlička and Pilitowska in [88], but in Theorem 5.3.2 we present them in a different and more explicit way that bears a strong resemblance to how we describe the irretractable solutions later in the chapter. We then start our classification by considering the irretractable indecomposable cycle sets of size $p^2$ whose permutation group is a $p$-group. In Theorem 5.4.9 we give a full classification together with an explicit description of their automorphisms. The next step is to consider those cycle sets whose permutation group is not a $p$-group. We prove that these can all be obtained by deforming one of the earlier classified cycle sets by an automorphism of order coprime to $p$. This deformation process is given in Lemma 5.5.3. We obtain the final classification in terms of cycle sets in Theorem 5.5.6. In Section 5.6 we transfer this classification back to the original setting and we present a complete list of irretractable indecomposable

solutions of size $p^2$. We also give a formula to compute the number of isomorphism classes in function of $p$ and give an affirmative answer to the earlier mentioned question by Cedó and Okniński.

All results in this chapter (except for the ones in Section 5.1) for which no external reference is given were obtained in collaboration with Carsten Dietzel and Silvia Properzi, and are published in [71].

## 5.1 Preliminaries on systems of imprimitivity

Let $G$ be a group acting on a set $X$. A *system of imprimitivity* is a partition $X = \bigsqcup_{i\in I} X_i$ that is invariant under the group action in the sense that for any $g \in G$, $i \in I$, there is a $j \in I$ such that $g \cdot X_i = X_j$. The subsets $X_i$ are called *blocks* of the system. A system of imprimitivity is *trivial* if either $|I| = 1$ or $|X_i| = 1$ for all $i \in I$, else it is non-trivial. If $X$ is finite and $G$ is transitive, then $G$ acts transitively on the blocks of a system of imprimitivity, and $|X_i| = |X_j|$ for all $i, j \in X$. In particular, all $|X_i|$ divide $|X|$.

**Lemma 5.1.1.** *Let $G$ be a non-abelian $p$-group with a transitive action on a set $X$ of size $p^2$, for $p$ a prime. Then $G$ has at most one non-trivial system of imprimitivity.*

*Proof.* If there is more than one non-trivial system of imprimitivity, a result of Lucchini [118, Theorem 1] implies that $G \leq \mathbb{S}_p \times \mathbb{S}_p$. But if $G$ is a $p$-group, this forces $G$ to be isomorphic to a subgroup of $\mathbb{Z}/p \times \mathbb{Z}/p$ and therefore to be abelian. □

Let $G, H$ be groups such that $G$ acts on a set $X$. The *wreath product* is the semidirect product $H \wr_X G = H^X \rtimes G$, where $H^X = \{(h_x)_{x\in X} \mid h_x \in H \text{ for all } x \in X\}$ is the iterated direct product of $H$ with itself indexed by $X$, and $G$ acts on $H^X$ by $g \cdot (h_x)_{x\in X} = (h_{g^{-1}\cdot x})_{x\in X}$. If the action of $G$ on $X$ is clear, we will generally suppress the subscript $X$ and write $H \wr G$.

If additionally $H$ acts on a set $Y$, then $H \wr G$ acts on $X \times Y$ by

$$(h, g) \cdot (x, y) = (g \cdot x, h_{g\cdot x} \cdot y).$$

**Proposition 5.1.2.** *Let $G \leq \mathbb{S}_{\mathbb{Z}/p\times\mathbb{Z}/p}$ be a transitive solvable group such that the sets $\{a\} \times \mathbb{Z}/p$, $a \in \mathbb{Z}/p$, form a system of imprimitivity. Then $G$ is conjugate to a subgroup of $\mathrm{Hol}(\mathbb{Z}/p) \wr \mathrm{Hol}(\mathbb{Z}/p)$. If moreover $G$ is a $p$-group, then $G$ is conjugate to a subgroup of $\mathbb{Z}/p \wr \mathbb{Z}/p$.*

*Proof.* Let $G$ be as above. As $G$ respects the given system of imprimitivity, $G \leq \mathbb{S}_p \wr \mathbb{S}_p$, where the action of the wreath product on $\mathbb{Z}/p \times \mathbb{Z}/p$ is precisely as described above.

As a special case of [86, Chapter II, Satz 3.2], we know that every solvable transitive subgroup of $\mathbb{S}_p$ is conjugate to a subgroup of $\mathrm{Hol}(\mathbb{Z}/p)$. We conclude that $G$ is conjugate to a subgroup of $\mathrm{Hol}(\mathbb{Z}/p) \wr \mathrm{Hol}(\mathbb{Z}/p)$. As $\mathbb{Z}/p \wr \mathbb{Z}/p$ is a Sylow $p$-subgroup of $\mathrm{Hol}(\mathbb{Z}/p) \wr \mathrm{Hol}(\mathbb{Z}/p)$ also the last part of the statement follows. □

We note in particular that elements of $\mathbb{Z}/p \wr \mathbb{Z}/p$ are precisely permutations of the form

$$(a, x) \mapsto (a + \beta, x + \gamma_a),$$

with $\beta, \gamma_0, \ldots, \gamma_{p-1} \in \mathbb{Z}/p$.

## 5.2 Some results on braces

**Lemma 5.2.1.** *Let $A$ be a brace. Then for all $a, b \in A$,*

$$\lambda_a(b) = -a + (a \circ b \circ \overline{a}) + \lambda_{a \circ b \circ \overline{a}}(a).$$

*In particular, $a \in \mathrm{Fix}(A)$ if and only if $\lambda_a(b) = a \circ b \circ \overline{a}$ for all $b \in A$.*

*Proof.* Observe that if $a, b \in A$, then

$$\lambda_a(b) = -a + (a \circ b) = -a + (a \circ b \circ \overline{a} \circ a) = -a + (a \circ b \circ \overline{a}) + \lambda_{a \circ b \circ \overline{a}}(a). \qquad \square$$

**Theorem 5.2.2.** *Let $A$ be a brace and $B$ a subbrace such that $(B, \circ)$ acts trivially on $(A, +)/B$ under the $\lambda$-action. Furthermore, assume that $(B, \circ)$ is normal in $(A, \circ)$. Then $B$ is an ideal of $A$.*

*Proof.* Let $b \in B$. We have to show that $\lambda_a(b) \in B$ for all $a \in A$. Since $B$ is normal in $(A, \circ)$ and $(B, \circ)$ acts trivially on $(A, +)/B$, we find $\lambda_{a \circ b \circ \overline{a}}(a) \in a + B$. Using Lemma 5.2.1 we deduce that

$$\lambda_a(b) = -a + {}^a b + \lambda_{{}^a b}(a) \in -a + B + a + B = B. \qquad \square$$

**Proposition 5.2.3.** *Let $A$ be a finite brace and $B$ a subbrace with $|A| = p|B|$, where $p$ is the smallest prime divisor of $|A|$. Then $B$ is an ideal of $A$.*

*Proof.* The quotient group $(A, +)/B$ is cyclic of order $p$ and therefore is acted upon trivially by $(B, \circ)$. Furthermore, since the index of $(B, \circ)$ in $(A, \circ)$ is the smallest prime divisor of $|A|$, the subgroup $(B, \circ)$ is normal in $(A, \circ)$. It follows from Theorem 5.2.2 that $B$ is an ideal of $A$. $\square$

Given a brace $A$ and a subset $S \subseteq A$ we define

$$\mathrm{Fix}_A(S) = \{a \in A \mid \lambda_s(a) = a \text{ for all } s \in S\}.$$

In fact, it follows from Lemma 5.2.1 that $\lambda_{\overline{a}}(\overline{a} \circ s \circ a) = -a + s + \lambda_s(a)$, so $\lambda_s(a) = a$ if and only if $\lambda_a(\overline{a} \circ s \circ a) = s$, which is equivalent to $\lambda_{\overline{a}}(s) = \overline{a} \circ s \circ a$. Therefore, we obtain the alternative description:

$$\mathrm{Fix}_A(S) = \{a \in A \mid \lambda_{\overline{a}}(s) = \overline{a} \circ s \circ a \text{ for all } s \in S\}.$$

**Lemma 5.2.4.** *Let $A$ be a finite brace, $L$ a left ideal of $A$ and $G$ a normal subgroup of $(A, \circ)$. Then $\mathrm{Fix}_A(L \cap G)$ is a subbrace of $A$ contained in the normalizer of $L \cap G$ in $(A, \circ)$.*

*Proof.* From the original definition of $\mathrm{Fix}_A(L \cap G)$ we see that $(\mathrm{Fix}_A(L \cap G), +)$ is a group. Let $a \in \mathrm{Fix}_A(L \cap G)$ and $b \in L \cap G$. Then $\lambda_{\overline{a}}(b) \in L$, but as $\lambda_{\overline{a}}(b) = \overline{a} \circ b \circ a$, also $\lambda_{\overline{a}}(b) \in G$. We conclude that $\lambda_{\overline{a}}(b) \in L \cap G$. Using the alternative description of $\mathrm{Fix}_A(L \cap G)$, we now see that $\mathrm{Fix}_A(L \cap G)$ is closed under the operation $\circ$ and non-empty. As $A$ is finite, we conclude that $(\mathrm{Fix}_A(L \cap G), \circ)$ is a subgroup of $(A, \circ)$. Therefore, $\mathrm{Fix}_A(L \cap G)$ is a subbrace. As $\overline{a} \circ b \circ a \in L \cap G$ for all $a \in \mathrm{Fix}_A(L \cap G)$, $b \in L \cap G$ we find indeed that $\mathrm{Fix}_A(L \cap G)$ is contained in the normalizer of $L \cap G$ in $(A, \circ)$. $\square$

## 5.3 Indecomposable retractable cycle sets of size $p^2$

It is clear that, up to isomorphism, there is a unique indecomposable cycle set of size $p^2$ whose retract has size 1. This cycle set is given by $X = \mathbb{Z}/p^2$ with cycle set operation $x \cdot y = y + 1$. Those cycle sets whose retract has size $p$ follow from results by Jedlička and Pilitowska [88]. We recall the following (slightly restrictive case of the) construction of indecomposable cycle sets of multipermutation level 2 as obtained in [88, Proposition 5.1 and 5.7].

Let $e_i$, $i \in \mathbb{Z}$, denote the elements in the canonical basis of $\bigoplus_{i\in\mathbb{Z}} \mathbb{Z}$. We define

$$c_k = \begin{cases} \sum_{i=1}^{-k} -e_{1-i} & k < 0 \\ 0 & k = 0 \\ \sum_{i=1}^{k} e_i & k > 0 \end{cases}.$$

**Theorem 5.3.1.** *Let $(X, \cdot)$ be an indecomposable cycle set of multipermutation level 2 whose retract has size $m$. Then there exist*

1. *a subgroup $H \leq \bigoplus_{i\in\mathbb{Z}} \mathbb{Z}$ such that $c_i - c_{i+m} \in H$, for all $i \in \mathbb{Z}$,*
2. *$s \in \left(\bigoplus_{i\in\mathbb{Z}} \mathbb{Z}\right)/H$,*

*such that $(X, \cdot)$ is isomorphic to a cycle set of the form $X = (\mathbb{Z} \times \bigoplus_{i\in\mathbb{Z}} \mathbb{Z})/\sim$ where*

$$(a, x) \sim (b, y) \iff a - b \equiv 0 \mod m, \text{ and } x - y \equiv \frac{a-b}{m} s \mod H,$$

*and*

$$[(a, x)] \cdot [(b, y)] = [(b - 1, y - c_{a-b} + c_{-b})].$$

*Moreover, different choices of $H$ and $s$ yield non-isomorphic cycle sets.*

For an abelian group $(A, +)$ we define $\chi_0 : A \to \mathbb{Z}$ as

$$\chi_0(x) = \begin{cases} 1 & x = 0 \\ 0 & x \neq 0 \end{cases}.$$

**Theorem 5.3.2.** *Let $(X, \cdot)$ be an indecomposable cycle set of multipermutation level 2 whose retract has size $m$. Then $(X, \cdot)$ is isomorphic to a cycle set of the form $X = \mathbb{Z}/m \times A$ with operation*

$$(a, x) \cdot (b, y) = (b + 1, y + \chi_0(b)S + \Phi(b - a)),$$

*where $(A, +)$ is an abelian group, $\Phi : \mathbb{Z}/m \to A$ is a non-constant map such that $\Phi(0) = 0$ and $\Phi(\mathbb{Z}/m)$ generates $A$, and $S \in A$. Two such cycle sets, given by $(A, \Phi, S)$ and $(B, \Phi', S')$, are isomorphic if and only if there exists a group isomorphism $f : A \to B$ such that $\Phi' = f\Phi$ and $f(S) = S'$.*

*Proof.* Let $H \leq \bigoplus_{i\in\mathbb{Z}} \mathbb{Z}$ and $s \in \left(\bigoplus_{i\in\mathbb{Z}} \mathbb{Z}\right)/H$ satisfying the conditions of Theorem 5.3.1. Observe that if $1 \leq a, b \leq m$ and $x, y \in \bigoplus_{i\in\mathbb{Z}} \mathbb{Z}$, then $(a, x) \sim (b, y)$ if and only if $a = b$ and $x - y \in H$. Also note that since

$$(a, x) \sim (a - m, x - s) \sim (a + m, x + s)$$

for every $a \in \mathbb{Z}$ and $x \in \bigoplus_{i\in\mathbb{Z}} \mathbb{Z}$, every element in $\mathbb{Z} \times \bigoplus_{i\in\mathbb{Z}} \mathbb{Z}$ is in relation with an element whose first components is contained in $\{1, \dots, m\}$. We define the map

$$\psi : \left(\mathbb{Z} \times \bigoplus_{i\in\mathbb{Z}} \mathbb{Z}\right) /\sim \to \mathbb{Z}/m \times \left(\bigoplus_{i\in\mathbb{Z}} \mathbb{Z}\right) /H,$$

as $\psi([(a, x)]) = (a, x)$ for $1 \leq a \leq m$. This is well-defined by the earlier observations. In particular,

$$\psi([(0, x)]) = \psi([(m, x + s)]) = (m, x + s).$$

Under this identification, we find that the cycle set as given in Theorem 5.3.1 is isomorphic to the cycle set on $\mathbb{Z}/m \times (\bigoplus_{i\in\mathbb{Z}} \mathbb{Z})/H$ given by

$$(a, x) \cdot (b, y) = (b - 1, y - \chi_0(b)s - c_{a-b} + c_{-b}).$$

Now instead of starting from $H \leq \bigoplus_{i\in\mathbb{Z}} \mathbb{Z}$ and $s \in \bigoplus_{i\in\mathbb{Z}} \mathbb{Z}/H$ we can also start with an abelian group $A$, an element $s \in A$ and a surjective group homomorphism $\phi : \bigoplus_{i\in\mathbb{Z}} \mathbb{Z} \to A$; we then set $H = \ker \phi$. As the $c_i$, $i \neq 0$, form a basis of $\bigoplus_{i\in\mathbb{Z}} \mathbb{Z}$, we can freely choose the images $\phi(c_i) \in A$ as long as $\phi(c_i) = \phi(c_{i+m})$. If we denote $\phi(c_i) = \Phi(i)$ we see that every such homomorphism $\phi$ uniquely corresponds to a map $\Phi : \mathbb{Z}/m \to A$ such that $\Phi(0) = 0$ and $\Phi(\mathbb{Z}/m)$ generates $A$. Using $\phi$ to identify $\bigoplus_{i\in\mathbb{Z}} \mathbb{Z}/H$ and $A$ we find a cycle set structure on $\mathbb{Z}/m \times A$ given by

$$(a, x) \cdot (b, y) = (b - 1, y - \chi_0(b)s - \Phi(a - b) + \Phi(-b)).$$

Recall that different choices of $H$ and $s$ give non-isomorphic cycle sets. It is clear that for two abelian groups $A, B$ and maps $\Phi : \mathbb{Z}/m \to A$ and $\Phi' : \mathbb{Z}/m \to B$, the associated homomorphisms $\phi$ and $\phi'$ have the same kernel $H$ if and only if there exists a group isomorphism $f : A \to B$ such that $\phi' = f\phi$, or equivalently $\Phi' = f\Phi$. Moreover, $s \in A$ and $s' \in B$ correspond to the same element in $\bigoplus_{i\in\mathbb{Z}} \mathbb{Z}/H$ precisely if $f(s) = s'$.

At last, define $g : \mathbb{Z}/m \to A$ as $g(b) = \sum_{i=0}^{b-1} \Phi(i)$ for $1 \leq b \leq m$. If $b \neq 0$, then $g(b+1) - g(b) = \Phi(b)$ and if $b = 0$ then $g(b + 1) - g(b) = -\sum_{i=1}^{m-1} \Phi(i)$. Under the bijection

$$\theta : (a, x) \mapsto (-a, -x + g(a)),$$

the cycle set structure now becomes

$$\begin{aligned}
\theta^{-1}(\theta(a, x) \cdot \theta(b, y)) &= \theta^{-1}((-a, -x + g(a)) \cdot (-b, -y + g(b))) \\
&= \theta^{-1}(-b - 1, -y + g(b) - \chi_0(b)s - \Phi(b - a) + \Phi(b)) \\
&= (b + 1, y - g(b) + \chi_0(b)s + \Phi(b - a) - \Phi(b) + g(b + 1)) \\
&= (b + 1, y + \chi_0(b)S + \Phi(b - a)),
\end{aligned}$$

where $S = s - \sum_{i=0}^{m-1} \Phi(i)$. To conclude the proof, note that if we are given an abelian group $B$, an isomorphism $f : A \to B$, and we set $\Phi' = f\Phi$, then $f(s) = s'$ if and only if

$$f(S) = f(s - \sum_{i=0}^{m-1} \Phi(i)) = s' - \sum_{i=1}^{m-1} \Phi'(i) = S'. \qquad \square$$

*Remark* 5.3.3. The solutions on $X = \mathbb{Z}/p \times A$ corresponding to the cycle sets in Theorem 5.3.2 are given by

$$r\begin{pmatrix}(a,x)\\(b,y)\end{pmatrix} = \begin{pmatrix}(b-1, y-\chi_0(b-1)S - \Phi(b-1-a))\\(a+1, x+\chi_0(a)S + \Phi(a-b+1))\end{pmatrix}.$$

**Corollary 5.3.4.** *Let $(X,\cdot)$ be a retractable indecomposable cycle set of size $p^2$ for $p$ a prime. Then $X$ has finite multipermutation level and is isomorphic to one of the following:*

1. *$X = \mathbb{Z}/p^2$ with $x \cdot y = y + 1$.*
2. *$X = \mathbb{Z}/p \times \mathbb{Z}/p$, with*

$$(a,x)\cdot(b,y) = (b+1, y+\chi_0(b)S + \Phi(b-a)),$$

*where $\Phi : \mathbb{Z}/p \to \mathbb{Z}/p$ is a non-constant map such that $\Phi(0) = 0$ and $S \in \mathbb{Z}/p$. The parameters $S, \Phi$ and $S', \Phi'$ define isomorphic cycle sets if and only if $S' = \alpha S$ and $\Phi' = \alpha\Phi$ for some $\alpha \in (\mathbb{Z}/p)^\times$.*

*Proof.* It follows from Proposition 1.2.27 that $|\operatorname{Ret}(X)| \in \{1, p\}$. If $|\operatorname{Ret}(X)| = 1$ then $X$ clearly has finite multipermutation level and is isomorphic to the given cycle set on $\mathbb{Z}/p^2$. If $|\operatorname{Ret}(X)| = p$, then we know that $\operatorname{Ret}(X)$ is isomorphic to the cycle set on $\mathbb{Z}/p$ with $x \cdot y = y + 1$ [73, Theorem 2.13]. In particular, $|\operatorname{Ret}^2(X)| = 1$ and thus $X$ has multipermutation level 2. The statement now follows directly from Theorem 5.3.2. □

## 5.4 Irretractable cycle sets whose permutation group is a $p$-group

### 5.4.1 Constructing the cycle sets

**Proposition 5.4.1.** *Let $(X,\cdot)$ be a finite irretractable cycle set such that $(\mathcal{G}(X,\cdot),\circ)$ is a $p$-group. Then $\operatorname{Soc}(\mathcal{G}(X,\cdot)) = \{0\}$ and $(\mathcal{G}(X,\cdot),\circ)$ is not abelian.*

*Proof.* As $X$ is irretractable, it follows from Corollary 4.1.9 that $\operatorname{Soc}(\mathcal{G}(X)) = \{0\}$. By Example 1.1.7 and Theorem 1.1.24 we find that $(\mathcal{G}(X),\circ)$ is not abelian, as otherwise its socle would be non-trivial. □

For the remainder of the section, we let $(X,\cdot)$ be an indecomposable irretractable cycle set of size $p^2$ and assume that its permutation group is a $p$-group. For simplicity, we write $\mathcal{G} = \mathcal{G}(X,\cdot)$. We also identify $X$ with its image in $\mathcal{G}$, which is a transitive cycle base of $\mathcal{G}$. By Lemma 5.1.1 and Proposition 5.4.1 we have a unique system of imprimitivity for the action of $\mathcal{G}$ on $X$. For $x \in X$ we denote by $\mathcal{B}_x$ the block containing $x$. We denote by $\mathcal{A}$ the abelian subgroup of $(\mathcal{G},\circ)$ which fixes the blocks set-wise. Note that $(\mathcal{A},\circ)$ has index $p$ in $(\mathcal{G},\circ)$.

**Proposition 5.4.2.** *The sets $\operatorname{Fix}(\mathcal{G})$ and $\mathcal{A}$ have trivial intersection.*

*Proof.* Suppose that $0 \neq f \in \operatorname{Fix}(\mathcal{G}) \cap \mathcal{A}$, without loss of generality we may assume that $f^{\circ p} = 0$, where we recall that $f^{\circ p}$ denotes the $p$-th power of $f$ in $(\mathcal{G},\circ)$. Recall from Lemma 5.2.1 that $\lambda_f$ coincides with conjugation by $f$ in the group $(\mathcal{G},\circ)$. Since $(\mathcal{A},\circ)$ is abelian, $\lambda_f$ fixes all elements in $\mathcal{A}$. By the comment in Example 1.1.7, we find

$$\operatorname{Fix}(\mathcal{G}) \cap Z(\mathcal{G},\circ) \subseteq \operatorname{Ann}(\mathcal{G}) = \{0\},$$

so $f \notin Z(\mathcal{G},\circ)$. Since $|\mathcal{G}|/|\mathcal{A}| = p$, we see that $\mathcal{A} = \{g \in \mathcal{G} \mid \lambda_f(g) = g\}$. As $\lambda_f$ is an automorphism, $\mathcal{A}$ is a subbrace of $\mathcal{G}$. By Proposition 5.2.3, $\mathcal{A}$ is an ideal of $\mathcal{G}$.

As $\mathcal{G}/\mathcal{A}$ is a brace of order $p$, it must be trivial and therefore the canonical map $\mathcal{G} \to \mathcal{G}/\mathcal{A}$ maps the transitive cycle base $X$ to a single element. Hence, there exists some $g \in \mathcal{G}$ such that for all $x \in X$ there exists some $a_x \in \mathcal{A}$ such that $x = g + a_x$. In particular, if we set $\gamma = f * g \in \mathcal{A}$, we find that also $f * x = f * g + f * a_x = \gamma$. By induction we find that $f^{\circ n} * x = n\gamma$ for all $n \geq 1$, since

$$\begin{aligned} f^{\circ n} * x &= \lambda_{f^{\circ n}}(x) - x \\ &= \lambda_f(\lambda_{f^{\circ n-1}}(x)) - \lambda_f(x) + \lambda_f(x) - x \\ &= \lambda_f(f^{\circ n-1} * x) + f * x \\ &= \lambda_f((n-1)\gamma) + \gamma = n\gamma. \end{aligned}$$

In particular, this implies that $p\gamma = 0$. If $\gamma = 0$, then $\lambda_f(x) = x$, for all $x \in X$ and therefore $\lambda_f = \mathrm{id}_{\mathcal{G}}$, which would imply that $f \in \mathrm{Soc}(\mathcal{G})$ and thus contradict Proposition 5.4.1. It therefore follows that $\gamma \neq 0$, which in turn implies that $\lambda_f$ has no fixed points on $X$. In particular, for each $a \in \mathcal{A}$ and $x \in X$, there exists some $n \geq 0$ such that $\lambda_a(x) = \lambda_f^n(x)$, hence $a * x = f^{\circ n} * x = n\gamma$.

Now let $I$ be the subgroup of $(\mathcal{G}, +)$ generated by

$$\{a * g \mid a \in \mathcal{A}, g \in \mathcal{G}\},$$

which is an ideal by [132, Corollary after Proposition 6]. Because $X$ generates $(\mathcal{G}, +)$ and $*$ is left distributive, $I$ is the subgroup of $(\mathcal{G}, +)$ generated by $\{a * x \mid a \in \mathcal{A}, x \in X\}$. By the previous discussion, $I = \{0, \gamma, \ldots, (p-1)\gamma\}$. As $|I| = p$, we find that $I \subseteq \mathrm{Fix}(\mathcal{G})$. Since $I$ is a minimal normal subgroup of the nilpotent group $(\mathcal{G}, \circ)$, we also find that $I \subseteq Z(\mathcal{G}, \circ)$, hence $I \subseteq \mathrm{Soc}(\mathcal{G})$ which is impossible. □

We now know that $\mathrm{Fix}(\mathcal{G}) \cap \mathcal{A} = 0$ but also from Theorem 1.1.24 we have $\mathrm{Fix}(\mathcal{G}) \neq 0$, hence $|\mathrm{Fix}(\mathcal{G})| = p$. This implies that the multiplicative group of $\mathcal{G}$ is the semidirect product

$$(\mathcal{G}, \circ) = (\mathcal{A}, \circ) \rtimes (\mathrm{Fix}(\mathcal{G}), \circ).$$

Therefore, $\mathcal{A}$ forms a system of representatives for $(\mathcal{G}, \circ)/\mathrm{Fix}(\mathcal{G})$. Since $\mathrm{Fix}(\mathcal{G})$ is a left ideal, its left cosets with respect to $(\mathcal{G}, +)$ and $(\mathcal{G}, \circ)$ coincide. We know that $\mathcal{A}$ is not necessarily closed under $+$, but by the above observation we can define $g \oplus h$ as the unique element in $\mathcal{A} \cap (g + h + \mathrm{Fix}(\mathcal{G}))$. As a consequence, the bijection

$$(\mathcal{A}, \oplus) \to (\mathcal{G}, +)/\mathrm{Fix}(\mathcal{G}),$$

is a group homomorphism.

**Proposition 5.4.3.** *The structure $(\mathcal{A}, \oplus, \circ)$ is a brace.*

*Proof.* For $a, b, c \in \mathcal{A}$, we calculate

$$\begin{aligned} \{a \circ b \ominus a \oplus a \circ c\} &= \mathcal{A} \cap (a \circ b - a + a \circ c + \mathrm{Fix}(\mathcal{G})) = \mathcal{A} \cap (a \circ (b + c) + \mathrm{Fix}(\mathcal{G})) \\ &= \mathcal{A} \cap \big((a + \mathrm{Fix}(\mathcal{G})) \circ (b + c + \mathrm{Fix}(\mathcal{G}))\big) \\ &= \big(\mathcal{A} \cap (a + \mathrm{Fix}(\mathcal{G}))\big) \circ \big(\mathcal{A} \cap (b + c + \mathrm{Fix}(\mathcal{G})\big) \\ &= \big(\mathcal{A} \cap (a + \mathrm{Fix}(\mathcal{G}))\big) \circ \{b \oplus c\} \\ &= \{a \circ (b \oplus c)\}. \end{aligned}$$

Hence $a \circ (b \oplus c) = a \circ b \ominus a \oplus a \circ c$. □

Denote by $\tilde{\mathcal{A}}$ the thus constructed brace on $\mathcal{A}$. We define the map

$$\rho : \mathcal{G} \to \tilde{\mathcal{A}},$$

where $\{\rho(g)\} = \mathcal{A} \cap (g \circ \mathrm{Fix}(\mathcal{G}))$. Note that $\rho$ is a group homomorphism $(\mathcal{G}, +) \to (\tilde{\mathcal{A}}, \oplus)$ but this is not necessarily true for $(\mathcal{G}, \circ) \to (\tilde{\mathcal{A}}, \circ)$. However, the restriction of $\rho$ to $\mathcal{A} \subseteq G$ is the identity map, hence in particular it respects the multiplicative operation. On $\tilde{\mathcal{A}}$, the $\lambda$-action is given by

$$\tilde{\lambda}_g(h) = \ominus g \oplus (g \circ h) = \ominus \rho(g) \oplus \rho(g \circ h) = \rho(-g + g \circ h) = \rho(\lambda_g(h)),$$

for $g, h \in \mathcal{A}$. This implies that the image $\rho(X) \subseteq \tilde{\mathcal{A}}$ is invariant under its $\tilde{\lambda}$-action (which is not necessarily transitive). Therefore, $\rho(X)$ is again a cycle set under the operation

$$\rho(x) \tilde{\cdot} \rho(y) = \tilde{\lambda}^{-1}_{\rho(x)}(\rho(y)).$$

**Proposition 5.4.4.** $|\rho(X)| = p$.

*Proof.* Note that $(\mathcal{G}, \circ)$ still acts transitively on $\rho(X)$ by $\lambda_g(\rho(x)) = \rho(\lambda_g(x))$ and that

$$\rho^{-1}(\rho(x)) \subseteq x + \mathrm{Fix}(\mathcal{G}).$$

In particular, $|\rho^{-1}(\rho(x))| \leq p$ and thus $|\tilde{X}| \in \{p, p^2\}$.

Suppose that $\rho : X \to \rho(X)$ is injective, then $(\mathcal{G}(\rho(X), \tilde{\cdot}), \circ)$ is isomorphic to $\mathcal{A}$ and each element of $\rho(X)$ acts differently on $\rho(X)$ by the $\tilde{\lambda}$-action, so $\rho(X)$ is irretractable. This contradicts Proposition 5.4.1 and thus $|\rho(X)| = p$. □

**Proposition 5.4.5.** *For all $x \in X$, we have the equality $\mathcal{B}_x = x + \mathrm{Fix}(\mathcal{G}) = x \circ \mathrm{Fix}(\mathcal{G})$. In particular, each block intersects $\mathcal{A}$ in precisely one element.*

*Proof.* By Proposition 5.4.4, for all $x \in X$, we have $x + \mathrm{Fix}(\mathcal{G}) \subseteq X$. As $(\mathcal{G}, \circ)$ leaves $\mathrm{Fix}(\mathcal{G})$ invariant under the $\lambda$-action, we deduce that the cosets $x + \mathrm{Fix}(\mathcal{G})$ form a non-trivial system of imprimitivity for the $\lambda$-action of $(\mathcal{G}, \circ)$ on $X$. Since we know from Lemma 5.1.1 that such a system is unique, this implies that $\mathcal{B}_x = x + \mathrm{Fix}(\mathcal{G})$.

Moreover, it was observed earlier that $\mathcal{A} \cap (g + \mathrm{Fix}(\mathcal{G}))$ is a singleton for each $g \in \mathcal{G}$. Together with the first part of this proposition, this gives the last part of the statement. □

**Proposition 5.4.6.** *Let $x \in X$, then $X = \mathrm{Fix}(\mathcal{G}) \circ x \circ \mathrm{Fix}(\mathcal{G})$.*

*Proof.* Let $0 \neq f \in \mathrm{Fix}(\mathcal{G})$. Then from Lemma 5.2.1 we get

$$f \circ \mathcal{B}_x \circ \overline{f} = \lambda_f(\mathcal{B}_x) \neq \mathcal{B}_x,$$

as $f \notin \mathcal{A}$. Therefore, $\mathrm{Fix}(\mathcal{G})$ acts transitively on the system of blocks by conjugation. Furthermore, by Proposition 5.4.5, $\mathrm{Fix}(\mathcal{G})$ acts transitively on every single block by right-multiplication. Therefore, each $y \in X$ is of the form $y = f \circ x \circ f \circ f'$ for some $f, f' \in \mathrm{Fix}(\mathcal{G})$. □

By Proposition 5.4.5, the set $X \cap \mathcal{A}$ is non-empty. Fix elements $\alpha_{0,0} \in X \cap \mathcal{A}$ and $0 \neq f \in \mathrm{Fix}(\mathcal{G})$. We now coordinatize the elements of $X$ in the following way: for $(a, x) \in \mathbb{Z}/p \times \mathbb{Z}/p$, we set

$$\alpha_{a,x} = \overline{f}^{\circ a} \circ \alpha_{0,0} \circ f^{\circ a} \circ f^{\circ x}.$$

By Proposition 5.4.6, this gives a unique coordinatization of the elements in $X$.

The map $\lambda_{\alpha_{0,0}}$ leaves all blocks invariant, therefore we can write $\lambda_{\alpha_{0,0}}(\alpha_{b,0}) = \alpha_{b,-\Phi(b)}$ for some map $\Phi : \mathbb{Z}/p \to \mathbb{Z}/p$. The cycle set operation $\cdot$ on $X$ can now be determined:

$$\begin{aligned}\alpha_{0,0} \cdot \alpha_{b,y} &= \lambda^{-1}_{\alpha_{0,0}}(\alpha_{b,-\Phi(b)} + (y + \Phi(b))f) \\ &= \alpha_{b,0} + (y + \Phi(b))f \\ &= \alpha_{b,y+\Phi(b)}.\end{aligned}$$

Also,

$$f^{\circ a} \cdot \alpha_{b,y} = \lambda_{\overline{f}^{\circ a}}\left(\overline{f}^{\circ b} \circ \alpha_{0,0} \circ f^{\circ b} \circ f^{\circ y}\right) = \overline{f}^{\circ(a+b)} \circ \alpha_{0,0} \circ f^{\circ(a+b)} \circ f^{\circ y} = \alpha_{a+b,y}.$$

from which we conclude that

$$\begin{aligned}\alpha_{a,x} \cdot \alpha_{b,y} &= f^{\circ(a+x)} \cdot (\alpha_{0,0} \cdot (\overline{f}^{\circ a} \cdot \alpha_{b,y})) \\ &= f^{\circ(a+x)} \cdot (\alpha_{0,0} \cdot \alpha_{b-a,y}) \\ &= f^{\circ(a+x)} \cdot \alpha_{b-a,y+\Phi(b-a)} \\ &= \alpha_{b+x,y+\Phi(b-a)}.\end{aligned}$$

**Theorem 5.4.7.** *Let $(X, \cdot)$ be an indecomposable, irretractable cycle set of size $p^2$ whose permutation group a $p$-group. Then $(X, \cdot)$ is isomorphic to a cycle set of the form $X = \mathbb{Z}/p \times \mathbb{Z}/p$ with*

$$(a, x) \cdot (b, y) = (b + x, y + \Phi(b - a))$$

*where $\Phi : \mathbb{Z}/p \to \mathbb{Z}/p$ is a non-constant map with $\Phi(A) = \Phi(-A)$, for all $A \in \mathbb{Z}/p$. Conversely, this construction always results in an indecomposable, irretractable cycle set whose permutation group is a $p$-group.*

*Proof.* In the preceding calculations, we have already established that the given multiplication rule is necessary. We now determine

$$\begin{aligned}((a, x) \cdot (b, y)) \cdot ((a, x) \cdot (c, z)) &= (b + x, y + \Phi(b - a)) \cdot (c + x, z + \Phi(c - a)) \\ &= (c + x + y + \Phi(b - a), z + \Phi(c - a) + \Phi(c - b)).\end{aligned}$$

Similarly,

$$((b, y) \cdot (a, x)) \cdot ((b, y) \cdot (c, z)) = (c + y + x + \Phi(a - b), z + \Phi(c - b) + \Phi(c - a)).$$

A comparison shows that in order for $(X, \cdot)$ to satisfy the first cycle set axiom, a necessary condition is that $\Phi(b - a) = \Phi(a - b)$ for all $a, b \in \mathbb{Z}/p$. This amounts to saying that $\Phi(A) = \Phi(-A)$, for all $A \in \mathbb{Z}/p$. By the same calculation, one sees that this condition on $\Phi$ is also sufficient. By construction, all maps $(b, y) \mapsto (a, x) \cdot (b, y)$ are bijective. Furthermore, the square map

$$\mathrm{Sq}(a, x) = (a, x) \cdot (a, x) = (a + x, x + \Phi(0))$$

is also bijective. Finally, irretractability is the same as saying that for any $a, a' \in \mathbb{Z}/p$, there is at least one $b \in \mathbb{Z}/p$ such that $\Phi(b - a) = \Phi(b - a')$. But this is equivalent to $\Phi$ not being constant.

Finally, for $b \in \mathbb{Z}/p$ with $\Phi(b) \neq 0$, we see that $(0, 0) \cdot (b, y) = (b, y + \Phi(b)) \neq (b, y)$ which shows that the orbit of $(b, y)$ contains at least the block $\{b\} \times \mathbb{Z}/p$. Since for example $(b, 1) \cdot (b, 0) = (b + 1, \Phi(0))$ is not contained in this block, we find that the orbit of $(b, y)$ is all of $X$, hence $X$ is indecomposable. Also note that $\mathcal{G}(X, \cdot)$ is contained in $\mathbb{Z}/p \wr \mathbb{Z}/p \leq \mathbb{S}_{\mathbb{Z}/p \times \mathbb{Z}/p}$, which implies that it is a $p$-group. □

We note the following corollary, which will be useful later in Section 5.5:

**Corollary 5.4.8.** *The elements in $X \cap \mathcal{A}$ generate the whole cycle set.*

*Proof.* Note that, using the explicit form in Theorem 5.4.7, we are considering the set

$$X \cap \mathcal{A} = \{(a, 0) \mid a \in \mathbb{Z}/p\}.$$

As $\Phi$ is non-constant, these elements generate the whole cycle set $X$. □

### 5.4.2 Getting rid of redundancy and determining automorphisms

The aim of this subsection is to determine unique representatives for the irretractable cycle sets determined in Section 5.4.1 and moreover, describe their automorphism groups.

Let $\mathcal{F}_p$ be the set of all non-constant maps $\Phi : \mathbb{Z}/p \to \mathbb{Z}/p$ with the property that $\Phi(A) = \Phi(-A)$, for all $A \in \mathbb{Z}/p$. $\mathcal{F}_p$ is acted upon by $(\mathbb{Z}/p)^\times$ via $({}^\alpha\Phi)(A) = \alpha^{-1}\Phi(\alpha A)$. From now on, let $\mathcal{S}_p$ be a fixed system of representatives for this action.

Recall from Theorem 5.4.7 that the cycle sets in the considered case are described as $\mathbb{Z}/p \times \mathbb{Z}/p$ with the operation

$$(a, x) \cdot (b, y) = (b + x, y + \Phi(b - a)),$$

where $\Phi \in \mathcal{F}_p$.

By Proposition 5.4.1, $(\mathcal{G}(X, \cdot), \circ)$ is non-abelian and by Lemma 5.1.1 it has a unique non-trivial system of imprimitivity that consists of the blocks $\{a\} \times \mathbb{Z}/p$. Assume that $X = \mathbb{Z}/p \times \mathbb{Z}/p$ comes with two cycle set operations $\cdot, \cdot'$ that are given by the parameters $\Phi, \Phi' \in \mathcal{F}_p$ and that $\phi : (X, \cdot) \to (X, \cdot')$ is an isomorphism. Then $\phi\mathcal{G}(X, \cdot)\phi^{-1} = \mathcal{G}(X, \cdot')$ so in particular $\phi$ must normalize the cyclic permutation action on the blocks and thus be of the form $\phi(a, x) = (\alpha a + \beta, \pi_a(x))$ for some $\pi_a \in \mathbb{S}_p$, $\alpha \in (\mathbb{Z}/p)^\times$, $\beta \in \mathbb{Z}/p$. We now calculate

$$\begin{aligned}
\phi((a, x) \cdot (b, y)) &= (\alpha(b + x) + \beta, \pi_{b+x}(y + \Phi(b - a))), \\
\phi(a, x) \cdot' \phi(b, y) &= (\alpha b + \beta + \pi_a(x), \pi_b(y) + \Phi'(\alpha(b - a)).
\end{aligned}$$

Equating these terms results in $\pi_a(x) = \alpha x$, considering the first coordinate. Taking this into account when considering the second coordinate leaves us with the equation

$$\alpha(y + \Phi(b - a)) = \alpha y + \Phi'(\alpha(b - a)) \Leftrightarrow \Phi(b - a) = \alpha^{-1}\Phi'(\alpha(b - a)).$$

This shows that $\Phi, \Phi'$ define isomorphic cycle sets if and only if there is an $\alpha \in (\mathbb{Z}/p)^\times$ such that $\Phi = {}^\alpha\Phi'$. Putting $\Phi = \Phi'$, the same considerations prove that $\phi$ provides an automorphism of a solution with parameter $\Phi$ if and only if $\phi(a, x) = (\alpha x + \beta, \alpha x)$ for $\alpha \in (\mathbb{Z}/p)^\times$, $\beta \in \mathbb{Z}/p$ with ${}^\alpha\Phi = \Phi$.

**Theorem 5.4.9.** *Let $p$ be a prime and let $(X, \cdot)$ be an indecomposable irretractable cycle set of size $p^2$ whose permutation group is a $p$-group. Then there is a unique $\Phi \in \mathcal{S}_p$ such that $X$ is isomorphic to the cycle set on $X = \mathbb{Z}/p \times \mathbb{Z}/p$ with multiplication*

$$(a, x) \cdot (b, y) = (b + x, y + \Phi(b - a)).$$

*The automorphisms of the latter are precisely the maps*

$$(a, x) \mapsto (\alpha a + \beta, \alpha x),$$

*for some $\alpha \in (\mathbb{Z}/p)^\times$, $\beta \in \mathbb{Z}/p$ with ${}^\alpha\Phi = \Phi$.*

## 5.5 All irretractable cycle sets

Throughout the whole section, we let $(X, \cdot)$ be an indecomposable irretractable cycle set of size $p^2$ and $\mathcal{G} = \mathcal{G}(X, \cdot)$. As we already covered the case where $\mathcal{G}$ is a $p$-group in Section 5.4, we can assume that $\mathcal{G}$ is not a $p$-group. Recall, however, that $\mathcal{G}$ is solvable. We associate $X$ with its image in $\mathcal{G}$, which is a transitive cycle base. As $X$ is irretractable, it follows from Corollary 4.1.9 that $\mathrm{Soc}(\mathcal{G}) = \{0\}$.

Let $\mathcal{G}_p$ be the Sylow $p$-subgroup of $(\mathcal{G}, +)$ and let $\mathcal{G}_{p'}$ be the Hall $p'$-subgroup of $(\mathcal{G}, +)$, both are characteristic in $(\mathcal{G}, +)$ hence they are left ideals of $\mathcal{G}$. We denote $X = \{x_1, \ldots, x_{p^2}\}$ and for $1 \leq i \leq p^2$ we define $y_i \in \mathcal{G}_p$ and $z_i \in \mathcal{G}_{p'}$ such that $x_i = y_i + z_i$. As the $\lambda$-action of $(\mathcal{G}_p, \circ)$ is transitive on $X$ and therefore also on $Y = \{y_i \mid 1 \leq i \leq p^2\}$, we find that $Y$ is a transitive cycle base of the brace $\mathcal{G}_p$. In particular, this implies that $|Y| \in \{1, p, p^2\}$.

Assume that $Y$ has finite multipermutation level. Let $q \neq p$ be a prime that divides $|\mathcal{G}|$ and let $\mathcal{G}_q$ be the Sylow $q$-subgroup of $(\mathcal{G}, +)$, which is a left ideal by the same reasoning as above. It follows from Lemma 5.2.4 that $\mathrm{Fix}_{\mathcal{G}}(\mathcal{G}_q)$ is a subbrace of $\mathcal{G}$ and thus $Y \cap \mathrm{Fix}_{\mathcal{G}}(\mathcal{G}_q)$ is a sub-cycle set of $Y$. By Theorem 4.4.1 we find that $Y \cap \mathrm{Fix}_{\mathcal{G}}(\mathcal{G}_q)$ is either empty or equal to $Y$. As $|Y|$ is a $p$-power, $\mathcal{G}_q$ fixes at least one point in $Y$ under the $\lambda$-action. This means that $Y \cap \mathrm{Fix}_{\mathcal{G}}(\mathcal{G}_q) = Y$ and thus $\mathcal{G}_p \subseteq \mathrm{Fix}_{\mathcal{G}}(\mathcal{G}_q)$. It follows that $(\mathcal{G}_p, \circ)$ normalizes $(\mathcal{G}_q, \circ)$ but as $(\mathcal{G}, \circ)$ acts faithful and transitive on a set of size $p^2$, this implies that $\mathcal{G}_q = \{0\}$ which contradicts the choice of $q$. We therefore deduce that $Y$ does not have finite multipermutation level. Together with the earlier observation that $|Y| \in \{1, p, p^2\}$, we conclude that $Y$ is irretractable of size $p^2$ and therefore as described in Theorem 5.4.7. In particular, we find that $(\mathcal{G}_p, \circ)$ is not abelian.

From now on, we consider the unique block system of $X$ under the action of $\mathcal{G}$. Recall that its uniqueness is guaranteed by Lemma 5.1.1. As before, we denote this block system by $\{\mathcal{B}_x \mid x \in X\}$. We denote the subgroup of $(\mathcal{G}, \circ)$ that fixes the blocks set-wise by $\mathcal{A}$. Then $\mathcal{A}_p$ is normal in $(\mathcal{G}, \circ)$ by Proposition 5.1.2. Also, we define $\mathcal{A}_p = \mathcal{A} \cap \mathcal{G}_p$ and $\mathcal{A}_{p'} = \mathcal{A} \cap \mathcal{G}_{p'}$. Note that $\mathcal{A}_p$ is a Sylow $p$-subgroup of $(\mathcal{A}, \circ)$ and $\mathcal{A}_{p'}$ is a Hall $p'$-subgroup of $(\mathcal{A}, \circ)$.

Let $a \in \mathcal{A}_p$ and $g \in \mathcal{G}_{p'}$, then Lemma 5.2.1 yields

$$\lambda_g(\overline{g} \circ a \circ g) = -g + a + \lambda_a(g),$$

hence

$$-a + \lambda_g(\overline{g} \circ a \circ g) = -g + \lambda_a(g).$$

As $-a + \lambda_g(\overline{g} \circ a \circ g)$ is contained in $\mathcal{G}_p$ and $-g + \lambda_a(g)$ is contained in $\mathcal{G}_{p'}$, we find that $\lambda_a(g) = g$. By Lemma 5.2.1 this implies that $g \circ a \circ \overline{g} = \lambda_g(a)$, so the $\lambda$-action of $\mathcal{G}_{p'}$ restricts to $\mathcal{A}_p$ and therefore also to $Y \cap \mathcal{A}_p$.

By Proposition 5.4.5 we know that $\mathcal{A}_p$ contains a unique representative of each block in the block system of $Y$ under the action of $(\mathcal{G}_p, \circ)$, thus also under the action of $(\mathcal{G}, \circ)$. This means that $\mathcal{A}_{p'}$ acts trivially on the set $Y \cap \mathcal{A}_p$ or equivalently $Y \cap \mathcal{A}_p \subseteq \mathrm{Fix}_{\mathcal{G}}(\mathcal{A}_{p'})$. From Lemma 5.2.4 we know that $\mathrm{Fix}_{\mathcal{G}}(\mathcal{A}_{p'})$ is a subbrace, since $\mathcal{A}_{p'} = \mathcal{A} \cap \mathcal{G}_{p'}$. In particular, $\mathrm{Fix}_{\mathcal{G}}(\mathcal{A}_{p'}) \cap Y$ is a sub-cycle set of $Y$ which contains $Y \cap \mathcal{A}_p$ which by Corollary 5.4.8 then implies that $\mathrm{Fix}_{\mathcal{G}}(\mathcal{A}_{p'}) \cap Y = Y$. However, as the $\lambda$-action of $\mathcal{G}$ on $Y$ is faithful, this means that $\mathcal{A}_{p'} = \{0\}$.

By Proposition 5.1.2 we find that $|\mathcal{G}_{p'}| < p$ and thus the $\lambda$-action of $\mathcal{G}_p$ on $\mathcal{G}_{p'}$ is trivial. As this same action acts transitively on $Z$, we find $|Z| = 1$. Let $Z = \{z\}$, then $\lambda_z$ is a brace automorphism of $\mathcal{G}_p$ by Lemma 5.2.1 and therefore also its restriction to $Y$ yields a cycle set automorphism. For any $x_i, x_j \in X$ we find

$$x_i \cdot x_j = (y_i + z) \cdot (y_j + z) = \lambda^{-1}_{y_i + z}(y_j + z) = \lambda_z^{-1}(y_i \cdot y_j) + z.$$

We find that the cycle set structure on $X$ is obtained by deforming the cycle set structure on $Y$ by an automorphism of $Y$. In Lemma 5.5.3 we will show that such a deformation is always possible.

*Remark* 5.5.1. We remark that the idea of starting from a finite cycle set $X$ and then considering its projection $Y$ onto the Sylow $p$-subgroup $\mathcal{G}_p$ is strongly related to the notion of cabling as described in Section 1.2.5. This connection was also explored in [74].

More precisely, let $|\mathcal{G}(X,\cdot)| = p^r m$ where $(p,m) = 1$. As for any non-zero multiple $k$ of $m$ the Sylow $p$-subgroup $\mathcal{G}(X,\cdot)_p$ of $(\mathcal{G}(X,\cdot),+)$ can be written as $\mathcal{G}(X,\cdot)_p = \{kg \mid g \in \mathcal{G}\}$, we find that $\mathcal{G}(X,\cdot)_p = \mathcal{G}(X,\cdot^{(k)})$, where $(X,\cdot^{(k)})$ denotes the $k$-cabling of $(X,\cdot)$. In particular, $\mathrm{Ret}(X,\cdot^{(k)})$ isomorphic to the cycle set $\{k\sigma_x \mid x \in X\} \subseteq \mathcal{G}(X,\cdot)$ where the equivalence class of $x$ is mapped to $k\sigma_x$. If we let $k$ be such that $k \equiv 1 \mod p^r$ then we find that $k\sigma_x$ is precisely the projection of $\sigma_x$ onto $\mathcal{G}(X,\cdot)_p$, hence in this case we find that $Y \cong \mathrm{Ret}(X,\cdot^{(k)})$, with $Y$ as before.

**Proposition 5.5.2.** *Let $(X,\cdot)$ be an indecomposable cycle set of order $p^n$, with $p$ a prime. Let $k$ be the largest divisor of $|\mathcal{G}(X,\cdot)|$ coprime to $p$. If $(X,\cdot^{(k)})$ has finite multipermutation level, then $\mathcal{G}(X,\cdot)$ is a $p$-group and thus $k = 1$.*

*Proof.* The proof follows essentially the same reasoning as earlier in this section, where we proved that $Y$ is not of finite multipermutation level.

First of all, as $(\mathcal{G}(X,\cdot^{(k)}),\circ)$ is a Sylow $p$-subgroup, $(X,\cdot^{(k)})$ is still an indecomposable cycle set. Now consider the sub-cycle set

$$Y = \{k\sigma_x \mid x \in X\} \cong \mathrm{Ret}(X,\cdot^{(k)}).$$

As $(X,\cdot^{(k)})$ has finite multipermutation level, so does $Y$.

Let $q \neq p$ be a prime and let $\mathcal{G}(X,\cdot)_q$ be the Sylow $q$-subgroup of $(\mathcal{G}(X,\cdot),+)$. If we consider the $\lambda$-action of $\mathcal{G}(X,\cdot)_q$ on $Y$, we find that it has fixed points. Since $\mathrm{Fix}(\mathcal{G}(X,\cdot)_q)$ is a subbrace of $\mathcal{G}(X,\cdot)_q$ we find that $\mathrm{Fix}(\mathcal{G}(X,\cdot)_q) \cap Y$ is a sub-cycle set of $Y$. As this sub-cycle set is non-empty, Theorem 4.4.1 implies that $Y \subseteq \mathrm{Fix}(\mathcal{G}(X,\cdot)_q)$ and hence $\mathcal{G}(X,\cdot)_p \subseteq \mathrm{Fix}(\mathcal{G}(X,\cdot)_q)$. As a result, $\mathcal{G}(X,\cdot)_q$ is a normal subgroup of $(\mathcal{G}(X,\cdot),\circ)$, but this is impossible as $(\mathcal{G}(X,\cdot),\circ)$ acts transitively and faithfully on a set of $p$-power order. We conclude that $\mathcal{G}(X,\cdot)$ must be a $p$-group, and thus $k = 1$. □

**Lemma 5.5.3.** *Let $(X,\cdot)$ be a cycle set and let $\phi$ be an automorphism of $(X,\cdot)$. Then the following statements hold:*

1. *$X$ is a cycle set for the operation $x \cdot_\phi y = \phi(x \cdot y)$.*
2. *If $(X,\cdot)$ is irretractable, then so is $(X,\cdot_\phi)$.*

*Proof.* By the functoriality of the construction of the structure brace $G(X,\cdot)$, we get an induced automorphism $\phi'$ of $G(X,r)$ which restricts to $\phi$ on the generating set $X \subseteq G(X,\cdot)$. We let $\mathrm{Triv}(\mathbb{Z})$ act on $G(X,\cdot)$ where $1$ acts by the automorphism $(\phi')^{-1}$, and consider the semidirect product

$$G(X,\cdot) \rtimes \mathrm{Triv}(\mathbb{Z}).$$

The set $X \times \{1\} \subseteq G(X,\cdot) \rtimes \mathrm{Triv}(\mathbb{Z})$ is closed under the $\lambda$-action. Hence, it forms a sub-cycle set that is precisely the cycle set described in the statement, up to the correspondence $x \mapsto (x,1)$.

If $(X,\cdot)$ is irretractable, then also $(X,\cdot_\phi)$ is irretractable as for any $x,y,z \in X$ it follows directly that $x \cdot z = y \cdot z$ if and only if $x \cdot_\phi z = y \cdot_\phi z$. □

**Lemma 5.5.4.** *Let $(X,\cdot)$ be a finite cycle set and $\phi$ an automorphism of $(X,\cdot)$ of order $m$ coprime to $|\mathcal{G}(X)|$ such that $\phi$ has a fixed point. Then*

$$\mathcal{G}(X,\cdot_\phi) = \mathcal{G}(X,\cdot) \rtimes \langle\phi\rangle,$$

*as subgroups of* $\mathbb{S}_X$ *and*

$$\mathcal{G}(X,\cdot_\phi) \cong \mathcal{G}(X,\cdot) \rtimes \mathrm{Triv}(\mathbb{Z}/m),$$

*as braces where* $1 \in \mathbb{Z}/m$ *acts on* $\mathcal{G}(X,\cdot)$ *by mapping* $\sigma_x$ *to* $\sigma_{\phi^{-1}(x)}$*. In particular, if* $(X,\cdot)$ *is indecomposable then so is* $(X,\cdot_\phi)$ *and* $(X,\cdot) = (X,(\cdot_\phi)^{(k)})$ *for any* $k \in \mathbb{Z}$ *such that* $k \equiv 0 \mod m$ *and* $k \equiv 1 \mod |\mathcal{G}(X)|$.

*Proof.* First of all, note that for $x \in X$, its $\sigma$-map with respect to the cycle set $(X,\cdot_\phi)$ is given by $\sigma_x\phi^{-1}$, where $\sigma_x$ is its $\sigma$-map with respect to the original cycle set $(X,\cdot)$. Explicitly, we have

$$\mathcal{G}(X,\cdot) = \langle \sigma_x \mid x \in X\rangle, \quad \mathcal{G}(X,\cdot_\phi) = \langle \phi^{-1}\sigma_x \mid x \in X\rangle.$$

Let $x \in X$ such that $\phi(x) = x$, then $\phi\sigma_x = \sigma_x\phi$ and thus $(\phi^{-1}\sigma_x)^n = \phi^{-n}\sigma_x^n$ for all $n \in \mathbb{Z}$. If we choose $n$ such that $n \equiv 0 \mod |\mathcal{G}(X,\cdot)|$ and $n \equiv 1 \mod m$, then $\phi^{-1} = (\phi^{-1}\sigma_x)^n \in \mathcal{G}(X,\cdot_\phi)$. It follows that $\mathcal{G}(X,\cdot_\phi)$ is generated by $\{\sigma_x \mid x \in X\} \cup \{\phi\}$. Since $\phi\sigma_x\phi^{-1} = \sigma_{\phi(x)}$, we find that $\phi$ normalizes $\mathcal{G}(X,\cdot)$ and since $\mathcal{G}(X,\cdot) \cap \langle\phi\rangle$ because their sizes are coprime, we conclude that $\mathcal{G}(X,\cdot_\phi) = \mathcal{G}(X,\cdot) \rtimes \langle\phi\rangle$ in $\mathbb{S}_X$.

Next, consider the semidirect product of braces $\mathcal{G}(X,\cdot) \rtimes \mathrm{Triv}(\mathbb{Z}/m)$ where $1 \in \mathbb{Z}/m$ acts by the automorphism $\sigma_x \mapsto \sigma_{\phi^{-1}(x)}$. Note that the map

$$X \times \mathbb{Z}/m \to \mathbb{S}_X : (x,n) \mapsto \sigma_x\phi^{-1},$$

extends to a group homomorphism $g : (\mathcal{G}(X,\cdot),\circ) \rtimes \mathbb{Z}/m \to \mathbb{S}_X$ since

$$g((0,1)(x,0)(0,-1)) = g(\phi^{-1}(x)) = \sigma_{\phi^{-1}} = \phi^{-1}\sigma_x\phi = g(0,1)g(x,0)g(0,-1).$$

Also for $x,y \in X$, $\lambda^{-1}_{(x,1)}(y,1) = (\phi(\lambda_x^{-1}(y),1)$ and thus

$$X \to \mathcal{G}(X,\cdot) \rtimes \mathrm{Triv}(\mathbb{Z}/m) : x \mapsto (x,1),$$

is a homomorphism of cycle sets, where we see $\mathcal{G}(X,\cdot) \rtimes \mathrm{Triv}(\mathbb{Z}/m)$ as a cycle set in the canonical way. By Theorem 1.2.21 we find a brace homomorphism $f : G(X,\cdot_\phi) \to \mathcal{G}(X,\cdot) \rtimes \mathrm{Triv}(\mathbb{Z}/m)$. Since the composition $gf : (G(X,\cdot_\phi),\circ) \to \mathbb{S}_X$ maps $x$ to $\sigma_x\phi^{-1}$, we find that $\ker gf = \ker f$ is precisely the socle of $G(X,\cdot_\phi)$ and thus we conclude that

$$\mathcal{G}(X,\cdot_\phi) \cong G(X,\cdot_\phi)/\ker f \cong \mathcal{G}(X,\cdot) \rtimes \mathrm{Triv}(\mathbb{Z}/m).$$

The first part of the statement implies that $(X,\cdot_\phi)$ is indecomposable when $(X,\cdot)$ is indecomposable and the last part of the statement follows from Remark 5.5.1. □

**Lemma 5.5.5.** *Let* $(X,\cdot)$*,* $(X,\cdot')$ *be finite cycle sets and let* $\phi \in \mathrm{Aut}(X,\cdot)$*,* $\psi \in \mathrm{Aut}(X,\cdot')$ *be such that* $|\mathcal{G}(X,\cdot)||\mathcal{G}(X,\cdot')|$ *is coprime to the orders of* $\phi$ *and* $\psi$*. Assume also that* $\phi$ *and* $\psi$ *both have a fixed point. Then* $f : (X,\cdot_\phi) \to (X,\cdot'_\psi)$ *is an isomorphism if and only if* $f : (X,\cdot) \to (X,\cdot')$ *is an isomorphism and* $\psi = f\phi f^{-1}$*. In particular,* $\mathrm{Aut}(X,\cdot_\phi)$ *is precisely the centralizer of* $\phi$ *in* $\mathrm{Aut}(X,\cdot)$.

*Proof.* Assume that $f : (X,\cdot_\phi) \to (X,\cdot'_\psi)$ is an isomorphism. From Lemma 5.5.4 and the assumptions we find the existence of some $k \in \mathbb{Z}$ such that $(X,(\cdot_\phi)^{(k)}) = (X,\cdot)$ and $(X,(\cdot'_\psi)^{(k)}) = (X,\cdot')$. The functoriality of cabling now yields that $f$ induces an isomorphism $f : (X,\cdot) \to (X,\cdot')$. For any $x,y \in X$ we find $f(x \cdot_\phi y) = f\phi(x \cdot y)$ and $f(x) \cdot_\psi f(y) = \psi f(x \cdot y)$, hence $f(x \cdot_\phi y) = f(x) \cdot_\psi f(y)$ if and only if $\psi = f\phi f^{-1}$. This proves one implication of the statement.

Conversely, assume that $f : (X,\cdot) \to (X,\cdot')$ is an isomorphism and $\psi = f\phi f^{-1}$. Then

$$f(x \cdot_\phi y) = f\phi(x \cdot y) = \psi(f(x \cdot y)) = \psi(f(x) \cdot' f(y)) = f(x) \cdot'_\psi f(y),$$

for all $x,y \in X$. □

**Theorem 5.5.6.** *Let $(X,\cdot)$ be an irretractable cycle set of size $p^2$ where $p$ is a prime. Then there exists a unique $\Phi \in \mathcal{S}_p$ and $\alpha \in (\mathbb{Z}/p)^\times$ satisfying ${}^\alpha\Phi = \Phi$ such that $X$ is isomorphic to the cycle set on $\mathbb{Z}/p \times \mathbb{Z}/p$ with multiplication*

$$(a,x)\cdot(b,y) = (\alpha b + \alpha x, \alpha y + \alpha\Phi(b-a)).$$

*If $\alpha = 1$, then the cycle sets are the ones that appear in Theorem 5.4.9. If $\alpha \neq 1$, then any automorphism of $(X,\cdot)$ is of the form $(a,x) \mapsto (\gamma a, \gamma x)$ for some $\gamma \in (\mathbb{Z}/p)^\times$ with ${}^\gamma\Phi = \Phi$.*

*Proof.* From the discussion preceding Lemma 5.5.3 we know that $(X,\cdot)$ can be obtained by starting from a cycle set structure on $X$ whose permutation group is a $p$-group and deforming such a cycle set by an automorphism of order coprime to $p$, in the sense of Lemma 5.5.3. From Theorem 5.4.9 it follows that, up to a cycle set isomorphism, $X = \mathbb{Z}/p \times \mathbb{Z}/p$ and

$$(a,x)\cdot(b,y) = (\alpha b + \alpha x + \beta, \alpha y + \alpha\Phi(b-a)),$$

for some $\Phi \in \mathcal{S}_p$, $\alpha \in (\mathbb{Z}/p)^\times$ and $\beta \in \mathbb{Z}/p$, satisfying ${}^\alpha\Phi = \Phi$. By Lemma 5.5.5 we may even assume $\beta = 0$. We therefore get that up to isomorphism the multiplication on $X$ is precisely as in the statement.

Conversely, it follows directly from Lemma 5.5.3 and Lemma 5.5.4 that $\mathbb{Z}/p \times \mathbb{Z}/p$ with the given multiplication always yields an indecomposable irretractable cycle set. As a consequence of Lemma 5.5.5, we find that different choices of $\alpha$ and $\Phi$ yield non-isomorphic solutions and also that the automorphisms are the ones described in the statement. Note in particular that the necessary conditions are satisfied since any point $(0,0)$ is always fixed under the considered automorphisms. □

*Remark* 5.5.7. Observe that if $\alpha \neq 1$ in Theorem 5.5.6, then $|\mathcal{G}(X,\cdot)|$ has prime divisors different from $p$. This means that the permutation braces of these solutions are all examples of singular brace as defined in [138].

## 5.6 Summary

We summarize our classification result in the following theorem.

**Theorem 5.6.1.** *Let $(X,\cdot)$ be an indecomposable cycle set of size $p^2$ for $p$ a prime. Then $X$ is isomorphic to a cycle set of one of the following forms:*

1. *$X = \mathbb{Z}/p^2$, with $x \cdot y = y + 1$.*
2. *$X = \mathbb{Z}/p \times \mathbb{Z}/p$, with*

$$(a,x)\cdot(b,y) = (b+1, y + \chi_0(b)S + \Phi(b-a)),$$

*where $\Phi : \mathbb{Z}/p \to \mathbb{Z}/p$ is a non-constant map with $\Phi(0) = 0$, $S \in \mathbb{Z}/p$ and $\chi_0 : \mathbb{Z}/p \to \mathbb{Z}/p$ with*

$$\chi_0(x) = \begin{cases} 1 & x = 0 \\ 0 & x \neq 0 \end{cases}.$$

*The parameters $S, \Phi$ and $S', \Phi'$ define isomorphic cycle sets if and only if $S = S'$ and $\alpha\Phi = \Phi'$ for some $\alpha \in (\mathbb{Z}/p)^\times$.*

3. $X = \mathbb{Z}/p \times \mathbb{Z}/p$, *with*
$$(a, x) \cdot (b, y) = (\alpha b + \alpha x, \alpha y + \alpha\Phi(b - a)),$$
*where* $\Phi : \mathbb{Z}/p \to \mathbb{Z}/p$ *is a non-constant map with* $\Phi(x) = \Phi(-x)$ *and* $\alpha \in (\mathbb{Z}/p)^\times$ *is such that* $\Phi(\alpha x) = \alpha\Phi(x)$. *The parameters* $\alpha, \Phi$ *and* $\alpha', \Phi'$ *define isomorphic cycle sets if and only if* $\alpha = \alpha'$ *and there is a* $\beta \in (\mathbb{Z}/p)^\times$ *such that* $\beta^{-1}\Phi(\beta x) = \Phi'(x)$, *for all* $x \in \mathbb{Z}/p$.

*These three cases are mutually exclusive.*

*Proof.* Corollary 5.3.4 tells us that the indecomposable cycle sets of size $p^2$ that have finite multipermutation level 1 and 2, are exactly the ones described in cases 1 and 2 respectively. On the other hand, the irretractable cycle sets are classified, up to isomorphism, in Theorem 5.5.6 and make up case 3. □

### 5.6.1 Indecomposable set-theoretical solutions of size $p^2$

Recall that given a cycle set on $X$, the associated solution is given by
$$r_X(x, y) = (\sigma_x(y), \sigma_{\sigma_x(y)}(x)),$$
where we recall that $\sigma_x$ is the inverse of the bijection $y \mapsto x \cdot y$. Therefore, we can obtain all indecomposable solutions of size $p^2$ simply translating the cycle sets obtained in Theorem 5.6.1 to set-theoretical solutions. For the first one we obtain $r(x, y) = (y - 1, x + 1)$ since $\sigma_x^{-1}(y) = y + 1$.

For the second family of cycle sets we find $\sigma^{-1}_{(a,x)}(b, y) = (b + 1, y + S\chi_0(b) + \Phi(b - a))$, hence
$$\sigma_{(a,x)}(b, y) = (b - 1, y - S\chi_0(b - 1) - \Phi(b - 1 - a)),$$
and
$$\begin{aligned}\tau_{(b,y)}(a, x) &= \sigma_{(a,x)}(b, y) \cdot (a, x) = (b - 1, y - S\chi_0(b - 1) - \Phi(b - 1 - a)) \cdot (a, x)\\ &= (a + 1, x + S\chi_0(a) + \Phi(a - b + 1)).\end{aligned}$$
Thus, the associated solution is
$$r\begin{pmatrix}(a, x)\\(b, y)\end{pmatrix} = \begin{pmatrix}(b - 1, y - S\chi_0(b - 1) - \Phi(b - 1 - a))\\(a + 1, x + S\chi_0(a) + \Phi(a - b + 1))\end{pmatrix}.$$
Finally, for the last family, we have $\sigma^{-1}_{(a,x)}(b, y) = (\alpha b + \alpha x, \alpha y + \alpha\Phi(b - a))$. Using the fact that $\Phi(\alpha x) = \alpha\Phi(x)$ for all $x \in \mathbb{Z}/p$, we find
$$\sigma_{(a,x)}(b, y) = \left(\alpha^{-1}b - x, \alpha^{-1}y - \Phi\left(\alpha^{-1}b - x - a\right)\right),$$
and
$$\begin{aligned}\tau_{(b,y)}(a, x) &= \sigma_{(a,x)}(b, y) \cdot (a, x) = \left(\alpha^{-1}b - x, \alpha^{-1}y - \Phi\left(\alpha^{-1}b - x - a\right)\right) \cdot (a, x)\\ &= \left(\alpha a + \alpha\left(\alpha^{-1}(y - \Phi(b - \alpha x - \alpha a))\right), \alpha x + \alpha\Phi\left(a - \alpha^{-1}(b - \alpha x)\right)\right)\\ &= (\alpha a + y - \Phi(b - \alpha x - \alpha a), \alpha x + \Phi(\alpha a - b + \alpha x)).\end{aligned}$$
Thus the associated solution is
$$r\begin{pmatrix}(a, x)\\(b, y)\end{pmatrix} = \begin{pmatrix}(\alpha^{-1}b - x, \alpha^{-1}y - \Phi(\alpha^{-1}b - x - a)))\\(\alpha a + y - \Phi(b - \alpha x - \alpha a), \alpha x + \Phi(\alpha a - \alpha x - b))\end{pmatrix}.$$

**Theorem 5.6.2.** *Each indecomposable non-degenerate involutive set-theoretical solution $(X, r)$ of the Yang–Baxter equation of size $p^2$ for some prime $p$ is isomorphic to one of the following solutions:*

1. *$X = \mathbb{Z}/p^2$, with $r(x, y) = (y + 1, x - 1)$.*
2. *$X = \mathbb{Z}/p \times \mathbb{Z}/p$, with*

$$r\begin{pmatrix}(a,x)\\(b,y)\end{pmatrix} = \begin{pmatrix}(b-1, y-\chi_0(b-1)S - \Phi(b-1-a))\\(a+1, x+\chi_0(a)S + \Phi(a-b+1))\end{pmatrix}$$

*where $\Phi : \mathbb{Z}/p \to \mathbb{Z}/p$ is a non-constant map with $\Phi(0) = 0$, $S \in \mathbb{Z}/p$ and $\chi_0 : \mathbb{Z}/p \to \mathbb{Z}/p$ with*

$$\chi_0(x) = \begin{cases} 1 & x = 0 \\ 0 & x \neq 0 \end{cases}.$$

*The parameters $S, \Phi$ and $S', \Phi'$ define isomorphic solutions if and only if $S = S'$ and $\alpha\Phi = \Phi'$ for some $\alpha \in (\mathbb{Z}/p)^\times$.*

3. *$X = \mathbb{Z}/p \times \mathbb{Z}/p$, with*

$$r\begin{pmatrix}(a,x)\\(b,y)\end{pmatrix} = \begin{pmatrix}(\alpha^{-1}b - x, \alpha^{-1}y - \Phi(\alpha^{-1}b - x - a))\\(\alpha a + y - \Phi(b - \alpha x - \alpha a), \alpha x + \Phi(\alpha a - \alpha x - b))\end{pmatrix}$$

*where $\Phi : \mathbb{Z}/p \to \mathbb{Z}/p$ is a non-constant map with $\Phi(x) = \Phi(-x)$ and $\alpha \in (\mathbb{Z}/p)^\times$ is such that $\Phi(\alpha x) = \alpha\Phi(x)$.*

*The parameters $\alpha, \Phi$ and $\alpha', \Phi'$ define isomorphic solutions if and only if $\alpha = \alpha'$ and there is a $\beta \in (\mathbb{Z}/p)^\times$ such that $\beta^{-1}\Phi(\beta x) = \Phi'(x)$ for all $x \in \mathbb{Z}/p$.*

In fact, these solutions are isomorphic to those constructed in [53, Theorem 5.1] as we will show in the remainder of this section. In particular, this answers [53, Question 7.3] affirmatively. We first recall the definition of a simple solution, see also [44, 65, 94] for a complete characterization of such solutions in terms of their permutation skew brace.

**Definition 5.6.3.** A solution $(X, r)$ is *simple* if for any solution $(Y, s)$ and any surjective homomorphism $f : (X, r) \to (Y, s)$, we have that either $f$ is an isomorphism or $|Y| = 1$.

**Theorem 5.6.4** ([53, Theorem 5.1])**.** *Let $p$ be a prime number. Let $t \in \mathbb{Z}/p$ be a non-zero element. Let $f : \mathbb{Z}/p \to \mathbb{Z}/p$ be a map such that:*

(S1) *$f(i) = f(-i)$, for all $i \in \mathbb{Z}/p$.*

(S2) *$f(t^s i) = t^s f(i) - (t^s - 1)f(0)$, for all $i \in \mathbb{Z}/p$ and $s \in \mathbb{Z}$.*

(S3) *$f$ is not a constant map.*

*Let $X = \mathbb{Z}/p \times \mathbb{Z}/p$ and $r : X^2 \to X^2$ be the map*

$$r\begin{pmatrix}(i,j)\\(k,l)\end{pmatrix} = \begin{pmatrix}\lambda_{(i,j)}(k,l)\\\lambda^{-1}_{\lambda_{(i,j)}(k,l)}(i,j)\end{pmatrix},$$

*where $\lambda_{(i,j)}(k, l) = (tk + j, t(l - f(tk + j - i)))$. Then $(X, r)$ is a simple solution of the YBE.*

We will denote the solution associated with cycle sets of the form *(3)* in Theorem 5.6.1 with parameters $\Phi, \alpha$ as $r^{\alpha,\Phi}$ with first component

$$\lambda^{\Phi,\alpha}_{(a,x)} : (b, y) \mapsto (\alpha^{-1}b - x, \alpha^{-1}y - \Phi(\alpha^{-1}b - x - a))).$$

Similarly, we will denote the solution constructed in Theorem 5.6.4 with parameters $f, t$ as $r^{f,t}$ with first component

$$\sigma^{f,t}_{(i,j)} : (k, l) \mapsto (tk + j, t(l - f(tk + j - i))).$$

With this notation and fixing $X = \mathbb{Z}/p \times \mathbb{Z}/p$, it is easy to prove that the map $\Psi(i, j) = (i, -j)$ is an isomorphism of solutions $\Psi : (X, r^{\Phi,\alpha}) \to (X, r^{f_{\Phi,\alpha},\alpha^{-1}})$, where $f_{\Phi,\alpha} : i \mapsto -\Phi(\alpha i)$, since

$$\begin{aligned}
\lambda^{\Phi,\alpha}_{\Psi(i,j)}(\Psi(k, l)) &= \lambda^{\Phi,\alpha}_{(i,-j)}((k, -l)) = (\alpha^{-1}(k + \alpha j), \alpha^{-1}(-l - \Phi(k + \alpha j - \alpha i))) \\
&= (\alpha^{-1}k + j, \alpha^{-1}(-l + f_{\Phi,\alpha}(\alpha^{-1}k + j - i))) \\
&= \Psi(\alpha^{-1}k + j, \alpha^{-1}(l - f_{\Psi,\alpha}(k + \alpha j - \alpha i)) \\
&= \Psi\left(\sigma^{f_{\Phi,\alpha},\alpha^{-1}}_{(i,j)}(k, l)\right).
\end{aligned}$$

It remains to show that, with the conditions for $\Phi$ and $\alpha$ given in Theorem 5.6.1, the parameters $f = f_{\Phi,\alpha}$ and $t = \alpha^{-1}$ satisfy the properties required by Theorem 5.6.4. Since $\Phi$ satisfies *(S1)* and *(S3)*, so does $f_{\Phi,\alpha}$. Moreover, since $\Phi(\alpha i) = \alpha\Phi(i)$, we have that

$$f_{\Phi,\alpha}(\alpha^{-s}i) = -\Phi(\alpha\alpha^{-s}i) = -\alpha^{-s}\Phi(\alpha i) = \alpha^{-s}f_{\Phi,\alpha}(i).$$

Hence $f_{\Phi,\alpha}$ satisfies *(S2)* if and only if $(\alpha^{-s} - 1)f_{\Phi,\alpha}(0) = 0$ for all $s \in \mathbb{Z}$, which is equivalent to $(\alpha - 1)\Phi(0) = 0$. But the latter is a consequence of the properties of $\Phi$ and $\alpha$ as $\Phi(0) = \Phi(\alpha 0) = \alpha\Phi(0)$.

### 5.6.2 Enumeration of indecomposable, irretractable cycle sets of size $p^2$

In this subsection, we will use the following convention extending the notation introduced in Section 5.2: for a group $G$ acting on a set $X$ by an action $(g, x) \mapsto {}^g x$, we denote the set of fixed points by

$$\mathrm{Fix}_X(G) = \{x \in X \mid {}^g x = x \text{ for all } g \in G\}.$$

Recall that we defined $\mathcal{F}_p$ as the set of all non-constant maps $\Phi : \mathbb{Z}/p \to \mathbb{Z}/p$ such that $\Phi(-A) = \Phi(A)$ for all $A \in \mathbb{Z}/p$. It is acted upon by the group $(\mathbb{Z}/p)^\times$ with the action given by ${}^\alpha\Phi : A \mapsto \alpha^{-1}\Phi(\alpha A)$.

By Theorem 5.6.1, every irretractable cycle set can be described by a pair $(\Phi, \alpha)$ where $\Phi \in \mathcal{F}_p$ and $\alpha \in (\mathbb{Z}/p)^\times$ such that ${}^\alpha\Phi = \Phi$. Furthermore, $(\Phi, \alpha)$ and $(\Phi', \alpha')$ define isomorphic cycle sets, if and only if $\alpha = \alpha'$ and $\Phi' = {}^\beta\Phi$ for some $\beta \in (\mathbb{Z}/p)^\times$. It follows directly that for $p = 2$ we find 2 non-isomorphic indecomposable irretractable cycle sets of size 4.

Assume $p \neq 2$ from now on. For a pair $(\Phi, \alpha)$ with $\Phi(0) \neq 0$, the condition $\Phi(\alpha A) = \alpha\Phi(A)$ forces $\alpha = 1$. As $\Phi(0) \neq 0$, there is exactly one $\beta \in (\mathbb{Z}/p)^\times$ such that ${}^\beta\Phi(0) = 1$. Therefore, each cycle set with parameters $(\Phi, \alpha)$, $\Phi(0) \neq 0$, is isomorphic to a unique cycle set with parameters $(\tilde{\Phi}, 1)$ where $\tilde{\Phi}(0) = 1$, and these parameters define mutually non-isomorphic cycle sets. We find $n_p = p^{\frac{p-1}{2}} - 1$ such cycle sets.

This leaves the case where $\Phi(0) = 0$. We define

$$\mathcal{F}'_p = \{\Phi \in \mathcal{F}_p \mid \Phi(0) = 0\}.$$

We first calculate, for a fixed $\alpha \in (\mathbb{Z}/p)^\times$, the number of isomorphism classes of cycle sets with parameters contained in the set

$$\{(\Phi, \alpha) \mid \Phi \in \mathcal{F}'_p, {}^\alpha\Phi = \Phi, \Phi(0) = 0\},$$

or equivalently, the number of orbits of $\mathrm{Fix}_{\mathcal{F}'_p}(\langle\alpha\rangle)$ under the action of $(\mathbb{Z}/p)^\times$.

Let $d$ denote the multiplicative order of $\alpha$. The condition $p \neq 2$ implies that $\mathrm{Fix}_{\mathcal{F}'_p}(\langle\alpha\rangle)$ is empty for $\alpha = -1$, as $\Phi(A) = \Phi(-A)$. More generally, the same applies whenever $-1 \in \langle\alpha\rangle \leq (\mathbb{Z}/p)^\times$. This means that we can restrict to the case that $d$ is odd. Writing $p - 1 = 2^k l$, with $2 \nmid l$, this amounts to restricting to the case where

$$\alpha \in \{x \in (\mathbb{Z}/p)^\times : x^l = 1\} =: \zeta_l \cong \mathbb{Z}/l.$$

A function $\Phi \in \mathcal{F}'_p$ that satisfies ${}^\alpha\Phi = \Phi$, is already defined by its values on coset representatives of $(\mathbb{Z}/p)^\times / \langle -1, \alpha\rangle$. Since $\Phi$ is non-constant and $\Phi(0) = 0$, we find $|\mathrm{Fix}_{\mathcal{F}'_p}(\langle\alpha\rangle)| = p^{\frac{p-1}{2d}} - 1$.

Next, we compute the number of elements in $\mathrm{Fix}_{\mathcal{F}'_p}(\langle\alpha\rangle)$ that are fixed by a given $\beta \in (\mathbb{Z}/p)^\times$ to apply Burnside's lemma afterwards. Once again, only the case where $\beta \in \zeta_l$ is non-trivial, so we can restrict to this case. Note that the elements fixed by both $\alpha$ and $\beta$ are precisely the ones contained in the set $\mathrm{Fix}_{\mathcal{F}'_p}(\langle\alpha, \beta\rangle)$. By the previous discussion this set has size $p^{\frac{p-1}{2c}} - 1$, where $c$ is the size of the group $\langle\alpha, \beta\rangle$. For any given $c \geq 1$ such that $d|c|l$, there are precisely $\varphi(\frac{c}{d})$ different cosets $[\beta] \in \zeta_l/\langle\alpha\rangle$ such that $|\langle\alpha, \beta\rangle| = c$. Since each of these cosets has size $d$, we find $d\varphi(\frac{c}{d})$ elements $\beta \in \zeta_l$ such that $|\langle\alpha, \beta\rangle| = c$. From Burnside's lemma, we get that there are

$$\begin{aligned}
\frac{1}{p-1} \sum_{\beta \in (\mathbb{Z}/p)^\times} |\mathrm{Fix}_{\mathcal{F}'_p}(\langle\alpha, \beta\rangle)| &= \frac{1}{p-1} \sum_{\beta \in (\mathbb{Z}/p)^\times} (p^{\frac{p-1}{2|\langle\alpha,\beta\rangle|}} - 1) \\
&= \frac{1}{p-1} \sum_{\substack{c \geq 1 \\ d|c|l}} \sum_{\substack{\beta \in (\mathbb{Z}/p)^\times \\ |\langle\alpha,\beta\rangle| = c}} (p^{\frac{p-1}{2c}} - 1) \\
&= \frac{d}{p-1} \sum_{\substack{c \geq 1 \\ d|c|l}} \varphi\left(\frac{c}{d}\right) (p^{\frac{p-1}{2c}} - 1)
\end{aligned}$$

equivalence classes for parameters of the form $(\Phi, \alpha)$ with $\Phi(0) = 0$.

Considering that there are $\varphi(d)$ choices of $\alpha \in \zeta_l$ such that $\alpha$ has order $d$, we get the following number of non-isomorphic cycle sets with parameters $(\Phi, \alpha)$ with $\Phi(0) = 0$:

$$n'_p = \frac{1}{p-1} \sum_{\substack{c,d \geq 1 \\ d|c|l}} d\varphi(d)\varphi\left(\frac{c}{d}\right) (p^{\frac{p-1}{2c}} - 1) = \frac{1}{p-1} \sum_{\substack{c,d \geq 1 \\ d|c|l}} d\varphi(d)\varphi\left(\frac{c}{d}\right) (p^{2^{k-1}\frac{l}{c}} - 1).$$

Note that the function

$$\psi(c) = \sum_{\substack{d \geq 1 \\ d|c}} d\varphi(d)\varphi\left(\frac{c}{d}\right)$$

is a convolution of multiplicative functions. Here, *multiplicative* means $\mu(mn) = \mu(m)\mu(n)$ for coprime

positive integers $m, n$. So also $\psi$ is a multiplicative function which evaluates on prime powers $q^\nu$, $\nu \geq 1$, as

$$\begin{aligned}
\psi(q^\nu) &= \sum_{k=0}^{\nu} q^k \varphi(q^k)\varphi(q^{\nu-k}) \\
&= q^\nu(q-1)q^{\nu-1} + (q-1)q^{\nu-1} + \sum_{k=1}^{\nu-1}(q-1)^2 q^{\nu+k-2} \\
&= (q-1)\left(q^{2\nu-1} + q^{\nu-1} + (q-1)q^{\nu-1}\sum_{k=1}^{\nu-1} q^{k-1}\right) \\
&= (q-1)\left(q^{2\nu-1} + q^{\nu-1} + q^{\nu-1}(q^{\nu-1}-1)\right) \\
&= (q-1)\left(q^{2\nu-1} + q^{2\nu-2}\right) \\
&= (q^2-1)q^{2\nu-2}.
\end{aligned}$$

For a number with prime factorization $c = \prod_i q_i^{\nu_i}$, we therefore get

$$\psi(c) = \prod_i (q_i^2 - 1) q_i^{2\nu_i - 2}.$$

The total number of indecomposable, non-isomorphic, irretractable cycle sets of size $p^2$ can therefore be described as:

$$n_p + n'_p = p^{\frac{p-1}{2}} - 1 + \sum_{c|l} \psi(c) \frac{p^{2^{k-1}\frac{l}{c}} - 1}{p-1}$$

where $p - 1 = 2^k l$ with $2 \nmid l$.

Chapter 6

# Indecomposable involutive solutions with abelian permutation group

It is natural to study classes of involutive solutions whose permutation group satisfies a certain condition. Arguably, the easiest such property is abelianity. It was proved by Cedó, Jespers and Okniński [50] that every finite involutive solution whose permutation group is abelian has finite multipermutation level. Gateva-Ivanova and Cameron proved, among other results, that square-free indecomposable involutive solutions with an abelian permutation group are necessarily trivial [79, Theorem 7.1]. In [90], Jedlička, Pilitowska and Zamojska-Dzienio gave an explicit construction of all finite indecomposable involutive solutions with an abelian permutation group of multipermutation level at most 2. It is interesting to note that the seemingly slightly stronger condition that the structure group is abelian implies triviality for involutive solutions [78, Theorem 6.1]. This no longer holds for non-involutive solutions; in [17] Bardakov and Nasybullov give a full classification of quandles whose structure group is a free abelian group on 2 generators. Finite quandles with an abelian permutation group were studied and classified by Lebed and Mortier in [113].

In this chapter, we characterize, and up to some extent classify and enumerate, indecomposable solutions with an abelian permutation group. In Section 6.1 we reduce this classification problem to classifying braces with a transitive cycle set whose multiplicative group is abelian. In Section 6.2 describe how all finite braces with an abelian multiplicative group and a transitive cycle base can be obtained starting from matrices. We define a group action on such matrices such that two matrices yield isomorphic braces precisely when they lie in the same orbit. Subsequently, we use these results to explicitly enumerate isomorphism classes of finite indecomposable solutions with an abelian permutation group of multipermutation level 2 and 3 in Section 6.3. At last, we also discuss infinite indecomposable solutions with an abelian permutation group in Section 6.4. We are able to give a full classification of the ones of multipermutation level 2 and of those that have a torsion-free permutation group.

All results in this chapter for which no external reference is given were obtained in collaboration with Marco Castelli and are contained in the preprint [45].

## 6.1 Reducing the classification to braces

Let $\mathbf{AbBr}$ be the category with as objects braces $A$ with an abelian multiplicative group, with a distinguished transitive cycle base $X$. We denote such an object by $(A, X)$. Morphisms $(A, X) \to (B, Y)$ are brace

morphisms $f : A \to B$ such that $f(X) \subseteq Y$. Also, let $\mathbf{AbSol}$ be the category formed by indecomposable involutive solutions with an abelian permutation group and homomorphisms of solutions. Note that for an object $(A, X) \in \mathbf{AbBr}$, the automorphism of $(A, X)$ coincides with $\mathrm{Aut}(A, X)$ as defined in Section 4.4. The following is a slight variation of [137, Corollary 2].

**Proposition 6.1.1.** *There exists a bijective correspondence between isomorphism classes of* $\mathbf{AbSol}$ *and isomorphism classes in* $\mathbf{AbBr}$*. Moreover, the size and multipermutation level of objects are preserved under this correspondence.*

*Proof.* Recall that every indecomposable involutive solution with an abelian permutation group can be obtained through the construction in Proposition 1.2.24 from a brace $A$, an element $x$ contained in a transitive cycle base $X$ and $K = \{0\}$. Moreover, it follows from Proposition 1.2.25 that the obtained solution does not depend on the choice of $x \in X$ and that the solutions associated to $(A, X), (B, Y) \in \mathbf{AbBr}$ are isomorphic if and only if $(A, X)$ and $(B, Y)$ are isomorphic. This correspondence clearly preserves the size of objects. Theorem 4.1.10 and Corollary 4.1.11 ensure that also the multipermutation level is preserved. □

It is a direct consequence of Proposition 6.1.1 that the classification of indecomposable solutions with an abelian permutation group can be obtained through a classification of braces whose multiplicative group is abelian and admit a transitive cycle base. In particular, all solutions are of the form described in the following example.

**Example 6.1.2.** Let $A$ be a one-generated nilpotent ring with generator $x$. Then from Proposition 4.2.13 it follows that $(1 + A)x = x + Ax$ is a transitive cycle base of the brace $A$. Let $(A, r_x)$ denote the indecomposable solution obtained from Proposition 1.2.24 from $A$, the element $x$ and $K = \{0\}$, then $r_x$ is explicitly given by

$$r_x(a, b) = (\sigma_a(b), \sigma^{-1}_{\sigma_a(b)}(a)),$$

where

$$\sigma_a(b) = \lambda_a(x) \circ b = (ax + x) \circ b = ax + x + b + axb + xb.$$

*Remark* 6.1.3. Recall from Theorem 4.2.5 that multipermutation braces with an abelian multiplicative group that admit a transitive cycle base are necessarily one-generated as a brace. Under the correspondence between Jacobson radical rings and two-sided braces, being one-generated as a ring is generally not the same as being one-generated as a skew brace; the latter is a weaker notion since a subring of a Jacobson radical ring is a monoid but not necessarily a group for the operation $\circ$. However, for a nil two-sided brace $A$ these two notions coincide as $\overline{a} = \sum_{i=1}^{\infty}(-a)^i$ for any $a \in A$.

## 6.2 Abelian one-generated braces

Let $A$ be a one-generated multipermutation brace with an abelian multiplicative group with generator $x \in A$. As $A$ is one-generated as a ring, every element $a \in A$ is of the form $\sum_{i=1}^{n} a_i x^i$, for some $n \geq 0$ and $a_i \in \mathbb{Z}$, where $x^n$ is the $*$-product of $n$ occurrences of $x$. More generally every element $a \in A^k$ can be written as $\sum_{i=k}^{n} a_i x^n$ for some $n \geq 0$ and $a_i \in \mathbb{Z}$, or equivalently $A^k = \{x^{k-1} * a \mid a \in A\}$ for $k > 1$. As $*$-multiplication by $x$ is an endomorphism of $(A, +)$, we obtain the following result.

**Lemma 6.2.1.** *Let $A$ be a brace generated by $x \in A$ with an abelian multiplicative group. Then we have a chain of surjective group homomorphisms*

$$(A/A^2, +) \to (A^2/A^3, +) \to (A^3/A^4, +) \to \dots$$

*where for all $i \geq 1$, the map $A^k/A^{k+1} \to A^{k+1}/A^{k+2}$ is given by $a + A^{k+1} \mapsto x * a + A^{k+2}$.*

**Definition 6.2.2.** Let $A$ be a finite one-generated brace with an abelian multiplicative group. We say that $A$ is of type $(m_1, \ldots, m_n)$, for $m_1, \ldots, m_n \geq 1$, if $|A^i/A^{i+1}| = m_i$ for $1 \leq i < n$ and $A^{n+1} = \{0\}$. We define $\mathbf{AbBr}(m_1, \ldots, m_n)$ as the full subcategory of $\mathbf{AbBr}$ consisting of objects $(A, X)$ with $A$ of type $(m_1, \ldots, m_n)$.

**Definition 6.2.3.** For a finite indecomposable multipermutation solution $(X, r)$, we say that $(X, r)$ is of type $(m_1, \ldots, m_n)$, for $m_1, \ldots, m_n \geq 1$, if $|\operatorname{Ret}^{i-1}(X, r)|/|\operatorname{Ret}^i(X, r)| = m_i$ for $1 \leq i < n$ and $|\operatorname{Ret}^n(X, r)| = 1$. We define $\mathbf{AbSol}(m_1, \ldots, m_n)$ as the full subcategory consisting of objects $(X, r) \in \mathbf{AbSol}$ such that $(X, r)$ is of type $(m_1, \ldots, m_n)$.

The following result generalizes the observation by Rump that $|A^2||\operatorname{Soc}(A)| = |A|$ for a finite brace $A$ with a cyclic multiplicative group; this was remarked in the introduction of [137] and follows from equation $(15)$ and Proposition 9 of [134].

**Lemma 6.2.4.** *Let $A$ be a finite one-generated brace with an abelian multiplicative group. Then*

$$|\operatorname{Soc}_k(A)||A^{k+1}| = |A|,$$

*or equivalently $|A^k| = |\operatorname{Ret}^{k-1}(A)|$ for all $k \geq 0$.*

*Proof.* We prove by induction that for all $k \geq 1$ and $a \in A$, $x^k * a = 0$ if and only if $a \in \operatorname{Soc}_k(A)$. For $k = 1$, note that $x^k * a = 0$ if and only if $a * A = A * a = 0$, the latter is equivalent to $a \in \operatorname{Soc}(A)$. Now assume that the statement holds for $k \geq 1$. Then $x^{k+1} * a = x^k * (x * a) = 0$ if and only if $x * a \in \operatorname{Soc}_k(A)$. However, as $x + \operatorname{Soc}_k(A)$ generates $A/\operatorname{Soc}_k(A)$, the case $k = 1$ yields that the latter is equivalent to $a + \operatorname{Soc}_k(A) \in \operatorname{Soc}(A/\operatorname{Soc}_k(A))$ hence $a \in \operatorname{Soc}_{k+1}(A)$. Now notice that $x^k * a = 0$ if and only if $a$ is contained in the kernel of the surjective homomorphism $(A, +) \to (A^{k+1}, +)$ given by multiplication by $x^k$. As $A^{k+1} = \{x^k * a \mid a \in A\}$, the statement now follows. □

**Proposition 6.2.5.** *Let $m_1, \ldots, m_n \geq 1$. The bijective correspondence from Proposition 6.1.1 restricts to a bijective correspondence between isomorphism classes of $\mathbf{AbSol}(m_1, \ldots, m_n)$ and isomorphism classes of $\mathbf{AbBr}(m_1, \ldots, m_n)$.*

*Proof.* This follows directly from Corollary 4.1.9 and Lemma 6.2.4. □

**Corollary 6.2.6.** *Let $m_1, \ldots, m_n \geq 1$ and $(X, r)$ in $\mathbf{AbSol}(m_1, \ldots, m_n)$. Then*

$$|\operatorname{Aut}(X, r)| = m_1 |\operatorname{Aut}(\mathcal{G}(X, r), X')|$$

*with $X'$ the image of $X$ in $\mathcal{G}(X, r)$.*

*Proof.* From Proposition 4.4.8 and Lemma 4.4.11 we know that $\operatorname{Aut}(X, r)$ has a normal subgroup isomorphic to $\operatorname{Soc}(\mathcal{G}(X, r))$ such that the quotient is isomorphic to $\operatorname{Aut}(\mathcal{G}(X, r), X')$. As $m_1 = |A/A^2|$, which is in turn equal to $|\operatorname{Soc}(A)|$ by Lemma 6.2.4, the statement follows. □

**Example 6.2.7.** Consider the ring $\mathbb{Z}[x]/(x^{n+1})$. Let $F_n$ denote its (non-unital) subring generated by $x$. Then clearly $F_n$ is nilpotent, in particular $F_n^n \neq 0$ but $F_n^{n+1} = 0$. It follows that $F_n$ is a one-generated brace with an abelian multiplicative group. The orbit of $x$ is $(1 + F_n)x = x + F_n^2$ and is a transitive cycle base of $F_n$.

From now on, the object $(F_n, x + F_n^2) \in \mathbf{AbBr}$ will be denoted by $F_n^*$. If $I$ is an ideal of $F_n$, then the image of $x + F_n^2$ in $F_n/I$ is a transitive cycle base of $F_n/I$ and $F_n/I$ together with this cycle base will be denoted by $(F_n/I)^*$.

**Proposition 6.2.8.** *Let $A$ be a one-generator two-sided brace with multipermutation level at most $n$ and $y \in A$ a generator, there is a unique surjective brace homomorphism $f : F_n \to A$ mapping $x$ to $y$.*

*Proof.* Let $F$ denote the (non-unital) subring of $\mathbb{Z}[x]$ generated by $x$. Then there exists a unique ring homomorphism $f' : F \to A$ where $x \mapsto y$. Since $\mathrm{mpl}(A) \leq n$, we find that that $y^{n+1} = 0$ and thus $f'$ yields a ring homomorphism $f : F_n \to A$. Since $f$ is also a brace homomorphism and $y$ generates $A$, $f$ is surjective. As $F_n$ is generated (as a brace) by $x$, the uniqueness of $f$ is guaranteed. □

**Corollary 6.2.9.** *Let $(A, Y) \in \mathbf{AbBr}$ with $A$ of multipermutation level at most $n$. Then there exists a surjective homomorphism $f : F_n^* \to (A, Y)$. In particular, $(A, Y)$ is isomorphic to $(F_n/\ker f)^*$.*

**Corollary 6.2.10.** *Let $(X, r) \in \mathbf{AbSol}$ with $\mathrm{mpl}(X, r) = n$. Then both the additive and multiplicative groups of $\mathcal{G}(X, r)$ are generated by at most $n$ elements.*

*Proof.* Clearly $(F_n, +)$ is free abelian of rank $n$. As $(F_n^k/F_n^{k+1}, \circ) \cong \mathbb{Z}$ for all $1 \leq k \leq n$ and $(F_n, \circ)$ is abelian, we find that also $(F_n, \circ)$ is free abelian of rank $n$. The first part of the result then follows from Corollary 6.2.9. □

*Remark* 6.2.11. For $n = 2$ the first part of the previous corollary was proved in [90].

Since a finite brace $A$ with an abelian multiplicative group is, in particular, two-sided, it is strongly nilpotent and therefore it has a (uniquely determined) type. By Proposition 1.1.25 we find that $A$ is a direct product of braces of prime power size. We therefore will restrict to braces, and thus also solutions, of prime power size. From Lemma 6.2.1 it follows that if $|A| = p^d$ for some prime $p$, then $A$ is of type $(p^{d_1}, \ldots, p^{d_n})$ for some $d_1 \geq d_2 \geq \ldots \geq d_n \geq 0$ such that $d = d_1 + \ldots + d_n$. In the remainder of this section, we fix the notation that $n \geq 1$, $p$ is a prime, $d_1, \ldots, d_n$ are integers such that $d_1 \geq \ldots \geq d_n \geq 0$ and $d = \sum_{i=1}^{n} d_i$.

From Corollary 6.2.9 it follows that any object in $\mathbf{AbBr}(p^{d_1}, \ldots, p^{d_n})$ is isomorphic to $(F_n/I)^*$ for some ideal $I$. This now yields two natural questions: (1) Can we determine all ideals $I$ of $F_n$ such that $(F_n/I)^* \in \mathbf{AbBr}(p^{d_1}, \ldots, p^{d_n})$? (2) Can we determine when two such ideals give an isomorphic quotient? We start by providing an answer to the first question.

We define group endomorphisms $s^+, s^- : \mathbb{Z}^n \to \mathbb{Z}^n$ by $s^+(v_1, \ldots, v_n) = (0, v_1, \ldots, v_{n-1})$ and $s^-(v_1, \ldots, v_n) = (v_2, \ldots, v_n, 0)$.

**Definition 6.2.12.** Let $\mathcal{M}(p^{d_1}, \ldots, p^{d_n})$ be the set of all $n \times n$-matrices $M$ such that

1. $M$ is upper triangular.
2. $M$ contains only positive integer elements.
3. Every diagonal element of $M$ is strictly greater than every other element in the same column.
4. For every $k$ such that $1 \leq k < n$, the image of the $k$-th row of $M$ under $s^+$ is contained in the subgroup of $\mathbb{Z}^n$ generated by $(k+1)$-th until $n$-th row.
5. The diagonal of $M$ is $(p^{d_1}, \ldots, p^{d_n})$.

**Proposition 6.2.13.** *There exists a bijective correspondence between matrices in $\mathcal{M}(p^{d_1}, \ldots, p^{d_n})$ and ideals of $I$ in $F_n$ such that $F_n/I$ is of type $(p^{d_1}, \ldots, p^{d_n})$.*

*Proof.* Let $\mathcal{M}'$ be the class of $n \times n$-matrices satisfying the first three conditions of Definition 6.2.12 and such that their diagonal contains only non-zero elements. It is easily seen that every integer $n \times n$-matrix of rank $n$ is row equivalent to a unique matrix in $\mathcal{M}'$. It follows from basic techniques from linear algebra that there exists a bijective correspondence between matrices in $\mathcal{M}'$ and subgroups $I$ of $\mathbb{Z}^n$ of finite index, where to a matrix $M = (m_{i,j}) \in \mathcal{M}'$ we associate the subgroup $I_M$ of $\mathbb{Z}^n$ generated by the rows of $M$. As the elements $x, x^2, \ldots, x^n$ form a basis of $(F_n, +)$, we obtain a correspondence between matrices in $\mathcal{M}'$ and finite subgroups of $(F_n, +)$.

We claim that $I_M$ is an ideal if and only if $M$ satisfies condition 4. Let $f_1, \ldots, f_n \in F_n$ be the generators of $I_M$ associated to the rows of $M$. In order for $I_M$ to be an ideal, we need that $x * f_k \in I_M$ for all $1 \leq k \leq n$. As the first $k$ coordinates of $f_k$ are 0, we find that the latter happens precisely if $x * f_k \in \langle f_{k+1}, \ldots, f_n \rangle_+$. Because $*$-multiplying $f_k$ by $x$ is the same as shifting its coordinates to the right, this proves the claim.

At last we prove that the lower series of $F_n/I$ is of type $(p^{d_1}, \ldots, p^{d_n})$ if and only if $M$ satisfies condition 5. For this, it suffices to note that $F_n^i$ consists of all elements which are 0 on the first $i-1$ coordinates, hence the additive group of $(F_n/I)^i/(F_n/I)^{i+1}$ is isomorphic to $\mathbb{Z}/m_{i,i}$, from which the last part of the statement follows. □

**Theorem 6.2.14.** *Let $M \in \mathcal{M}(p^{d_1}, \ldots, p^{d_n})$ and let $A = F_n/I_M$. Then $(A, r_{x+I_M})$ is a solution in $\mathbf{AbSol}(p^{d_1}, \ldots, p^{d_n})$ and every solution in $\mathbf{AbSol}(p^{d_1}, \ldots, p^{d_n})$ is isomorphic to such a solution.*

*Proof.* This follows from Corollary 6.2.9 and Proposition 6.2.13. □

*Remark* 6.2.15. If, within the setting of Theorem 6.2.14, we identify an element $a_1x^1 + \ldots + a_nx^n$, then we find for $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n) \in F_n$ that the $\sigma$-map of the solution $(A, r_{x+I_M})$ in Theorem 6.2.14 is given by $\sigma_{a+I_M}(b + I_M) = (c_1(a, b), \ldots, c_n(a, b)) + I_M$ with $c_1(a, b) = b_1 + 1$ and

$$c_i(a, b) = a_{i-1} + b_{i-1} + b_i + \sum_{1 \leq k < i-1} a_k b_{i-k}.$$

**Proposition 6.2.16.** *The set $\mathcal{M}(p^{d_1}, \ldots, p^{d_n})$ has size $p^{d-d_1}$.*

*Proof.* We will prove this by induction on $n$. If $n = 1$, the statement is clear. Now let $n \geq 2$. Let $M' \in \mathcal{M}(p^{d_2}, \ldots, p^{d_n})$. We will count the number of matrices $M \in \mathcal{M}(p^{d_1}, \ldots, p^{d_n})$ such that if we remove the first row and column of $M$, we obtain $M'$.

Let $f_i \in \mathbb{Z}^n$ be the $i$-th row of such $M$. Then $f_2, \ldots, f_n$ are completely determined by $M'$, so we need to compute the number of choices of $f_1$. Let us consider what the conditions in Definition 6.2.12 imply on $f_1$: condition 1 does not impose restrictions on $f_1$, condition 4 means that $s^+(f_1) \in \langle f_2, \ldots, f_n \rangle_+$ and condition 5 means that the first coordinate of $f_1$ is $p^{d_1}$. Conditions 2 and 3 mean that we can determine $f_1$ up to equivalence in $\mathbb{Z}^n/\langle f_2, \ldots, f_n \rangle_+$, as the conditions then ensure a unique choice of representative. Note that considering $f_1$ up to this equivalence does not conflict in any way with the restrictions imposed by 4 and 5.

Clearly

$$H = \langle s^-(f_3), \ldots, s^-(f_n), (0, \ldots, 0, 1) \rangle_+,$$

is the largest subgroup of $\mathbb{Z}^n$ such that $s^+(H) \subseteq \langle f_3, \ldots, f_n \rangle_+$ so in particular $\langle f_2, \ldots, f_n \rangle_+ \subseteq H$. Then the condition $s^+(f_1) \in \langle f_2, \ldots, f_n \rangle_+$ is equivalent to $f_1 \in p^{d_1-d_2}s^-(f_2) + H$. So the number of choices of $f_1$ is precisely the number of elements in the coset $p^{d_1-d_2}s^-(f_2) + H$ modulo $\langle f_2, \ldots, f_n \rangle_+$, but this is precisely the index $|H : \langle f_2, \ldots, f_n \rangle_+|$, which we can calculate as

$$\frac{|s^+(\mathbb{Z}^n) : \langle f_2, \ldots, f_n \rangle_+|}{|s^+(\mathbb{Z}^n) : H|} = \frac{p^{d-d_1}}{p^{d-d_1-d_2}} = p^{d_2}.$$

We conclude that $|\mathcal{M}(p^{d_1},\dots,p^{d_n})| = p^{d_2}|\mathcal{M}(p^{d_2},\dots,p^{d_n})|$ which by the induction hypothesis is $p^{d-d_1}$. □

**Corollary 6.2.17.** $\mathbf{AbSol}(p^{d_1},\dots,p^{d_n})$ *contains at most* $p^{d-d_1}$ *isomorphism classes.*

*Proof.* This follows directly from Theorem 6.2.14 and Proposition 6.2.16. □

Now that we know how to describe and count the ideals of finite index of $F_n$, we focus on the second question that arose earlier. We will describe the isomorphism classes of quotients of $F_n$ through orbits of a certain group action. We first treat general quotients and then restrict to a more specific case as above.

**Lemma 6.2.18.** *For every* $y \in x + F_n^2$*, there exists a unique automorphism of* $F_n^*$ *mapping* $x$ *to* $y$*.*

*Proof.* Let $y \in x+F_n^2$. It is clear that $y^n = 0$, hence there exists a unique ring endomorphism $\phi_y$ of $F_n$ such that $\phi_y(x) = y$. By Proposition 4.2.13, $y$ generates $F_n$ as a brace, hence $\phi_y$ is surjective. Because $(F_n,+)$ is free of finite rank, it follows that $\phi_y$ is an automorphism of $F_n$, which by construction is an automorphism of $F_n^*$ as well. □

**Corollary 6.2.19.** *Let* $I$ *and* $J$ *be ideals of* $F_n$ *and* $\phi : (F_n/I)^* \to (F_n/J)^*$ *an isomorphism. Then there exists an automorphism* $\hat{\phi} : F_n^* \to F_n^*$ *such that* $\hat{\phi}(I) = J$ *and* $\hat{\phi}$ *is a lifting of* $\phi$ *in the sense that the following diagram commutes.*

$$\begin{array}{ccc} F_n & \xrightarrow{\hat{\phi}} & F_n \\ \downarrow & & \downarrow \\ F_n/I & \xrightarrow{\phi} & F_n/J \end{array}$$

*Proof.* Let $y \in \phi(x + I)$ for some $y \in x + F_n^2$. In particular, this implies that for any $a_i \in \mathbb{Z}$ we find that $\sum_{i=1}^n a_i x^i \in I$ if and only if $\sum_{i=1}^n a_i y^i \in J$. Now define $\hat{\phi} : F_n \to F_n$ as the automorphism mapping $x$ to $y$, which exists by the previous lemma. Then in particular, $\hat{\phi}(I) \subseteq I = J$, and thus $\hat{\phi}$ fits in the above diagram. □

Consider the action of $\mathrm{Aut}(F_n^*)$ on ideals of $F_n$ where $\phi \in \mathrm{Aut}(F_n^*)$ maps an ideal $I$ to $\phi(I)$. We then obtain the following result.

**Proposition 6.2.20.** *There is a bijective correspondence between isomorphism classes of quotients of* $F_n^*$ *and orbits of ideals of* $F_n$ *under the action by* $\mathrm{Aut}(F_n^*)$*. Under this correspondence, the orbit of an ideal* $I$ *is mapped to the isomorphism class of* $(F_n/I)^*$*.*

*Proof.* Let $I, J$ be ideals of $F_n$. Assume that there exists an isomorphism $\theta : (F_n/I)^* \to (F_n/J)^*$. Then using Corollary 6.2.19 we find that $\phi$ lifts to an automorphism $\hat{\phi}$ of $F_n^*$ such that $\hat{\phi}(I) = J$. Conversely, any automorphism of $F_n^*$ mapping $I$ to $J$ induces an isomorphism between $F_n/I$ and $F_n/J$. □

For counting purposes, it is more convenient to consider a slight variation of this action such that we have a finite group acting on a finite set. We do so by restricting to ideals $I$ of $F_n$ such that $F_n/I$ is of type $(p^{d_1},\dots,p^{d_n})$. Let $(p^d x)$ be the ideal of $F_n$ generated by $p^d x$ and let $F_{n,p^d} = F_n/(p^d F_n)$. Ideals of $F_n$ of index $p^d$ always contain $p^d F_n$, so they are in correspondence with ideals of $F_{n,p^d}$ of index $p^d$. By abuse of notation, we will also denote the image of $x$ in $F_{n,p^d}$ by $x$, and $F_{n,p^d}^*$ is short for the object in $\mathbf{AbBr}$ consisting of $F_{n,p^d}$ and the transitive cycle base containing $x$. It is clear that every $(A,X) \in \mathbf{AbBr}$ with $|A| = p^d$ is isomorphic to $(F_{n,p^d}/I)^*$ for some ideal $I$. As every automorphism of $F_n$ maps $p^d F_n$ to itself, we immediately obtain the following variations of Lemma 6.2.18 and Corollary 6.2.19.

**Lemma 6.2.21.** *For every $y \in x + F_{n,p^d}^2$, there exists a unique automorphism of $F_{n,p^d}^*$ mapping $x$ to $y$.*

**Corollary 6.2.22.** *Let $I$ and $J$ be ideals of $F_{n,p^d}$ and $\phi : (F_{n,p^d}/I)^* \to (F_{n,p^d}/J)^*$ an isomorphism. Then there exists an automorphism $\hat{\phi} : F_{n,p^d}^* \to F_{n,p^d}^*$ such that $\hat{\phi}(I) = J$ and $\hat{\phi}$ is a lifting of $\phi$ in the sense that the following diagram commutes.*

$$\begin{array}{ccc} F_{n,p^d} & \xrightarrow{\hat{\phi}} & F_{n,p^d} \\ \downarrow & & \downarrow \\ F_{n,p^d}/I & \xrightarrow{\phi} & F_{n,p^d}/J \end{array}$$

Consider the action of $\mathrm{Aut}(F_{n,p^d}^*)$ on ideals of $F_{n,p^d}$ where $\phi \in \mathrm{Aut}(F_{n,p^d}^*)$ maps an ideal $I$ to $\phi(I)$. We then obtain the following variation of Proposition 6.2.20.

**Theorem 6.2.23.** *Isomorphism classes of $\mathbf{AbBr}(p^{d_1}, \ldots, p^{d_n})$ are in bijective correspondence with orbits of ideals $I$ of $F_{n,p^d}$ such that $F_{n,p^d}$ is of type $(p^{d_1}, \ldots, p^{d_n})$ under the action of $\mathrm{Aut}(F_{n,p^d}^*)$. Under this correspondence, the orbit of an ideal $I$ is mapped to the isomorphism class of $(F_{n,p^d}/I)^*$.*

Using the bijective correspondence from Proposition 6.2.13, we obtain an action $\cdot$ of $\mathrm{Aut}(F_{n,p^d}^*)$ on $\mathcal{M}(p^{d_1}, \ldots, p^{d_n})$, where $\phi \cdot M$ is the unique matrix in $\mathcal{M}(p^{d_1}, \ldots, p^{d_n})$ equivalent to $\phi(I_M)$. The orbit of some $M \in \mathcal{M}(p^{d_1}, \ldots, p^{d_n})$ under this action is denoted by $\mathcal{O}(M)$. We denote the number of isomorphism classes in $\mathbf{AbSol}(p^{d_1}, \ldots, p^{d_n})$ by $|\mathbf{AbSol}(p^{d_1}, \ldots, p^{d_n})|$. From Proposition 6.1.1 and Theorem 6.2.23, we obtain the main result of this section.

**Theorem 6.2.24.** *Isomorphism classes in $\mathbf{AbSol}(p^{d_1}, \ldots, p^{d_n})$ are in bijective correspondence with orbits of the action of $\mathrm{Aut}(F_{n,p^d}^*)$ on $\mathcal{M}(p^{d_1}, \ldots, p^{d_n})$. In particular,*

$$|\mathbf{AbSol}(p^{d_1}, \ldots, p^{d_n})| = \sum_{M \in \mathcal{M}(p^{d_1}, \ldots, p^{d_n})} \frac{1}{|\mathcal{O}(M)|},$$

## 6.3 Explicit calculations

In what follows, we will explicitly apply the results of Section 6.2 to the cases $n = 2$ and $n = 3$. We first cover the case where $n = 2$, which was already done in [90] using different techniques, and we subsequently also give an explicit formula for $|\mathbf{AbSol}(p^{d_1}, p^{d_2}, p^{d_3})|$. For $n > 3$, the applied techniques do not seem to generalize; however, it would be interesting to see up to which multipermutation level $n$ and size $p^d$ one could enumerate the number of isomorphism classes of solutions with the help of a computer.

### 6.3.1 Multipermutation level 2

Let $M \in \mathcal{M}(p^{d_1}, p^{d_2})$. So $M$ is of the form

$$M = \begin{pmatrix} p^{d_1} & m \\ 0 & p^{d_2} \end{pmatrix},$$

where $m$ can be freely chosen such that $0 \leq m < p^{d_2}$. Recall that the automorphisms of $F_{2,p^d}^*$ are in bijection with elements in the coset $x + F_{2,p^d}$; to every element $y$ in this coset we associate the unique automorphism $\phi_y$ which maps $x$ to $y$. For any $a, b \in \mathbb{Z}/p^d$ we find

$$\phi_{x+ax^2}(\phi_{x+bx^2}(x)) = \phi_{x+ax^2}(x + bx^2) = x + ax^2 + b(x + ax^2)^2 = x + (a + b)x^2 = \phi_{x+(a+b)x^2}(x).$$

Hence $\mathrm{Aut}(F^*_{2,p^2}) \cong \mathbb{Z}/p^d$. If we let $\phi_{x+ax^2}$ act on $M$, we find that the result $\phi_{x+ax^2} \cdot M$ is the unique matrix in $\mathcal{M}(p^{d_1}, p^{d_2})$ which is row-equivalent to

$$M = \begin{pmatrix} p^{d_1} & m + ap^{d_1} \\ 0 & p^{d_2}, \end{pmatrix}.$$

As $d_1 \geq d_2$, we thus find that $\phi_{x+ax^2} \cdot M = M$ and therefore the action is trivial.

**Theorem 6.3.1.** *Let $p$ be a prime, $d_1 \geq d_2 \geq 0$, and $A = \mathbb{Z}/p^{d_1} \times \mathbb{Z}/p^{d_2}$. Then for any $0 \leq m < p^{d_2}$, the map*

$$r\begin{pmatrix}(a_1, a_2)\\(b_1, b_2)\end{pmatrix} = \begin{pmatrix}(b_1 + 1, a_1 + b_1 + b_2 - \chi_0(b_1 + 1)m)\\(a_1 - 1, a_2 - a_1 - b_1 + \chi_0(a_1)m)\end{pmatrix}$$

*yields a solution $(A, r) \in \mathbf{AbSol}(p^{d_1}, p^{d_2})$. Here, $\chi_0 : \mathbb{Z}/p^{d_1} \to \mathbb{Z}/p^{d_2}$ is defined as*

$$\chi_0(x) = \begin{cases} 1 & x = 0 \\ 0 & x \neq 0 \end{cases}.$$

*Moreover, every solution in $\mathbf{AbSol}(p^{d_1}, p^{d_2})$ is isomorphic to such a solution for a unique choice of $m$.*

*Proof.* The first part of the statement is a consequence of Theorem 6.2.14 and Remark 6.2.15, where the ideal $I_M$ of $F_2$ is generated by $\{p^{d_1}x + mx^2, p^{d_2}x^2\}$. Indeed, it follows directly that

$$\sigma_{(a_1,a_2)}(b_1, b_2) = (b_1 + 1, a_1 + b_1 + b_2 - \chi_0(b_1 + 1)m),$$

and using (1.6) we also find

$$\begin{aligned}\tau_{(b_1,b_2)}(a_1, a_2) &= \sigma^{-1}_{\sigma_{(a_1,a_2)}(b_1,b_2)}(a_1, a_2)\\ &= \sigma^{-1}_{(b_1+1,a_1+b_1+b_2-\chi_0(b_1+1)m)}(a_1, a_2)\\ &= (a_1 - 1, a_2 - a_1 - b_1 + \chi_0(a_1)m).\end{aligned}$$

The second part of the statement follows from Theorem 6.2.24, combined with the observation that the considered action on $\mathcal{M}(p^{d_1}, p^{d_2})$ is trivial. □

**Corollary 6.3.2.** *Let $p$ be a prime, $d \geq 0$. The total number of solutions of size $p^d$ and multipermutation level at most 2 in $\mathbf{AbSol}$ is given by*

$$(p^{\lfloor d/2 \rfloor + 1} - 1)/(p - 1),$$

*where $\lfloor d/2 \rfloor$ is the largest integer $n$ such that $n \leq d/2$.*

*Proof.* We find

$$\sum_{\substack{d_1+d_2=d\\ d_1 \geq d_2 \geq 0}} |\mathbf{AbSol}(p^{d_1}, p^{d_2})| = \sum_{\substack{d_1+d_2=d\\ d_1 \geq d_2 \geq 0}} p^{d_2} = \sum_{d_2=0}^{\lfloor d/2 \rfloor} p^{d_2} = (p^{\lfloor d/2 \rfloor + 1} - 1)/(p - 1),$$

from which the statement follows. □

*Remark* 6.3.3. The classification given in Theorem 6.3.1 was also obtained by Jedlička, Pilitowska and Zamojska-Dzienio in [90], albeit in another form. It is interesting to note that the techniques used in the classification in [90] differ strongly from ours. One benefit of our techniques is that the general theoretical framework earlier in the section does not in any way pose strict assumptions on the permutation level; the downside is that it is not immediately clear what the multiplicative and additive group of the permutation brace look like precisely. The techniques used in [90] rely strongly on the assumption that the multipermutation level is 2 and do not seem to generalize to higher multipermutation levels; however, through their classification, it is immediately clear what the permutation group of a solution looks like.

### 6.3.2 Multipermutation level 3

Now let us compute the number of solutions in $\mathbf{AbSol}$ of a given size and multipermutation level at most 3. To do so, we first compute $|\mathbf{AbSol}(p^{d_1}, p^{d_2}, p^{d_3})|$. We may assume that $d_3 > 0$, as otherwise the value can be obtained from the case $n = 2$. It will be convenient to consider the matrices in $\mathcal{M}(p^{d_1}, p^{d_2}, p^{d_3})$ up to row-equivalence (which we will denote by $\sim$). This is no problem as no two matrices in $\mathcal{M}(p^{d_1}, p^{d_2}, p^{d_3})$ are row-equivalent and the ideal $I_M$ can easily be constructed from any matrix which is row-equivalent to $M$, hence the action on $\mathcal{M}(p^{d_1}, p^{d_2}, p^{d_3})$ is still straightforward to compute. From the defining conditions of $\mathcal{M}(p^{d_1}, p^{d_2}, p^{d_3})$ we find that all $M \in \mathcal{M}(p^{d_1}, p^{d_2}, p^{d_3})$ are of the form

$$\begin{pmatrix} p^{d_1} & p^{d_1-d_2}m_2 + \alpha p^{d_3} & m_1 \\ 0 & p^{d_2} & m_2 \\ 0 & 0 & p^{d_3} \end{pmatrix},$$

for $0 \leq m_1, m_2 < p^{d_3}$ and $0 \leq \alpha < p^{d_2-d_3}$.

Once again, for $y \in x + F_{3,p^d}^2$ we denote the unique automorphism of $F_{3,p^d}^*$ mapping $x$ to $y$ by $\phi_y$. We need to determine all $y \in x + F_{3,p^d}^2$ such that $\phi_y$ acts trivially on $M$. Let $y = x + ax^2 + bx^3$. So $y^2 = x^2 + 2ax^3$ and $y^3 = x^3$ in $F_{3,p^d}$. We then know that

$$\begin{aligned} \phi_y \cdot M &\sim \begin{pmatrix} p^{d_1} & p^{d_1-d_2}m_2 + \alpha p^{d_3} + ap^{d_1} & m_1 + bp^{d_1} + 2a(p^{d_1-d_2}m_2 + \alpha p^{d_3}) \\ 0 & p^{d_2} & m_2 + p^{d_2} \\ 0 & 0 & p^{d_3} \end{pmatrix} \\ &\sim \begin{pmatrix} p^{d_1} & p^{d_1-d_2}m_2 + \alpha p^{d_3} & m_1 + ap^{d_1-d_2}m_2 \\ 0 & p^{d_2} & m_2 \\ 0 & 0 & p^{d_3} \end{pmatrix}. \end{aligned}$$

From which we find that $\phi_y \cdot M \sim M$ if and only if

$$ap^{d_1-d_2}m_2 \equiv 0 \pmod{p^{d_3}} \tag{6.1}$$

If we let $r(M) \geq 0$ be the smallest value such that (6.1) holds for $a = p^{r(M)}$, then we find that

$$\mathrm{Stab}_{\mathrm{Aut}(F_{3,p^d}^*)}(M) = \{\phi_{x+ax^2+bx^3} \mid a \in p^{r(M)}\mathbb{Z}/p^d, b \in \mathbb{Z}/p^d\},$$

so in particular $|\mathrm{Stab}_{\mathrm{Aut}(F_{3,p^d}^*)}(M)| = p^{2d-r(M)}$ and thus $|\mathcal{O}(M)| = p^{r(M)}$.

Let $\nu_p : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ denote the $p$-valuation, then $r(M) = \max\{0, -d_1 + d_2 + d_3 - \nu(m_2)\}$. Theorem 6.2.24 now yields

$$\begin{aligned}
|\mathbf{AbSol}(p^{d_1}, p^{d_2}, p^{d_3})| &= \sum_{M \in \mathcal{M}(p^{d_1}, p^{d_2}, p^{d_3})} p^{-r(M)} \\
&= \sum_{\substack{0 \le m_1, m_2 < p^{d_3} \\ 0 \le \alpha < p^{d_2 - d_3}}} p^{-\max\{0, -d_1 + d_2 + d_3 - \nu(m_2)\}} \\
&= p^{d_2} \sum_{m_2 = 0}^{p^{d_3} - 1} p^{-\max\{0, -d_1 + d_2 + d_3 - \nu(m_2)\}}
\end{aligned}$$

For a given $v$, with $0 \le v < d_3$, there are precisely $p^{d_3 - v} - p^{d_3 - v - 1}$ integers $k$, with $1 \le k < p^{d_3}$, such that $\nu_p(k) = v$. We therefore find that

$$\begin{aligned}
|\mathbf{AbSol}(p^{d_1}, p^{d_2}, p^{d_3})| &= p^{d_2} \left( 1 + \sum_{v=0}^{d_3 - 1} \frac{p^{d_3 - v} - p^{d_3 - v - 1}}{p^{\max\{0, -d_1 + d_2 + d_3 - v\}}} \right) \\
&= p^{d_2} \left( 1 + \sum_{w=0}^{d_3 - 1} \frac{p^{w+1} - p^w}{p^{\max\{0, -d_1 + d_2 + w + 1\}}} \right).
\end{aligned}$$

If $d_1 = d_2$ then

$$\begin{aligned}
|\mathbf{AbSol}(p^{d_1}, p^{d_2}, p^{d_3})| &= p^{d_2} \left( 1 + \sum_{w=0}^{d_3 - 1} \frac{p^{w+1} - p^w}{p^{w+1}} \right) \\
&= p^{d_2} (1 + d_3 (1 - p^{-1})).
\end{aligned}$$

If $d_1 > d_2$ and $d_1 < d_2 + d_3$ then

$$\begin{aligned}
|\mathbf{AbSol}(p^{d_1}, p^{d_2}, p^{d_3})| &= p^{d_2} \left( 1 + \sum_{w=0}^{d_1 - d_2 - 1} (p^{w+1} - p^w) + \sum_{w=d_1 - d_2}^{d_3 - 1} \frac{p^{w+1} - p^w}{p^{-d_1 + d_2 + w + 1}} \right) \\
&= p^{d_2} \left( 1 + p^{d_1 - d_2} - 1 + p^{d_1 - d_2} \sum_{w=d_1 - d_2}^{d_3 - 1} (1 - p^{-1}) \right) \\
&= p^{d_1} (1 + (-d_1 + d_2 + d_3)(1 - p^{-1})).
\end{aligned}$$

If $d_1 > d_2$ and $d_1 \ge d_2 + d_3$ then

$$\begin{aligned}
|\mathbf{AbSol}(p^{d_1}, p^{d_2}, p^{d_3})| &= p^{d_2} \left( 1 + \sum_{w=0}^{d_3 - 1} p^{w+1} - p^w \right) \\
&= p^{d_2} \left( 1 + p^{d_3} - 1 \right) \\
&= p^{d_2 + d_3}
\end{aligned}$$

We obtain the following result, whose proof is given above for $d_3 > 0$ and follows from Theorem 6.3.1 for $d_3 = 0$.

**Theorem 6.3.4.** *Let $p$ be a prime and $d_1 \geq d_2 \geq d_3 \geq 0$. Then*

$$|\mathbf{AbSol}(p^{d_1}, p^{d_2}, p^{d_3})| = \begin{cases} p^{d_1}(1 + (-d_1 + d_2 + d_3)(1 - p^{-1})) & d_1 < d_2 + d_3 \\ p^{d_2+d_3} & d_1 \geq d_2 + d_3 \end{cases}.$$

*In particular, the number of isomorphism classes of solutions of size $p^d$ and multipermutation level at most 3 in* $\mathbf{AbSol}$ *can be computed as*

$$\sum_{\substack{d_1 \geq d_2 \geq d_3 \geq 0 \\ d_1+d_2+d_3=d}} |\mathbf{AbSol}(p^{d_1}, p^{d_2}, p^{d_3})|.$$

## 6.4 Infinite indecomposable involutive solutions with an abelian permutation group

In [90, Theorem 6.1] for each $m = 0$ or $m \geq 2$ an indecomposable involutive solutions of multipermutation level 2 and permutation group $\mathbb{Z} \times \mathbb{Z}/m$ was given. In this section, we will show that they are the only ones. Furthermore, we classify indecomposable involutive multipermutation solutions with a torsion-free abelian permutation group.

**Proposition 6.4.1.** *Let $A$ be an infinite one-generated brace with an abelian multiplicative group and multipermutation level 2, and let $X$ be a transitive cycle base of $A$. Then $(A, X)$ is isomorphic to $(F_2/I_m)^*$ for some $m$ with either $m = 0$ or $m \geq 2$, where $I_m = \mathbb{Z}mx^2$. Moreover, the multiplicative group of $F_2/I_m$ is isomorphic to $\mathbb{Z} \times (\mathbb{Z}/m)$.*

*Proof.* By Corollary 6.2.9 we know that $(A, X)$ is isomorphic to $(F_2/I)^*$ for some ideal $I$. It is possible that $I = \{0\}$, in which case $I = I_0$. Now assume that $I \neq \{0\}$. We know that $(I, +)$ should be cyclic because otherwise $(F_2/I, +)$ is finite. Let $lx + mx^2$, with $l, m \in \mathbb{Z}$ and $m \geq 0$, be a generator of $(I, +)$. Then $x * (lx + mx^2) = lx^2 \in I$ is an additive multiple of $lx + mx^2$, hence $l = 0$. We find that $I = I_m$ for some $m$ with either $m = 0$ or $m \geq 2$, since $m = 1$ would mean that $\mathrm{mpl}(F_n/I) = 1$. Because $F_2 * F_2^2 = F_2^2 * F_2 = 0$, we find that $I_m$ is an ideal for every choice of $m$. As $(F_2/I_m, +) \cong \mathbb{Z} \times (\mathbb{Z}/m)$, it is clear that different choices of $m$ yield non-isomorphic braces $F_2/I_m$.

It remains to show that $(F_2/I_m, \circ) \cong \mathbb{Z} \times (\mathbb{Z}/m)$. To see this, it suffices to note that

$$((F_2/I_m)/(F_2/I_m)^2, \circ) \cong \mathbb{Z},$$

and $((F_2/I_m)^2, \circ) \cong \mathbb{Z}/m$. □

**Theorem 6.4.2.** *Let $m = 0$ or $m \geq 2$ then $\mathbb{Z} \times \mathbb{Z}/m$ with*

$$r\begin{pmatrix}(a_1, a_2)\\(b_1, b_2)\end{pmatrix} = \begin{pmatrix}(b_1 + 1, a_1 + b_1 + b_2)\\(a_1 - 1, a_2 - a_1 - b_1)\end{pmatrix}$$

*is an infinite indecomposable involutive solution whose permutation group is isomorphic to $\mathbb{Z} \times \mathbb{Z}/m$ and multipermutation level 2. Moreover, every infinite indecomposable solution with an abelian permutation group and multipermutation level 2 is isomorphic to such a solution.*

*Proof.* Let $m = 0$ or $m \geq 2$. An easy computation shows that the solution associated with $(F_n/I_m)^*$ is precisely the solution in the statement, and it satisfies the required properties. Conversely, if $(X, r)$ is an indecomposable solution with an abelian permutation group and multipermutation level 2, then its permutation brace must satisfy the conditions of Proposition 6.4.1, hence the statement follows from Proposition 6.1.1. □

**Proposition 6.4.3.** *Let $A$ be a brace of multipermutation level $n$, with a transitive cycle base $X$ and with an abelian torsion-free multiplicative group. Then $(A, X)$ is isomorphic to $F_n^*$.*

*Proof.* From Corollary 6.2.9 we know that $A \cong F_n/I$ for some ideal $I$. Assume that $I \neq 0$. As $\mathrm{Soc}(F_n) = F_n^n$, it follows that $I \cap F_n^n \neq 0$ by [55, Theorem 2.8]. If $I \cap F_n^n \neq F_n^n$, we find that $x^n$ has a finite order in $(F_n, \circ)$. This implies that $I \cap F_n^n = F_n^n$, but then $F_n/I$ has a multipermutation level strictly less than $n$. We conclude that $I = \{0\}$. □

**Theorem 6.4.4.** *Let $n > 1$. Then the solution $(F_n, r_x)$ (as in Example 6.1.2) is the unique indecomposable involutive solution with abelian torsion-free permutation group and multipermutation level $n$.*

*Proof.* This is a direct consequence of Proposition 6.1.1 and Proposition 6.4.3. □

*Remark* 6.4.5. The solutions in Theorem 6.4.4 can be expressed explicitly in terms of the additive group $\mathbb{Z}^n$ of $F_n$, just as the ones discussed in Remark 6.2.15.

Chapter 7

# Skew braces and Hopf–Galois structures

As discussed in Section 1.5.3, a main role in the development of Hopf–Galois theory was played by a groundbreaking result of Greither and Pareigis [82]. This result was followed by new approaches to the theory, and problems of existence and classification have been studied by several authors; given a group $N$, does there exist a Hopf–Galois structure of type $N$ on $L/K$? Can we classify and count the Hopf–Galois structures on $L/K$? A precise survey of the main results developed in the last years can be found in [63].

A problem that can be approached with Greither–Pareigis theory regards the surjectivity of the Hopf–Galois correspondence. For example, if we consider the classical structure, then we recover the usual Galois correspondence, which is surjective. But it was proved in [82] that if we consider the canonical non-classical structure, then the image of the Hopf–Galois correspondence consists precisely of the normal intermediate fields of $L/K$; this shows that if $G$ is Hamiltonian (that is, non-abelian with all the subgroups normal), then the Hopf–Galois correspondence is surjective, but as soon as the group is not abelian nor Hamiltonian, we find a Hopf–Galois structure for which the Hopf–Galois correspondence is not surjective.

More generally, given a Hopf–Galois structure on $L/K$ with Hopf algebra $H$ corresponding to a regular subgroup $N$ of $\mathbb{S}_G$ normalized by $\mathcal{L}(G)$, we know that there exists a bijective correspondence between $K$-Hopf subalgebras of $H$ and subgroups of $N$ normalized by $\mathcal{L}(G)$; the first explicit proof of this fact can be found in [67, Proposition 2.2]. Recall that we use $\mathcal{L} : G \to \mathbb{S}_G$ to denote the left regular action. As there always exists a bijective correspondence between intermediate fields of $L/K$ and subgroups of the Galois group $G$, we can translate the Hopf–Galois correspondence to find a correspondence between subgroups of $N$ normalized by $\mathcal{L}(G)$ and subgroups of $G$. This means that for groups of small order the problem can be approached from a quantitative point of view; in [102], the authors used GAP [77] to deal with groups of order $42$ and found some non-classical Hopf–Galois structures for which the number of subgroups of the Galois group $G$ equals the number of subgroups of $N$ normalized by $\mathcal{L}(G)$, meaning that the Hopf–Galois correspondence for these structures is surjective.

A deeper look in the literature seems to suggest that these cases are not really common. Besides these examples and the aforementioned classical structure and canonical non-classical structure when $G$ is Hamiltonian, there exists only one other known class of Hopf–Galois structures for which the Hopf–Galois correspondence is surjective. The problem of the surjectivity of the Hopf–Galois correspondence was rephrased as a problem on finite commutative Jacobson radical rings by Childs [59], who showed that given a Hopf–Galois structure on $L/K$ with Hopf algebra $H$, there exists a bijective correspondence between $K$-Hopf subalgebras of $H$ and ideals of the associated rings. In this way, Childs proved that for all the Hopf–Galois structures on a Galois extension with Galois group cyclic of odd prime power order, the Hopf–Galois cor-

respondence is surjective. Independently of Childs, Bachiller noted in [10] that Hopf–Galois structures of abelian type and left braces are connected since they are both inherently related to regular subgroups of the holomorph of abelian groups. This connection was then further deepened in [60] and in the appendix of Byott and Vendramin in [151], where Childs' and Bachiller's ideas were refined in order to relate Hopf–Galois structures with skew braces.

To the best knowledge of the author, besides the ones in [59], there are no further examples of Galois field extensions such that the Hopf–Galois correspondence is surjective for every Hopf–Galois structure on this extension. An interesting approach to better understand this phenomenon is given in [60, 62]. Namely, instead of looking for Hopf–Galois structures for which the Hopf–Galois correspondence is surjective, one can study the failure of the surjectivity. Given a Hopf–Galois structure on $L/K$ with Hopf algebra $H$, how far is the Hopf–Galois correspondence from being surjective? The idea is to compute (or estimate) the ratio between the number of $K$-Hopf subalgebras of $H$ and the number of intermediate fields of $L/K$, which was translated by Childs in a problem regarding just the associated skew brace. A possible explanation for the lack of new examples could be given by the fact that the substructures of skew braces studied by Childs, which seem to arise naturally from Hopf–Galois theory, are not the usual substructures considered in the theory of the skew braces, namely, left ideals, strong left ideals, and ideals. This issue was initially addressed by Koch and Truman [103], who showed that the substructures studied by Childs coincide with left ideals of the opposite skew brace. They moved the problem to a more familiar setting, and combined this observation with the results of [102] to describe some known properties of Hopf–Galois structures in terms of the opposite skew brace.

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

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

The idea is that using this new point of view one can explicitly see how the knowledge of the structure of a skew brace gives useful and qualitative information for the associated Hopf–Galois structure.

This chapter is organized as follows. In Section 7.1, we discuss the earlier-mentioned known connection between skew braces and Hopf–Galois structures in more detail. We also mention some of the less convenient properties of this connection. In Section 7.2, we explicitly describe the new connection that we propose. We remark how the known advantages of the usual connection still apply in the new perspective, and we see how some old and new results can be explained and derived. In Section 7.3, we use the new point of view to deal with the Hopf–Galois correspondence. In particular, we present new qualitative results, examples, and statements to explain from a more general perspective why in some situations the Hopf–Galois correspondence is surjective. Concretely, in Theorem 7.3.23 we obtain a full classification of Galois field extensions such that the Hopf–Galois correspondence is surjective for any Hopf–Galois structure on it. A main role here is played by bi-skew braces.

All results in this chapter for which no external reference is given were obtained in collaboration with Lorenzo Stefanello and have been published in [155].

## 7.1 The existing connection

We recall the well-known connection between Hopf–Galois structures and skew braces. While it was originally developed in the appendix of Byott and Vendramin in [151], we present here an equivalent version,

which does not involve explicitly the holomorph, as described in [125, Proposition 2.1]. See also [63, section 2.8]. This is based on the following result, which is a different interpretation of Proposition 1.1.9. Here we use a slightly refined version of the notation as in Section 1.5.3: for a group $(G, \cdot)$, the left regular action is denoted by

$$\mathcal{L}^{\cdot} : G \to \mathbb{S}_G,$$

and the right regular action by

$$\mathcal{R}^{\cdot} : G \to \mathbb{S}_G.$$

**Proposition 7.1.1.** *Let $(G, \cdot)$ and $(G, \circ)$ be groups with the same identity. Then $(G, \cdot, \circ)$ is a skew brace if and only if $\mathcal{L}^{\cdot}(G)$ is normalized by $\mathcal{L}^{\circ}(G)$ in $\mathbb{S}_G$.*

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

- Consider a Hopf–Galois structure on $L/K$, corresponding to a regular subgroup $N$ of $\mathbb{S}_G$ normalized by $\mathcal{L}^{\circ}(G)$. We can use the bijection

  $$\nu : N \to G : \eta \mapsto \eta(1)$$

  to transport the group structure of $N$ to $G$. In this way, we find a group structure $(G, \cdot)$ for which $\mathcal{L}^{\cdot}(G) = N$. By Proposition 7.1.1, we conclude that $(G, \cdot, \circ)$ is a skew brace.

- Let $(A, \cdot, \circ)$ be a skew brace with $(A, \circ) \cong (G, \circ)$. Use this bijection to transport the structure of $(A, \cdot)$ to $G$, to find a skew brace $(G, \cdot, \circ)$ isomorphic to $(A, \cdot, \circ)$. By Proposition 7.1.1, we have that $N = \mathcal{L}^{\cdot}(G)$ is normalized by $\mathcal{L}^{\circ}(G)$, so we obtain a Hopf–Galois structure on $L/K$.

**Example 7.1.2.** Peculiarly, under this connection, the classical structure yields the almost trivial skew brace. On the other hand, the trivial skew brace is obtained by the canonical non-classical structure. See Examples 1.5.7 and 1.5.8.

We immediately state an important and well-known consequence.

**Theorem 7.1.3.** *Let $N$ and $G$ be finite groups. Then the following are equivalent:*

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

We underline that the previous connection is not bijective, as distinct Hopf–Galois structures can correspond to isomorphic skew braces. This was precisely quantified in [125, Corollary 2.4]; see also [104, Corollary 3.1]. However, there is a way to obtain from this connection a bijective correspondence. Indeed, as a consequence of Proposition 7.1.1 (see [43, section 7]), given a group $(G, \circ)$, there exists a bijective correspondence between group operations $\cdot$ such that $(G, \cdot, \circ)$ is a skew brace and regular subgroups of $\mathbb{S}_G$ normalized by $\mathcal{L}^{\circ}(G)$, via

$$\cdot \mapsto \mathcal{L}^{\cdot}(G).$$

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

## 7.2 A refined connection

We begin with our main result, in which we propose an adapted version of the connection between Hopf–Galois structures and skew braces. We underline that some of the consequences, as developed in this section, can also be obtained from the usual theory, for example from [102], together with the observations on opposite skew braces in [103, Theorem 5.6]. However, we prefer to develop the theory directly from this new perspective, to highlight how old and new statements can be derived in a transparent way, without too much effort.

**Theorem 7.2.1.** *Let $L/K$ be a finite Galois extension of fields with Galois group $(G, \circ)$. Then the following data are equivalent:*

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

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

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

*Proof.* Denote by $\mathcal{S}$ the set of group operations $\cdot$ on $G$ such that $(G, \cdot, \circ)$ is a skew brace, and by $\mathcal{N}$ the set of regular subgroups of $\mathbb{S}_G$ normalized by $\mathcal{L}^\circ(G)$. Consider the composition

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

where the first map is the bijection that sends $\cdot$ to $\cdot_{\mathrm{op}}$ and the second map is the bijection that sends $\cdot$ to $\mathcal{L}^\cdot(G)$, as described at the end of Section 7.1. Since $\mathcal{L}^{\cdot_{\mathrm{op}}}(G) = \mathcal{R}^\cdot(G)$, we obtain a bijection

$$\mathcal{S} \to \mathcal{N} : \cdot \mapsto \mathcal{R}^\cdot(G),$$

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

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

$$\sigma \mapsto \mathcal{R}^\cdot(\sigma)^{-1}.$$

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

$$\mathcal{R}^\cdot(\lambda_\sigma(\tau))^{-1} = \mathcal{L}^\circ(\sigma)\mathcal{R}^\cdot(\tau)^{-1}\mathcal{L}^\circ(\sigma)^{-1}.$$

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

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

while the right-hand side element is the unique element of $\mathcal{R}^\cdot(G)$ which sends $1 \in G$ to

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

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

$$\sum_{\sigma\in G}\ell_\sigma\sigma\mapsto\sum_{\sigma\in G}\ell_\sigma\mathcal{R}^{\cdot}(\sigma)^{-1}.$$

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

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

□

*Remark* 7.2.2. Following the proof of Theorem 7.2.1, it should be clear that we are associating with a Hopf–Galois structure on $L/K$ the skew brace that is opposite to the usual one. Explicitly, given a Hopf–Galois structure in Greither–Pareigis terms, so a regular subgroup $N$ of $\mathbb{S}_G$ normalized by $\mathcal{L}^\circ(G)$, then the way to find the operation $\cdot$ associated to this structure is the following:

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

where $\nu\colon N\to G$ is the usual bijection that maps $\eta$ to $\eta(1)$.

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

*Notation* 7.2.3. To lighten the notation, we associate a Hopf–Galois structure on $L/K$ with a skew brace $(G,\cdot,\circ)$, implicitly meaning the operation $\cdot$ such that $(G,\cdot,\circ)$ is a skew brace.

We immediately see that the new version of the connection fixes the behavior described in Example 7.1.2.

**Example 7.2.4.** Consider the trivial skew brace $(G,\circ,\circ)$. As the $\lambda$-action in this case is given by $\lambda_\sigma=\mathrm{id}$, we find that the Hopf algebra in the Hopf–Galois structure on $L/K$ associated with $(G,\circ,\circ)$ is $K[G,\circ]$, and we recover the classical structure.

**Example 7.2.5.** If instead we consider the almost trivial skew brace $(G,\circ_{\mathrm{op}},\circ)$, we find the Hopf–Galois structure on $L/K$ originally corresponding to $\mathcal{L}^\circ(G)$, that is, the canonical non-classical structure.

**Example 7.2.6.** Let $A$ and $B$ be finite groups. Consider a group homomorphism $\alpha\colon B\to\mathrm{Aut}(A)$, and suppose that $(G,\circ)$ is the semidirect product of $A$ and $B$ with respect to $\alpha$. Given $(a,b)\in G$ and $x\in L$, write $(a,b)(x)$ for the Galois action. Finally, take $(G,\cdot)=A\times B$. Then by [83, Example 1.4], we have that $(G,\cdot,\circ)$ is a skew brace. We obtain a Hopf–Galois structure on $L/K$, which we now describe.

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

$$\lambda_{(c,d)}(a,b)=(\alpha_d(a),b).$$

In particular, the $K$-Hopf algebra $L[G,\cdot]^{(G,\circ)}$ we obtain consists of the elements

$$\sum_{(a,b)\in G}\ell_{(a,b)}(a,b)\in L[G,\cdot],$$

that satisfy,

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

for all $(c, d) \in G$. Such an element acts on $L$ as follows:

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

The known results about existence and classification can also be translated and obtained using the new point of view. Indeed, Theorem 7.1.3 immediately follows from Theorem 7.2.1, as well as the result counting the number of Hopf–Galois structures associated with the same isomorphism class of a skew brace. We recall this result and its proof here, which is just a slight modification of the proof of [104, Corollary 3.1].

**Proposition 7.2.7.** *Let $(G, \cdot, \circ)$ be a skew brace. Then there are*

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

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

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

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

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

We also remark that Byott's translation [34] for Galois extensions, an extremely useful tool to count Hopf–Galois structures, can be obtained in this fashion. We recall here the statement and a quick proof, along the lines of the one described in [58, section 7], but without involving regular subgroups. Let $(N, \cdot)$ be a group of the same order as $(G, \circ)$. Denote by $e(G, N)$ the number of Hopf–Galois structures on $L/K$ of type $(N, \cdot)$, which by Theorem 7.2.1 equals the number of operations $\cdot$ such that $(G, \cdot, \circ)$ is a skew brace with $(G, \cdot) \cong (N, \cdot)$, and denote by $f(G, N)$ the number of operations $\circ$ such that $(N, \cdot, \circ)$ is a skew brace with $(N, \circ) \cong (G, \circ)$.

**Theorem 7.2.8.** *The following equality holds:*

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

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

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

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

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

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

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

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

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

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

**Theorem 7.2.9.** *The $K$-Hopf subalgebra of $L[G,\cdot]^{(G,\circ)}$ are precisely those of the form $L[G',\cdot]^{(G,\circ)}$ for left ideals $G'$ of $(G,\cdot,\circ)$. Moreover, $L[G',\cdot]^{(G,\circ)}$ is normal in $L[G,\cdot]^{(G,\circ)}$ if and only if $G'$ is a strong left ideal of $(G,\cdot,\circ)$.*

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

Consider a left ideal $G'$ of $(G,\cdot,\circ)$. Then $G'$ corresponds to an intermediate field $L^{H'}$ of $L/K$ via the Hopf–Galois correspondence, where $H'=L[G',\cdot]^{(G,\circ)}$. But as $G'$ is a subgroup of $(G,\circ)$, we have that $G'$ also corresponds to an intermediate field $F$ of $L/K$ via the usual Galois correspondence. We denote both fields by $L^{G'}$, the ambiguity justified by the following pleasant consequence of Theorem 7.2.1.

**Corollary 7.2.10.** *Within the above setting, the equality $L^{H'}=F$ holds.*

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

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

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

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

**Corollary 7.2.11.** *The grouplike elements of the $K$-Hopf algebra $L[G,\cdot]^{(G,\circ)}$ are precisely the elements of* $\mathrm{Fix}(G,\cdot,\circ)$.

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

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

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

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

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

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

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

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

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

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

  as $K$-Hopf algebras.

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

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

  as $F_2$-Hopf algebras.

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

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

## 7.3 The Hopf–Galois correspondence

In this final section, we study the Hopf–Galois correspondence with respect to the new version of the connection. We fix a finite Galois extension of fields $L/K$ with Galois group $(G, \circ)$. From the discussion of Section 7.2, we immediately derive the following result.

**Corollary 7.3.1.** *Consider a Hopf–Galois structure on $L/K$, with associated skew brace $(G, \cdot, \circ)$. Then the Hopf–Galois correspondence for this structure is surjective if and only if every subgroup of $(G, \circ)$ is a left ideal of $(G, \cdot, \circ)$.*

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

**Example 7.3.2.** Consider the classical structure, with associated skew brace $(G, \circ, \circ)$. In this case, every subgroup of $(G, \circ)$ is a left ideal of $(G, \circ, \circ)$, so we find, as expected, that the Hopf–Galois correspondence for this structure is surjective.

We note the following facts, which are direct consequences of Corollary 7.3.1

**Corollary 7.3.3.** *If $(G, \cdot, \circ)$ is a skew brace and $(G, \cdot)$ has less subgroups than $(G, \circ)$. Then for the Hopf–Galois structure on $L/K$ associated with $(G, \cdot, \circ)$, the Hopf–Galois correspondence is not surjective.*

**Corollary 7.3.4.** *Suppose that $(G, \cdot, \circ)$ is a skew brace isomorphic to the direct product of skew braces $(G_i, \cdot, \circ)$ of pairwise coprime orders. If all the subgroups of $(G_i, \circ)$ are left ideals of $(G_i, \cdot, \circ)$, the Hopf–Galois correspondence is surjective.*

We focus our attention now on Hopf–Galois structures associated with bi-skew braces. In this case, the $\lambda$-action acts by automorphisms of $(G, \circ)$, so we easily derive the following fact.

**Lemma 7.3.5.** *Consider a Hopf–Galois structure on $L/K$ such that the associated skew brace $(G, \cdot, \circ)$ is a bi-skew brace. Let $G'$ be a characteristic subgroup of $(G, \circ)$. Then $L^{G'}$ is in the image of the Hopf–Galois correspondence for this structure.*

**Corollary 7.3.6.** *Suppose that $(G, \circ)$ is a cyclic group, and consider a Hopf–Galois structure on $L/K$ such that the associated skew brace $(G, \cdot, \circ)$ is a bi-skew brace. Then the Hopf–Galois correspondence for this structure is surjective.*

**Example 7.3.7.** Suppose that $(G, \circ)$ is cyclic of order $8$. As shown in [133], there exists a skew brace $(G, \circ, \cdot)$ with $(G, \cdot) \cong Q_8$, the quaternion group. A straightforward calculation shows that $(G, \circ, \cdot)$ is a bi-skew brace. We conclude by Corollary 7.3.6 that for the Hopf–Galois structure on $L/K$ associated with the skew brace $(G, \cdot, \circ)$, the Hopf–Galois correspondence is surjective.

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

**Example 7.3.8.** Suppose that $(G, \circ)$ is the direct product of an abelian group $A$ and the cyclic group $C_2$ of order 2. Denote by $\alpha$ the action of $C_2$ on $A$ via inversion, and consider the semidirect product $(G, \cdot) = A \rtimes C_2$ with respect to this action. Then $(G, \cdot, \circ)$ is a bi-skew brace; see Example 2.2.6. Here the $\lambda$-action of $(G, \cdot, \circ)$ is given as follows:

$$\lambda_{(c,d)}(a, b) = (\alpha_d(a), b),$$

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

We deal now with bi-skew braces $(G, \cdot, \circ)$ whose $\lambda$-action is by inner automorphisms of $(G, \circ)$, as featured in Example 2.4.11. Denote by $N(G, \circ)$ the *norm* of $(G, \circ)$, that is, the intersection of the normalizers of the subgroups of $(G, \circ)$. It is clear that conjugation by $\sigma$ in $(G, \circ)$ is a power automorphism of $(G, \circ)$ if and only if $\sigma \in N(G, \circ)$.

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

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

here by $\psi(\sigma)$ we denote any element in the coset $\psi(\sigma)$ in $N(G,\circ)/Z(G,\circ)$, with a little abuse of notation justified by the fact that if $\tau \in Z(G,\circ)$, then conjugation by $\tau$ is trivial.

**Theorem 7.3.9.** *For all group homomorphisms $\psi\colon (G,\circ) \to N(G,\circ)/Z(G,\circ)$, we have that $(G,\cdot_\psi,\circ)$ is a bi-skew brace, and for the Hopf–Galois structure on $L/K$ associated with $(G,\cdot_\psi,\circ)$, the Hopf–Galois correspondence is surjective.*

*Proof.* Let $\psi\colon (G,\circ) \to N(G,\circ)/Z(G,\circ)$ be a group homomorphism. By the main theorem of [140], the quotient $N(G,\circ)/Z(G,\circ)$ is abelian, so as described in Example 2.4.11 we find that $(G,\cdot_\psi,\circ)$ is a bi-skew brace and the $\lambda$-action of $(G,\cdot_\psi,\circ)$ is given by $\lambda_\sigma(\tau) = \overline{\psi(\sigma)} \circ \tau \circ \psi(\sigma)$. In particular, the $\lambda$-action of $(G,\cdot_\psi,\circ)$ is given by conjugation by elements of $N(G,\circ)$ in $(G,\circ)$, so by power automorphisms of $(G,\circ)$, and therefore we obtain our assertion. □

**Example 7.3.10.** Suppose that $(G,\circ) = Q_8$, the quaternion group of order $8$. There are 22 Hopf–Galois structures on $L/K$, and 6 of them are of cyclic type; see [151, Table 2]. As $(G,\circ)$ is Hamiltonian, we derive that $N(G,\circ) = G$, so $N(G,\circ)/Z(G,\circ) \cong C_2 \times C_2$. Since there are $16$ distinct group homomorphisms

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

we obtain $16$ distinct Hopf–Galois structures on $L/K$ for which the Hopf–Galois correspondence is surjective. We find indeed all the Hopf–Galois structures on $L/K$ except for the $6$ of cyclic type, for which the Hopf–Galois correspondence is not surjective by Corollary 7.3.3.

**Example 7.3.11.** Suppose that $(G,\circ)$ is the extraspecial group of order $p^3$ and exponent $p^2$, with $p$ an odd prime. Then $N(G,\circ)$ is the elementary abelian subgroup of $(G,\circ)$ of order $p^2$, while the center is cyclic of order $p$. As there are $p^2$ distinct group homomorphisms

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

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

The following result, whose proof is immediate, shows that the behavior of the canonical non-classical structure can also be displayed by other Hopf–Galois structures.

**Proposition 7.3.12.** *Consider a Hopf–Galois structure on $L/K$ such that associated skew brace $(G,\cdot,\circ)$ is a bi-skew brace with $\lambda$-action $\lambda\colon (G,\circ) \to \mathrm{Inn}(G,\circ)$. Then every normal intermediate field $K$ of $L/K$ is in the image of the Hopf–Galois correspondence for this structure.*

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

**Example 7.3.13.** Consider the canonical non-classical structure, with associated skew brace $(G,\circ_{\mathrm{op}},\circ)$. Here $\lambda_\sigma(\tau) = \sigma \circ \tau \circ \overline{\sigma}$ for all $\sigma,\tau \in G$. Applying Proposition 7.3.12, we recover the well-known property of the canonical non-classical structure.

**Example 7.3.14.** Suppose that $(G,\circ)$ is nilpotent of class two, and define

$$\sigma \cdot \tau = \sigma \circ \sigma \circ \tau \circ \overline{\sigma}.$$

Then by Example 2.4.11 we have that $(G,\cdot,\circ)$ is a bi-skew brace and the $\lambda$-action of $(G,\cdot,\circ)$ is given by $\lambda_\sigma(\tau) = \overline{\sigma} \circ \tau \circ \sigma$. By Proposition 7.3.12, we derive that for the associated Hopf–Galois structure on $L/K$, the image of the Hopf–Galois correspondence consists precisely of the normal intermediate fields of $L/K$.

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

We study now a question posed in [62]. Let $L_1/K_1$ be a finite Galois extension of fields with Galois group $(G, \circ)$, and consider a Hopf–Galois structure on $L_1/K_1$, with associated skew brace $(G, \cdot, \circ)$. We can rewrite the *Hopf–Galois correspondence ratio*, defined as the ratio of the number of intermediate fields of $L_1/K_1$ in the image of the Hopf–Galois correspondence to the number of intermediate fields of $L_1/K_1$, as follows:

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

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

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

**Theorem 7.3.15.** *The following facts hold:*

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

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

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

**Example 7.3.16.** Suppose that $(G, \cdot, \circ)$ is the skew brace of Example 7.3.8 with $p$ an odd prime and $A = C_p$. Then $(G, \cdot)$ is dihedral of order $2p$ and $(G, \circ)$ is cyclic of order $2p$. There are $p + 3$ subgroups of $(G, \cdot)$ and $4$ subgroups of $(G, \circ)$, and as every subgroup of $(G, \circ)$ is a left ideal of $(G, \cdot, \circ)$, we have the following equalities:

$$\begin{aligned} GC(L_1/K_1, L_1[G, \cdot]^{(G,\circ)}) &= 1, \\ GC(L_2/K_2, L_2[G, \circ]^{(G,\cdot)}) &= \frac{4}{p+3}, \\ \frac{GC(L_1/K_1, L_1[G, \cdot]^{(G,\circ)})}{GC(L_2/K_2, L_2[G, \circ]^{(G,\cdot)})} &= \frac{p+3}{4}. \end{aligned}$$

We conclude by focusing our attention on Hopf–Galois structures associated with skew braces that are not necessarily bi-skew braces. We begin with the following theorem, which was proved in [106]. We provide a quick proof for convenience.

**Theorem 7.3.17.** *Let $N$ be a group. If there exists $m$ such that the number of characteristic subgroups of order $m$ of $N$ is greater than the number of subgroups of order $m$ of $(G, \circ)$. Then $L/K$ has no Hopf–Galois structures of type $N$.*

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

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

**Proposition 7.3.18.** *Consider a Hopf–Galois structure on $L/K$, with associated skew brace $(G, \cdot, \circ)$. Suppose that the number of characteristic subgroups of $(G, \cdot)$ equals the number of subgroups of $(G, \circ)$. Then the Hopf–Galois correspondence for this structure is surjective.*

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

**Example 7.3.19.** Suppose that $(G, \circ)$ is cyclic of odd prime power order, and consider a Hopf–Galois structure on $L/K$, with associated skew brace $(G, \cdot, \circ)$. By [105], also $(G, \cdot)$ is cyclic, so by Proposition 7.3.18, we conclude that the Hopf–Galois correspondence is surjective; we have recovered [59, Proposition 4.3].

**Example 7.3.20.** Suppose that $(G, \circ)$ is cyclic of order $2^m$, with $m \geq 1$, and consider a Hopf–Galois structure on $L/K$, with associated skew brace $(G, \cdot, \circ)$. We claim that the Hopf–Galois correspondence for this structure is surjective.

If $m = 1, 2$, then by the explicit classification in [9, Proposition 2.4], one can check that $(G, \cdot, \circ)$ is a bi-skew brace, so the result follows from Corollary 7.3.6.

Suppose now that $m \geq 3$. By [36, Theorem 6.1], necessarily $(G, \cdot)$ is cyclic, the dihedral group, or the generalized quaternion group. With the unique exception of $m = 3$ and $(G, \cdot) \cong Q_8$, the numbers of characteristic subgroups of $(G, \cdot)$ and subgroups of $(G, \circ)$ coincide, so we conclude by Proposition 7.3.18.

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

*Remark* 7.3.21. With the classification given in [9], it is easy to construct a skew brace $(G, \cdot, \circ)$ with $(G, \circ)$ cyclic of order $p^3$, where $p$ is a prime, such that $(G, \cdot, \circ)$ is not a bi-skew brace. Thus Examples 7.3.19 and 7.3.20 do not follow from Corollary 7.3.6.

We shall now conclude by characterizing all the Galois extensions that behave like Examples 7.3.19 and 7.3.20. First, a useful lemma.

**Lemma 7.3.22.** *Suppose that $(G, \circ)$ is isomorphic to a direct product of groups $(A, \circ)$ and $(B, \circ)$, and that there exists a skew brace $(A, \cdot, \circ)$ such that not every subgroup of $(A, \circ)$ is a left ideal of $(A, \cdot, \circ)$. Then there exists a Hopf–Galois structure on $L/K$ for which the Hopf–Galois correspondence is not surjective.*

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

**Theorem 7.3.23.** *The following are equivalent:*

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

*Proof.* Suppose first that $(G, \circ)$ is cyclic of order $n$ and for all primes $p$ and $q$ dividing $n$, we have that $p$ does not divide $q - 1$. Consider a Hopf–Galois structure on $L/K$, with associated skew brace $(G, \cdot, \circ)$. If $n$ is even, then $n$ has no odd prime divisors, so the result follows from Example 7.3.20.

If instead $n$ is odd, then by [160, Corollary 1.6], we have that $(G, \cdot)$ is isomorphic to a semidirect product of cyclic groups $C_a \rtimes C_b$, where $a$ and $b$ are coprime and $ab = n$. But by the assumption on the divisors of the order of $(G, \circ)$, this semidirect product is necessarily a direct product. In particular, $(G, \cdot)$ is cyclic, and we can apply [55, Corollary 4.3] to deduce that $(G, \cdot, \circ)$ is isomorphic to a direct product of skew braces of coprime odd prime power order. The assertion then follows from Corollary 7.3.4 and Example 7.3.19.

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

Suppose first that $(G, \circ)$ is Hamiltonian. Then there exists an abelian group $A$ such that $(G, \circ)$ is isomorphic to the direct product of $Q_8$ and $A$; see [84, Theorem 12.5.4]. As already mentioned, there exists a skew brace $(G', \cdot, \circ)$ where $(G', \circ) \cong Q_8$ and $(G', \cdot)$ is cyclic. By applying Corollary 7.3.3 and Lemma 7.3.22, we derive a contradiction.

We deduce that $(G, \circ)$ is necessarily abelian. Suppose that $(G, \circ)$ is not cyclic. Then there exists a prime $p$ such that $(G, \circ)$ is isomorphic to a direct product of the form $C_{p^r} \times C_{p^s} \times A$, where $1 \leq s \leq r$. Write $\sigma$ for a generator of $C_{p^r}$ and $\tau$ for a generator of $C_{p^s}$. In a slight variation of [154, Example 6.7], there exists a skew brace $(G', \cdot, \circ)$ such that $(G', \circ)$ equals $C_{p^r} \times C_{p^s}$ with the direct product operation and

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

Note that the subgroup $C_{p^r} \times \{1\}$ of $(G', \circ)$ is not a subgroup of $(G', \cdot)$, so in particular it is not a left ideal of $(G', \cdot, \circ)$. Again by Lemma 7.3.22, we find a contradiction.

We deduce that $(G, \circ)$ is necessarily cyclic. Suppose that there exist primes $p$ and $q$ dividing the order of $(G, \circ)$ such that $p$ divides $q - 1$. Let $(G', \circ)$ be the direct product of the Sylow $q$-subgroup $Q$ and the Sylow $p$-subgroup $P$ of $(G, \circ)$. By assumption on $p$ and $q$, we can construct a non-trivial semidirect product $(G', \cdot)$ of $Q$ and $P$. By [83, Example 1.5], we have that $(G', \cdot, \circ)$ is a skew brace. Suppose that $\{1\} \times P$ is a left ideal of $(G', \cdot, \circ)$. Then $\{1\} \times P$ is not a left ideal of $(G', \cdot_{\mathrm{op}}, \circ)$, because otherwise $\{1\} \times P$ would be normal subgroup of $(G', \cdot)$. As $(G, \circ)$ is isomorphic to the direct product of all its Sylow subgroups, we find a contradiction from Lemma 7.3.22. □

*Remark* 7.3.24. Recently, in [156], Stefanello and Tsang classified all groups $(G, \cdot)$ such that for any skew brace $(G, \cdot, \circ)$ every subgroup of $(G, \circ)$ is a left ideal. The classification of such groups is very similar to the one in Theorem 7.3.23.

Chapter 8

# A Lazard correspondence for skew braces and post-Lie rings

In [147], Smoktunowicz proved that the construction of the group of formal flows, originally developed for pre-Lie algebras in [2], could be adapted to left nilpotent pre-Lie rings of prime power order $p^k$, with $k+1<p$, to obtain braces with the same additive structure. Recall from Corollary 8.6.4 that a skew brace of prime power order is always left nilpotent. She also gives an inverse construction for strongly nilpotent braces of order $p^k$, with $k<p-1$, whose strong nilpotency index is at most $p-1$. This correspondence was used in [127] to classify all strongly nilpotent braces of order $p^4$, for $p>5^5$, while the non-strongly nilpotent ones of this order were classified earlier in [128]. In [143], Shalev and Smoktunowicz also gave a construction that starts from a brace $(A,+,\circ)$ of order $p^k$, with $k+1<p$, in order to obtain a pre-Lie ring on the quotient group $(A,+)/\{a\in A \mid p^2a=0\}$. Although the strong nilpotency condition is no longer present, one cannot hope that this yields a correspondence, as the additive group is not preserved. We also note that in [87], Iyudu gave a construction of the associated graded pre-Lie ring of a strongly nilpotent brace.

It was known by Auslander [8] that from a regular affine action of a Lie group on $\mathbb{R}^n$ one obtains a pre-Lie algebra by differentiation. Kim proved in [98] that a pre-Lie algebra is obtained from such a regular affine action if and only if it is transitive. In [27], Burde, Dekimpe and Deschamps established a correspondence between regular affine actions of connected, simply connected nilpotent Lie groups and certain post-Lie algebras. Here too, left nilpotency plays a crucial role, as well as the fact that for a finite dimensional Lie algebra $\mathfrak{g}$, we can naturally identify $\mathfrak{der}(\mathfrak{g})$ with the tangent space of $\mathrm{Aut}^\infty(\mathfrak{g})$ at 1. Consequently, the tangent space of $\mathrm{Hol}^\infty(G)$ at 1 can be identified with $\mathfrak{aff}(\mathfrak{g})$, for $G$ a Lie group whose tangent space is $\mathfrak{g}$. Note that a similar result does generally not hold for the Lazard correspondence. A first obstruction is that for a Lazard Lie algebra $\mathfrak{g}$, the group $\mathrm{Aut}(\mathfrak{g})$ and the Lie algebra $\mathfrak{der}(\mathfrak{g})$ are usually not nilpotent, so there is no hope to relate them through the Lazard correspondence. The following example illustrates this.

**Example 8.0.1.** Consider a field $K$ and let $\mathfrak{g}$ be the trivial Lie algebra on $K^n$ with filtration

$$K^n \supseteq \{0\}\times K^{n-1} \supseteq \{0\}^2\times K^{n-2} \supseteq \ldots \supseteq \{0\}^{n-1}\times K\times\{0\}^n.$$

Then $\mathfrak{g}$ is Lazard if $K$ has characteristic 0 or $n$ is smaller than the characteristic of $K$. The group of automorphisms of $\mathfrak{g}$, viewed simply as a Lie algebra, is the group of invertible $n\times n$-matrices over $K$, which is not nilpotent and, in most cases, not even solvable. One could also consider the automorphisms of

$\mathfrak{g}$ as a filtered Lie algebra, but then one finds the group of invertible upper triangular $n \times n$-matrices over $K$, which is always solvable, but not nilpotent. Similarly, the derivations of $\mathfrak{g}$, viewed as a Lie algebra, form the Lie algebra of $n \times n$-matrices over $K$, which is non-solvable. If we restrict to those derivations of $\mathfrak{g}$ that also map $\mathfrak{g}_i$ to $\mathfrak{g}_i$, then we obtain the Lie algebra of upper triangular matrices, which is solvable, but not nilpotent.

Bai, Guo, Sheng and Tang showed more generally how, starting from a regular affine action of a Lie group on another Lie group, one obtains a post-Lie algebra through differentiation [15]. Conversely, also a construction by formal integration was given to construct a skew brace starting from a post-Lie algebra of characteristic 0 and with some completeness conditions.

The goal of this chapter is to develop a Lazard correspondence between post-Lie rings and skew braces, and to discuss how the above-mentioned results and constructions follow from the obtained correspondence. First, filtered Lie algebras and filtered groups are discussed in more detail in Sections 8.1 and 8.2. In particular, we introduce semidirect sums and products and study how they behave with respect to the property of being Lazard. In Section 8.3 we relate derivations and automorphisms of Lazard Lie algebras, and we show that, when working in the right setting, the Lazard correspondence maps semidirect sums of Lazard Lie algebras to semidirect products of Lazard groups. Note the similarity to how the tangent plane at 1 of a semidirect product of Lie groups $A \rtimes G$ can be identified with the semidirect sum $\mathfrak{a} \oplus_\delta \mathfrak{g}$ where $\mathfrak{a}$ and $\mathfrak{g}$ are the tangent spaces in 1 of $A$ and $G$ respectively. In particular, choosing the correct definitions of the holomorph of a filtered group and the affine Lie ring of a filtered Lie ring, we find in Proposition 8.3.5 that the Lazard correspondence relates these two objects. In Section 8.4 we then introduce the notion of Lazard post-Lie rings and Lazard skew braces, and we obtain a functorial bijective correspondence between these two families in Theorem 8.4.14 which is our principal result of this chapter. The notion of $L$-nilpotency appears naturally when studying Lazard post-Lie rings and Lazard skew braces, and we further discuss this in Sections 8.5 and 8.6. In particular, in Theorem 8.6.6 we prove that any left nilpotent skew brace with a nilpotent additive group has a nilpotent multiplicative group and the nilpotency class can be bounded in terms of the $L$-nilpotency class. This extends one implication of [55, Theorem 4.8]. In Section 8.7 we then discuss implications on the theory of post-Lie rings and skew braces of prime power order. In particular, we prove an analog of Theorem 1.4.34 by showing that for a fixed prime power $p^n$ there is a functorial bijective correspondence between post-Lie rings of size $p^n$ and $L$-nilpotency class less than $p$ and skew braces satisfying the same restrictions. In Section 8.8 we study the other extremal case where $R = \mathbb{R}$, in particular we relate our results to the work of Burde, Dekimpe and Deschamps, and Bai, Guo, Shang and Teng. We conclude this chapter by extending our correspondence to post-Lie rings and skew braces that can be obtained as a completion of Lazard ones. Subsequently, we compare this to the work by Agrachev and Gamkrelidze on the formal group of flows of a pre-Lie algebra, and to the formal integration of complete post-Lie algebras as introduced by Bai, Guo, Sheng and Tang.

Throughout the whole chapter, algebras, Lie algebras and post-Lie algebras are taken over a commutative ring $R$ unless specified otherwise. In particular, all results for algebras, Lie algebras and post-Lie algebras also hold for rings, Lie rings and post-Lie rings respectively, since this concerns the particular case $R = \mathbb{Z}$.

All results for which no external reference is given are the author's own work and are contained in the preprint [159].

## 8.1 Filtered Lie algebras

For $\mathfrak{g}$ a filtered Lie algebra, we denote by $\mathfrak{Der}_f(\mathfrak{g})$ the set of all derivations $\delta$ of the Lie algebra $\mathfrak{g}$ such that moreover $\delta(\mathfrak{g}_i) \subseteq \mathfrak{g}_{i+1}$ for all $i \geq 1$.

**Lemma 8.1.1.** *Let $\mathfrak{g}$ be a filtered Lie algebra. Then $\mathfrak{der}_f(\mathfrak{g})$ is a Lie subalgebra of $\mathfrak{der}(\mathfrak{g})$. Moreover, it is a filtered Lie algebra for the filtration*

$$\mathfrak{der}_f(\mathfrak{g})_i = \{\delta \in \mathfrak{der}_f(\mathfrak{g}) \mid \delta(\mathfrak{g}_j) \subseteq \mathfrak{g}_{i+j} \text{ for all } j \geq 1\}.$$

*Proof.* It is a direct consequence of its definition that $\mathfrak{der}_f(\mathfrak{g})_i$ is a submodule of $\mathfrak{der}_f(\mathfrak{g})$ for each $i \geq 1$. Also, if $\delta \in \mathfrak{der}_f(\mathfrak{g})_i$ and $\delta' \in \mathfrak{der}_f(\mathfrak{g})_j$ then $\delta\delta' \in \mathfrak{der}_f(\mathfrak{g})_{i+j}$ which implies the inclusion $[\mathfrak{der}_f(\mathfrak{g})_i, \mathfrak{der}_f(\mathfrak{g})_j] \subseteq \mathfrak{der}_f(\mathfrak{g})_{i+j}$. □

**Example 8.1.2.** Let $x$ be an element of a filtered Lie algebra $\mathfrak{g}$. Then the adjoint map $\mathrm{ad}_x$ where

$$\mathrm{ad}_x : \mathfrak{a} \to \mathfrak{a} : y \mapsto [x, y],$$

is contained in $\mathfrak{der}_f(\mathfrak{g})$. More precisely, if $x \in \mathfrak{g}_i$ then $\mathrm{ad}_x \in \mathfrak{der}_f(\mathfrak{g})_i$.

Let $\mathfrak{g}, \mathfrak{a}$ be filtered Lie algebras and let $\delta : \mathfrak{g} \to \mathfrak{der}_f(\mathfrak{a})$ be a homomorphism of filtered Lie algebras. Then, as in Proposition 1.3.18, we can consider the semidirect sum $\mathfrak{a} \oplus_\delta \mathfrak{g}$. Recall that this is the direct sum of the underlying modules together with the Lie bracket

$$[(a, x), (b, y)] = ([a, b] + \delta_x(b) - \delta_y(a), [x, y]),$$

for $a, b \in \mathfrak{a}$, $x, y \in \mathfrak{g}$.

**Lemma 8.1.3.** *Let $\mathfrak{g}, \mathfrak{a}$ be filtered Lie algebras and let $\delta : \mathfrak{g} \to \mathfrak{der}_f(\mathfrak{a})$ be a homomorphism of filtered Lie algebras. Then $\mathfrak{a} \oplus_\delta \mathfrak{g}$ is a filtered Lie algebra for the filtration given by $(\mathfrak{a} \oplus_\delta \mathfrak{g})_i = \mathfrak{a}_i \oplus \mathfrak{g}_i$ for $i \geq 1$.*

*Proof.* Let $i, j \geq 1$, $a \in \mathfrak{a}_i$, $b \in \mathfrak{a}_j$, $x \in \mathfrak{g}_i$ and $y \in \mathfrak{g}_j$. Then it suffices to note that $[a, b] \in \mathfrak{a}_{i+j}$ and $[x, y] \in \mathfrak{g}_{i+j}$, and also $\delta_x(b), \delta_y(a) \in \mathfrak{a}_{i+j}$ since $\delta$ is a homomorphism of filtered Lie algebras. □

**Definition 8.1.4.** Let $f : \mathfrak{a} \to \mathfrak{h}$, $g : \mathfrak{h} \to \mathfrak{g}$ and $h : \mathfrak{g} \to \mathfrak{h}$ be homomorphisms of filtered Lie algebras, then

$$0 \longrightarrow \mathfrak{a} \xrightarrow{f} \mathfrak{h} \underset{h}{\overset{g}{\rightleftarrows}} \mathfrak{g} \longrightarrow 0$$

is a *split exact sequence of filtered Lie algebras* if

1. the image of $f$ is precisely the kernel of $g$,
2. the composition $gh$ is the identity map on $\mathfrak{g}$,
3. $f$ induces an isomorphism of filtered Lie algebras $\mathfrak{a} \cong f(\mathfrak{a})$.

*Remark* 8.1.5. It is important to note here that not every injective homomorphism of filtered Lie algebras $f : \mathfrak{a} \to \mathfrak{h}$ induces an isomorphism $\mathfrak{a} \cong f(\mathfrak{a})$, the reason being that a bijective homomorphism is not always an isomorphism. Indeed, a bijective homomorphism of filtered Lie algebras $f : \mathfrak{a} \to \mathfrak{h}$ is an isomorphism if moreover $f(\mathfrak{a}_i) = \mathfrak{h}_i$ for all $i \geq 1$. The same remark holds for filtered groups and algebras.

The following lemma is straightforward to verify.

**Lemma 8.1.6.** *Let $\mathfrak{g}, \mathfrak{a}$ be filtered Lie algebras and let $\delta : \mathfrak{g} \to \mathfrak{der}_f(\mathfrak{a})$ be a homomorphism of filtered Lie algebras. Then*

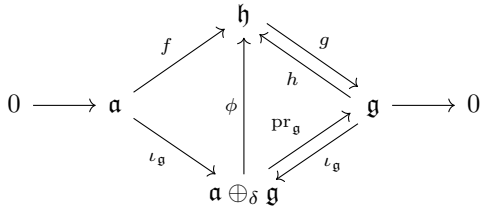
$$0 \longrightarrow \mathfrak{a} \xrightarrow{\iota_\mathfrak{a}} \mathfrak{a} \oplus_\delta \mathfrak{g} \underset{\iota_\mathfrak{g}}{\overset{\mathrm{pr}_\mathfrak{g}}{\rightleftarrows}} \mathfrak{g} \longrightarrow 0$$

*where $\iota_\mathfrak{a}, \iota_\mathfrak{g}$ are the inclusion maps and $\mathrm{pr}_\mathfrak{g}$ is the projection map, is a split exact sequence of filtered Lie algebras.*

**Lemma 8.1.7.** *Let*

$$0 \longrightarrow \mathfrak{a} \xrightarrow{f} \mathfrak{h} \underset{h}{\overset{g}{\rightleftarrows}} \mathfrak{g} \longrightarrow 0$$

*be a split exact sequence of filtered Lie algebras. Then there exists a homomorphism of filtered Lie algebras $\delta : \mathfrak{g} \to \mathfrak{der}_f(\mathfrak{a})$ and an isomorphism of filtered Lie algebras $\phi : \mathfrak{a} \oplus_\delta \mathfrak{g} \to \mathfrak{h}$ such that*




*commutes.*

*Proof.* Define

$$\delta : \mathfrak{g} \to \mathfrak{der}_f(\mathfrak{a}) : x \mapsto \delta_x,$$

with $\delta_x(a) = [h(x), a]$ for all $a \in \mathfrak{a}$, where we identify $\mathfrak{a}$ with $f(\mathfrak{a})$. Since $f(\mathfrak{a}) = \ker g$ is an ideal of $\mathfrak{h}$, the map $\delta_x$ is indeed contained in $\mathfrak{der}_f(\mathfrak{a})$. Also define

$$\phi : \mathfrak{a} \oplus_\delta \mathfrak{g} \to \mathfrak{h} : (a, x) \mapsto f(a) + h(x).$$

The map $\phi$ clearly makes the diagram in the statement commute. Moreover, it is a linear bijection and

$$\begin{aligned}
\phi([(a,x),(b,y)]) &= \phi([a,b] + \delta_x(b) - \delta_y(a), [x,y]) \\
&= f([a,b] + \delta_x(b) - \delta_y(a)) + h([x,y]) \\
&= [f(a), f(b)] + [h(x), f(b)] - [h(y), f(a)] + [(h(x), h(y)] \\
&= [f(a) + h(x), f(b) + h(y)] \\
&= [\phi(a,x), \phi(b,x)]
\end{aligned}$$

for all $a, b \in \mathfrak{a}$, $x, y \in \mathfrak{g}$. It remains to prove that $\phi$ behaves well with respect to the filtrations. To see this, we prove that $\mathfrak{h}_i = f(\mathfrak{a}_i) + h(\mathfrak{g}_i)$ for all $i \geq 1$. Note that one inclusion is trivial since $f$ and $h$ are homomorphisms of filtered Lie algebras. Now let $f(a) + h(x) \in \mathfrak{h}_i$. Since $g$ and $h$ are homomorphisms of filtered Lie algebras we find $g(f(a) + h(x)) = x \in \mathfrak{g}_i$ and $h(x) \in \mathfrak{h}_i$. As a consequence, $f(a) \in \mathfrak{h}_i$ and thus also $a \in \mathfrak{a}_i$. We conclude that $f(a) + h(x) \in f(\mathfrak{a}_i) + h(\mathfrak{g}_i)$ which proves the statement. □

## 8.2 Filtered groups

For a filtered group $G$, we denote by $\mathrm{Aut}_f(G)$ the set of all group automorphisms $\phi$ such that $\phi(G_i) = G_i$ and $\phi(g)g^{-1} \in G_{i+1}$ for all $i \geq 1$ and $g \in G_i$.

**Lemma 8.2.1.** *Let $G$ be a filtered group. Then $\mathrm{Aut}_f(G)$ is a subgroup of $\mathrm{Aut}(G)$. Moreover, it is a filtered group for the filtration*

$$\mathrm{Aut}_f(G)_i = \{\phi \in \mathrm{Aut}_f(G) \mid \phi(g)g^{-1} \in G_{i+j} \text{ for all } j \geq 1 \text{ and } g \in G_j\}.$$

*Proof.* Let $i, j \geq 1$, $\phi, \psi \in \mathrm{Aut}_f(G)_i$ and $g \in G_j$. Then

$$\phi(\psi(g))g^{-1} = \left(\phi(\psi(g))\psi(g)^{-1}\right)\psi(g)g^{-1} \in G_{i+j},$$

and

$$\phi^{-1}(g)g^{-1} = (\phi(\phi^{-1}(g))\phi^{-1}(g)^{-1})^{-1} \in G_{i+j},$$

which shows that $\mathrm{Aut}_f(G)_i$ is a subgroup of $\mathrm{Aut}(G)$.

It remains to prove that $[\mathrm{Aut}_f(G)_i, \mathrm{Aut}_f(G)_j]$ is contained in $\mathrm{Aut}_f(G)_{i+j}$. Consider the semidirect product $G \rtimes \mathrm{Aut}_f(G)$. We identify $G$ and $\mathrm{Aut}_f(G)$ with the subgroups $G \times \{1\}$ and $\{1\} \times \mathrm{Aut}_f(G)$. For $g \in G$ and $\phi \in \mathrm{Aut}_f(G)$ we find that the commutator of $(1, \phi)$ and $(g, 1)$ is given by

$$[(1, f), (g, 1)] = (1, f)(g, 1)(1, f)^{-1}(1, g)^{-1} = (f(g)g^{-1}, 1). \tag{8.1}$$

The filtration on $\mathrm{Aut}_f(G)$ is therefore defined in such a way that

$$[\mathrm{Aut}_f(G)_i, G_j] \subseteq G_{i+j},$$

so in particular the subgroups $G_i$ are normal in $G \rtimes \mathrm{Aut}_f(G)$. For any $k \geq 1$,

$$[\mathrm{Aut}_f(G)_i, [\mathrm{Aut}_f(G)_j, G_k]] \subseteq [\mathrm{Aut}_f(G)_i, G_{j+k}] \subseteq G_{i+j+k},$$

so the three subgroups lemma implies that

$$[G_k, [\mathrm{Aut}_f(G)_i, \mathrm{Aut}_f(G)_j]] \subseteq G_{i+j+k},$$

and thus we conclude that $[\mathrm{Aut}_f(G)_i, \mathrm{Aut}_f(G)_j]$ is indeed contained in $\mathrm{Aut}_f(G)_{i+j}$. □

**Example 8.2.2.** Let $g$ be an element of a filtered group $G$. Then conjugation by $g$ is contained in $\mathrm{Aut}_f(G)$ since $ghg^{-1}h^{-1} \in G_{i+1}$ for all $i \geq 1$ and $h \in G_i$. More precisely, if $g \in G_i$ then we find that the corresponding inner automorphism is contained in $\mathrm{Aut}_f(G)_i$.

**Lemma 8.2.3.** *Let $A, G$ be filtered groups and $\lambda : G \to \mathrm{Aut}_f(A)$ a homomorphism of filtered groups. Then the semidirect product of groups $A \rtimes_\lambda G$ is a filtered group for the filtration*

$$(A \rtimes_\lambda G)_i = A_i \rtimes_\lambda G_i.$$

*Proof.* For all $i, j \geq 1$ we have

$$[A_i \rtimes_\lambda G_i, A_j \rtimes_\lambda G_j] = [A_i, A_j][A_i, G_j][A_j, G_i][G_i, G_j],$$

where we identify $A$ and $G$ with the corresponding subgroup of $A \rtimes_\lambda G$. Clearly $[A_i, A_j] \subseteq A_{i+j}$ and $[G_i, G_j] \subseteq G_{i+j}$. Since $\lambda$ is a homomorphism of filtered groups, it follows from (8.1) that also $[A_i, G_j] \subseteq A_{i+j}$ and $[A_j, G_i] \subseteq A_{i+j}$. This concludes the proof. □

**Definition 8.2.4.** Let $f : A \to H$, $g : H \to G$ and $h : G \to H$ be homomorphisms of filtered groups. Then

$$1 \longrightarrow A \xrightarrow{f} H \underset{h}{\overset{g}{\rightleftarrows}} G \longrightarrow 1$$

is a *split exact sequence of filtered groups* if

1. the image of $f$ is precisely the kernel of $g$,
2. the composition $gh$ is the identity map on $G$,
3. $f$ induces an isomorphism of filtered groups $A \cong f(A)$.

The following lemma is straightforward to verify.

**Lemma 8.2.5.** *Let $G, A$ be filtered groups and let $\lambda : G \to \mathrm{Aut}_f(A)$ be a homomorphism of filtered groups. Then*

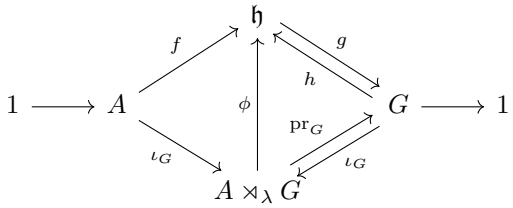
$$1 \longrightarrow A \xrightarrow{\iota_A} A \rtimes_\lambda G \underset{\iota_G}{\overset{\mathrm{pr}_G}{\rightleftarrows}} G \longrightarrow 1$$

*where $\iota_A, \iota_G$ are the inclusion maps and $\mathrm{pr}_G$ is the projection map, is a split exact sequence of filtered groups.*

**Lemma 8.2.6.** *Let*

$$1 \longrightarrow A \xrightarrow{f} H \underset{h}{\overset{g}{\rightleftarrows}} G \longrightarrow 1$$

*be a split exact sequence of filtered groups. Then there exists a homomorphism of filtered groups $\lambda : G \to \mathrm{Aut}_f(A)$ and an isomorphism of filtered groups $\phi : A \rtimes_\lambda G \to H$ such that*




*commutes.*

*Proof.* The proof is completely analogous to the proof of Lemma 8.1.7. □

## 8.3 Relating semidirect sums and products

For $\mathfrak{g}$ a filtered Lie algebra we denote by $\mathrm{Aut}_f(\mathfrak{g})$ the set of Lie algebra automorphisms $\phi$ of $\mathfrak{g}$ such that $\phi(x) - x \in \mathfrak{g}_{i+1}$ for all $i \geq 1$ and $x \in \mathfrak{g}_i$.

**Lemma 8.3.1.** *Let $\mathfrak{g}$ be a filtered Lie algebra. Then $\mathrm{Aut}_f(\mathfrak{g})$ is a subgroup of $\mathrm{Aut}(\mathfrak{g})$. Moreover, it is a filtered group for the filtration*

$$\mathrm{Aut}_f(\mathfrak{g})_i = \{\phi \in \mathrm{Aut}(\mathfrak{g}) \mid \phi(x) - x \in \mathfrak{g}_{i+j} \text{ for all } j \geq 1 \text{ and } x \in \mathfrak{g}_j\}.$$

*Proof.* Consider the additive group $(\mathfrak{g}, +)$ together with the filtration on $\mathfrak{g}$. Then $\mathrm{Aut}_f(\mathfrak{g})$ is a subgroup of $\mathrm{Aut}_f(\mathfrak{g}, +)$ as defined in Section 8.2. Since $\mathrm{Aut}_f(\mathfrak{g})_i = \mathrm{Aut}_f(\mathfrak{g}) \cap \mathrm{Aut}_f(\mathfrak{g}, +)_i$, the statement follows. □

**Lemma 8.3.2.** *Let $\mathfrak{g}$ be a Lazard Lie algebra. Then $\mathrm{Aut}_f(\mathfrak{g}) = \mathrm{Aut}_f(\mathbf{Laz}(\mathfrak{g}))$ as filtered groups.*

*Proof.* We know by Theorem 1.4.27 that automorphisms of $\mathfrak{g}$ and $\mathbf{Laz}(\mathfrak{g})$, seen as filtered structures, coincide. It remains to show that $\mathrm{Aut}_f(\mathfrak{g})_i = \mathrm{Aut}_f(\mathbf{Laz}(\mathfrak{g}))_i$ for all $i \geq 1$. Let $x, y \in \mathfrak{g}$ such that $x + y \in \mathfrak{g}_i \setminus \mathfrak{g}_{i+1}$, then

$$[x, y] + \mathfrak{g}_{i+1} = [x, y] - [x + y, y] + \mathfrak{g}_{i+1} = \mathfrak{g}_{i+1},$$

hence $x + y + \mathfrak{g}_{i+1} = \mathrm{BCH}(x, y) + \mathfrak{g}_{i+1}$ and thus $\mathrm{BCH}(x, y) \in \mathfrak{g}_i \setminus \mathfrak{g}_{i+1}$. We find that $x + y \in \mathfrak{g}_i$ if and only if $\mathrm{BCH}(x, y) \in \mathfrak{g}_i$. In particular, for $\phi \in \mathrm{Aut}_f(\mathfrak{g})$ and $x \in \mathfrak{g}$ we conclude that $\mathrm{BCH}(\phi(x), -x) \in \mathfrak{g}_i$ if and only if $\phi(x) - x \in \mathfrak{g}_i$, from which the claim follows. □

**Lemma 8.3.3.** *Let $\mathfrak{g}$ be a Lazard Lie algebra. Then also $\mathfrak{der}_f(\mathfrak{g})$ is Lazard.*

*Proof.* By Lemma 1.4.28, it is sufficient to prove that $\mathfrak{der}_f(\mathfrak{g})_i$ can be given the structure of a $\mathbb{Q}_{\mathcal{P}_i}$-module, with $\mathcal{P}_i$ the set of all prime numbers at most $i$. Let $\delta \in \mathfrak{der}_f(\mathfrak{g})_i$. Since then in particular, $\delta(\mathfrak{g}) \subseteq \mathfrak{g}_{i+1}$ we can define for all $r \in \mathbb{Q}_{\mathcal{P}_i}$,

$$r\delta : \mathfrak{g} \to \mathfrak{g} : x \mapsto r\delta(x),$$

which is also contained in $\mathfrak{der}_f(\mathfrak{g})_i$. This gives $\mathfrak{der}_f(\mathfrak{g})_i$ the structure of a $\mathbb{Q}_{\mathcal{P}_i}$-module. □

It is well-known that the exponential and logarithmic maps induce a bijection between strict upper triangular $n \times n$-matrices and upper unitriangular $n \times n$-matrices over $\mathbb{Q}$. The same holds over fields of characteristic $p > 0$ as long as $n < p$. The following lemma should be seen as a generalized version of this. Note that this solves the problem that was discussed in the beginning of the chapter about there generally not being a relation between $\mathrm{Aut}(\mathfrak{g})$ and $\mathfrak{der}(\mathfrak{g})$ for an arbitrary (Lazard) Lie algebra.

**Theorem 8.3.4.** *Let $\mathfrak{g}$ be a Lazard Lie ring. Then*

$$\exp : \mathbf{Laz}(\mathfrak{der}_f(\mathfrak{g})) \to \mathrm{Aut}_f(\mathfrak{g})$$

*is an isomorphism of filtered groups. In particular, $\mathrm{Aut}_f(\mathfrak{g})$ is Lazard.*

*Proof.* Since $\mathrm{End}_f(\mathfrak{g})_i$ is an ideal of $\mathrm{End}_f(\mathfrak{g})$ for all $i \geq 1$, we obtain the equality

$$\exp(\mathrm{End}_f(\mathfrak{g})_i) = 1 + \mathrm{End}_f(\mathfrak{g})_i,$$

see also Example 1.4.8 and Lemma 1.4.30. It therefore remains to prove that $\exp(\mathfrak{der}_f(\mathfrak{g})) = \mathrm{Aut}_f(\mathfrak{g})$. The statement then follows in combination with Proposition 1.4.24.

Let $\delta \in \mathfrak{der}_f(\mathfrak{g})$ and $x, y \in \mathfrak{g}$. We claim that

$$\delta^n([x, y]) = \sum_{m=0}^{n} \binom{n}{m} [\delta^m(x), \delta^{n-m}(y)], \tag{8.2}$$

for $n \geq 0$. Indeed, for $n = 0$ this is trivial, and by induction

$$\begin{aligned}
\delta^{n+1}([x, y]) &= \delta\left(\sum_{m=0}^{n} \binom{n}{m} [\delta^m(x), \delta^{n-m}(y)]\right) \\
&= \sum_{m=0}^{n} \binom{n}{m} ([\delta^{m+1}(x), \delta^{n-m}(y)] + [\delta^m(x), \delta^{n+1-m}(y)]) \\
&= [\delta^{n+1}, y] + [x, \delta^{n+1}(y)] + \sum_{m=0}^{n-1} \left(\binom{n}{m-1} + \binom{n}{m}\right) [\delta^m(x), \delta^{n+1-m}(y)] \\
&= \sum_{m=0}^{n+1} \binom{n+1}{m} [\delta^m(x), \delta^{n+1-m}(y)].
\end{aligned}$$

We find

$$\begin{aligned}\exp(\delta)([x,y]) &= \sum_{n=0}^{\infty}\sum_{m=0}^{n}\frac{1}{n!}\binom{n}{m}[\delta^m(x),\delta^{n-m}(y)] = \sum_{l=0}^{\infty}\sum_{m=0}^{\infty}\frac{1}{l!m!}[\delta^m(x),\delta^l(y)]\\ &= [\exp(\delta)(x),\exp(\delta)(y)],\end{aligned}$$

which proves that $\exp(\delta)\in \mathrm{Aut}_f(\mathfrak{g})$ and thus the inclusion $\exp(\mathfrak{der}_f(\mathfrak{g}))\subseteq \mathrm{Aut}_f(\mathfrak{g})$ follows.

Conversely, let $\phi\in \mathrm{Aut}_f(\mathfrak{g})$ and set $\delta=\log(\phi)$, which we know is contained in $\mathrm{End}_f(\mathfrak{g})_1$. We will prove by induction on $k$ that

$$\delta([x,y])+\mathfrak{g}_{i+j+k} = [\delta(x),y]+[x,\delta(y)]+\mathfrak{g}_{i+j+k}, \tag{8.3}$$

for all $i,j,k\geq 1$, $x\in\mathfrak{g}_i$, $y\in\mathfrak{g}_j$. Taking $k$ large enough then yields $\delta\in\mathfrak{der}_f(\mathfrak{g})$. For $k=1$, the statement is trivial since $\delta\in\mathrm{End}_f(\mathfrak{g})_1$. Assume that (8.3) holds for some $k\geq 1$. Then

$$\delta([\delta^r(x),\delta^s(y)])+\mathfrak{g}_{i+j+k+1} = [\delta^{r+1}(x),\delta^s(y)]+[\delta^r(x),\delta^{s+1}(y)]+\mathfrak{g}_{i+j+k+1}, \tag{8.4}$$

for $r,s\geq 0$ such that $r+s\geq 1$, since either $\delta^r(x)\in\mathfrak{g}_{i+1}$ or $\delta^s(y)\in\mathfrak{g}_{j+1}$.

We now prove by induction on $n$ that

$$\delta^n([x,y])+\mathfrak{g}_{i+j+k+1} = \sum_{m=0}^{n}\binom{n}{m}[\delta^j(x),\delta^{n-m}(y)]+\mathfrak{g}_{i+j+k+1}, \tag{8.5}$$

for all $i,j\geq 1$, $n\geq 2$, $x\in\mathfrak{g}_i$ and $y\in\mathfrak{g}_j$. Applying $\delta$ on both sides of (8.3) yields

$$\delta^2([x,y])+\mathfrak{g}_{i+j+k+1} = \delta([\delta(x),y])+\delta([x,\delta(y)])+\mathfrak{g}_{i+j+k+1},$$

so using (8.4) we indeed find that (8.5) holds for $n=2$. Next, assume that (8.5) holds for some $n\geq 2$, then similar to the proof of (8.2) we find

$$\begin{aligned}\delta^{n+1}([x,y]) &\in \delta\left(\sum_{m=0}^{n}\binom{n}{m}[\delta^m(x),\delta^{n-m}(y)]+\mathfrak{g}_{i+j+k+1}\right)\\ &\subseteq \sum_{m=0}^{n}\binom{n}{m}([\delta^{m+1}(x),\delta^{n-m}(y)]+[\delta^m(x),\delta^{n+1-m}(y)])+\mathfrak{g}_{i+j+k+1}\\ &= \sum_{m=0}^{n+1}\binom{n+1}{m}[\delta^m(x),\delta^{n+1-m}(y)]+\mathfrak{g}_{i+j+k+1},\end{aligned}$$

where the inclusion follows from (8.4). This concludes the proof of (8.5) for all $n\geq 2$, which we can now use to obtain

$$\begin{aligned}\phi([x,y])+\mathfrak{g}_{i+j+k+1} &= [x,y]+\delta([x,y])+\sum_{n=2}^{\infty}\sum_{m=0}^{n}\frac{1}{n!}\binom{n}{m}[\delta^m(x),\delta^{n-m}(y)]+\mathfrak{g}_{i+j+k+1}\\ &= [x,y]+\delta([x,y])+\sum_{n=2}^{\infty}\sum_{m=0}^{\infty}\frac{1}{n!m!}[\delta^m(x),\delta^n(y)]+\mathfrak{g}_{i+j+k+1},\end{aligned}$$

while we also know that

$$[\phi(x), \phi(y)] = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \frac{1}{n!m!} [\delta^m(x), \delta^n(y)].$$

Comparing both, we find

$$\delta([x, y]) + \mathfrak{g}_{i+j+k+1} = [\delta(x), y] + [x, \delta(y)] + \mathfrak{g}_{i+j+k+1}.$$

This proves that (8.3) holds for $k + 1$ and thus concludes the proof. □

**Proposition 8.3.5.** *Let $\mathfrak{a}, \mathfrak{g}$ be Lazard Lie rings and let $\delta : \mathfrak{g} \to \mathfrak{Der}_f(\mathfrak{a})$ be a homomorphism of filtered Lie algebras. Then there is a unique filtered group isomorphism*

$$\gamma : \mathbf{Laz}(\mathfrak{a} \oplus_\delta \mathfrak{g}) \to \mathbf{Laz}(\mathfrak{a}) \rtimes_\lambda \mathbf{Laz}(\mathfrak{g})$$

*such that $\gamma(a, 0) = (a, 0)$ and $\gamma(0, x) = (0, x)$, where*

$$\lambda : \mathbf{Laz}(\mathfrak{g}) \to \mathrm{Aut}_f(\mathbf{Laz}(\mathfrak{a})) : x \mapsto \lambda_x,$$

*with $\lambda_x = \exp(\delta_x)$.*

*Proof.* From Lemma 8.1.6 we know that

$$0 \longrightarrow \mathfrak{a} \xrightarrow{\iota_\mathfrak{a}} \mathfrak{a} \oplus_\delta \mathfrak{g} \underset{\iota_\mathfrak{g}}{\overset{\mathrm{pr}_\mathfrak{g}}{\rightleftarrows}} \mathfrak{g} \longrightarrow 0$$

is a split exact sequence of filtered Lie algebras. After application of the functor $\mathbf{Laz}$, we obtain a split exact sequence of filtered groups

$$1 \longrightarrow \mathbf{Laz}(\mathfrak{a}) \xrightarrow{\iota_\mathfrak{a}} \mathbf{Laz}(\mathfrak{a} \oplus_\delta \mathfrak{g}) \underset{\iota_\mathfrak{g}}{\overset{\mathrm{pr}_\mathfrak{g}}{\rightleftarrows}} \mathbf{Laz}(\mathfrak{g}) \longrightarrow 1$$

which by Lemma 8.2.6 means there exists an isomorphism $\gamma : \mathbf{Laz}(\mathfrak{a} \oplus_\delta \mathfrak{g}) \to \mathbf{Laz}(\mathfrak{a}) \rtimes_\lambda \mathbf{Laz}(\mathfrak{g})$ with $\gamma(a, 0) = (a, 0)$ and $\gamma(0, x) = (0, x)$ for all $a \in \mathfrak{a}$, $x \in \mathfrak{g}$. The action $\lambda$ is indeed the one given in the statement because of Lemma 1.4.31. □

We continue with the same setting as Proposition 8.3.5. Since $\mathfrak{a} \times \{0\}$ is a normal subgroup of both $\mathbf{Laz}(\mathfrak{a} \oplus_\delta \mathfrak{g})$ and $\mathbf{Laz}(\mathfrak{a}) \rtimes_\lambda \mathbf{Laz}(\mathfrak{g})$, and $\gamma(\mathfrak{a} \times \{0\}) = \mathfrak{a} \times \{0\}$, we find that $\gamma$ does not affect the second component. Define $V : \mathfrak{a} \times \mathfrak{g} \to \mathfrak{a}$ as

$$\gamma(a, x) = (V(a, x), x).$$

Then in $\mathbf{Laz}(\mathfrak{a}) \rtimes_\lambda \mathbf{Laz}(\mathfrak{g})$ we find

$$(V(a, x), 0) = (V(a, x), x)(0, x)^{-1} = \gamma(a, x)\gamma(0, x)^{-1} = \gamma(\mathrm{BCH}((a, x), (0, -x))).$$

Since

$$\begin{aligned}
[(a,x),(0,-x)] &= (-\delta_{-x}(a),0)\\
&= (\delta_x(a),0),\\
[(a,x),[(a,x),(0,-x)]] &= [(a,x),(\delta_x(a),0)]\\
&= ([a,\delta_x(a)]+\delta_x^2(a),0),\\
[(0,-x),[(0,-x),(a,x)]] &= [(0,-x),(-\delta_x(a),0)]\\
&= (\delta_x^2(a),0),\\
[(0,-x),[(a,x),[(a,x),(0,-x)]]] &= [(0,-x),([a,\delta_x(a)]+\delta_x^2(a),0)]\\
&= (-\delta_x([a,\delta_x(a)])-\delta_x^3(a),0)\\
&= (-[a,\delta_x^2(a)]-\delta_x^3(a),0),
\end{aligned}$$

we can use (1.13) to find

$$V(a,x) = a+\frac{1}{2}\delta_x(a)+\frac{1}{6}\delta_x^2(a)+\frac{1}{12}[a,\delta_x(a)]+\frac{1}{24}([a,\delta_x^2(a)]+\delta_x^3(a))+\dots \tag{8.6}$$

where further terms are of order at least 5.

Similarly, we define $U:\mathfrak{a}\times\mathfrak{g}\to\mathfrak{a}$ as

$$\gamma^{-1}(a,x) = (U(a,x),x),$$

and we find

$$(U(a,x),0) = (U(a,x),x)+(0,-x) = P((a,x),(0,-x))),$$

with $P$ as in (1.14), evaluated in the group $\mathbf{Laz}(\mathfrak{a})\rtimes_\lambda \mathbf{Laz}(\mathfrak{g})$. We find the following group theoretic commutators in $\mathbf{Laz}(\mathfrak{a})\rtimes_\lambda \mathbf{Laz}(\mathfrak{g})$, where for readability we use juxtaposition for multiplication in the groups $\mathbf{Laz}(\mathfrak{a})$, $\mathbf{Laz}(\mathfrak{g})$ and $\mathbf{Laz}(\mathfrak{a})\rtimes_\lambda \mathbf{Laz}(\mathfrak{g})$:

$$\begin{aligned}
[(a,x),(0,-x)] &= (a,x)(0,-x)(a,x)^{-1}(0,-x)^{-1}\\
&= (a,x)(0,-x)(\lambda_x^{-1}(a^{-1}),-x)(0,x)\\
&= (a\lambda_x^{-1}(a^{-1}),0),\\
[(a,x),[(a,x),(0,-x)]] &= [(a,x),(a\lambda_x^{-1}(a^{-1}),0)]\\
&= (a\lambda_x(a\lambda_x^{-1}(a^{-1}))a^{-1}\lambda_x^{-1}(a)a^{-1},0)\\
&= (a\lambda_x(a)a^{-2}\lambda_x^{-1}(a)a^{-1},0),\\
[(a,x),[(a,x),[(a,x),(0,-x)]]] &= [(a,x),(a\lambda_x(a)a^{-2}\lambda_x^{-1}(a)a^{-1},0)]\\
&= (a\lambda_x(a\lambda_x(a)a^{-2}\lambda_x^{-1}(a)a^{-1})a^{-1}a\lambda_x^{-1}(a^{-1})a^2\lambda_x(a^{-1})a^{-1},0)\\
&= (a\lambda_x(a)\lambda_x^2(a)\lambda_x(a^{-2})a\lambda_x(a^{-1})\lambda_x^{-1}(a^{-1})a^2\lambda_x(a^{-1})a^{-1},0),\\
[(0,-x),[(a,x),(0,-x)]] &= [(0,-x),(a\lambda_x^{-1}(a^{-1}),0)]\\
&= (\lambda_x^{-1}(a\lambda_x^{-1}(a^{-1}))\lambda_x^{-1}(a)a^{-1},0)\\
&= (\lambda_x^{-1}(a)\lambda_x^{-2}(a^{-1})\lambda_x^{-1}(a)a^{-1},0),
\end{aligned}$$

and

$$\begin{aligned}[(0,-x),[(0,-x),[(a,x),&(0,-x)]]] = [(0,-x),(\lambda_x^{-1}(a)\lambda_x^{-2}(a^{-1})\lambda_x^{-1}(a)a^{-1},0)]\\ &= (\lambda_x^{-1}(\lambda_x^{-1}(a)\lambda_x^{-2}(a^{-1})\lambda_x^{-1}(a)a^{-1})a\lambda_x^{-1}(a^{-1})\lambda_x^{-2}(a)\lambda_x^{-1}(a^{-1}),0)\\ &= (\lambda_x^{-2}(a)\lambda_x^{-3}(a^{-1})\lambda_x^{-2}(a)\lambda_x^{-1}(a^{-1})a\lambda_x^{-1}(a^{-1})\lambda_x^{-2}(a)\lambda_x^{-1}(a^{-1}),0).\end{aligned}$$

Explicitly, the terms of order less than 5 are given by

$$\begin{aligned}U(a,\lambda_x) = a(a\lambda_x^{-1}(a^{-1}))^{-\frac{1}{2}}&(a\lambda_x(a)a^{-2}\lambda_x^{-1}(a)a^{-1})^{\frac{1}{12}}\\ &(a\lambda_x(a)\lambda_x^2(a)\lambda_x(a^{-2})a\lambda_x(a^{-1})\lambda_x^{-1}(a^{-1})a^2\lambda_x(a^{-1})a^{-1})^{-\frac{1}{24}}\\ &(\lambda_x^{-2}(a)\lambda_x^{-3}(a^{-1})\lambda_x^{-2}(a)\lambda_x^{-1}(a^{-1})a\lambda_x^{-1}(a^{-1})\lambda_x^{-2}(a)\lambda_x^{-1}(a^{-1}))^{\frac{1}{24}}\cdots\end{aligned} \tag{8.7}$$

In the case that $\mathfrak{a}$ is abelian, we have more explicit formulae for $V$ and $U$.

**Lemma 8.3.6.** *Let $\mathfrak{a},\mathfrak{g}$ be Lazard Lie algebras and let $\delta:\mathfrak{g}\to\mathfrak{Der}_f(\mathfrak{a})$ be a homomorphism of filtered Lie algebras. If $\mathfrak{a}$ is a trivial Lie algebra, then $V$ and $U$ simplify to*

$$V(a,x) = \sum_{k=1}^{\infty}\frac{1}{k!}\delta_x^{k-1}(a), \tag{8.8}$$

$$U(a,x) = \sum_{k=1}^{\infty}\frac{1}{k}(\mathrm{id}-\lambda_x)^{k-1}(a). \tag{8.9}$$

*Proof.* Similar to Example 1.3.20 we consider $A = R\oplus\mathfrak{a}$ as a filtered algebra, where

$$(r,a)(s,b) := (rs, rb+sa),$$

for $r,s\in R$ and $a,b\in\mathfrak{a}$, and filtration $A_0 = A$ and $A_i = \{0\}\oplus\mathfrak{a}_i$ for $i\geq 1$. Then

$$\rho:\mathfrak{a}\oplus_\delta\mathfrak{g}\to\mathrm{End}_f(A,+):(a,x)\mapsto\rho_{(a,x)},$$

with

$$\rho_{(a,x)}(r,b) = (0, ra+\delta_x(b)),$$

is a homomorphism of filtered Lie algebras. The proof of this is precisely the same as given in Example 1.3.20. Since $(V(a,x),0) = \mathrm{BCH}((a,x),(0,-x))$ in $\mathfrak{a}\oplus_\delta\mathfrak{g}$, it follows from Proposition 1.4.24 that

$$\rho_{(V(a,x),0)} = \log(\exp(\rho_{(a,x)})\exp(\rho_{(0,-x)})),$$

and since

$$\exp(\rho_{(V(a,x),0)})(1,0) = (1,0)+(0,V(a,x))+0+0+\ldots = (1,V(a,x)),$$

we find

$$(1,V(a,x)) = \exp(\rho_{(a,x)})\exp(\rho_{(0,-x)})(1,0).$$

Clearly $\exp(\rho_{(0,-x)})(1,0) = (1,0)$ and thus

$$(1,V(a,x)) = \exp(\rho_{(a,x)})(1,0) = \left(1,\sum_{k=1}^{\infty}\frac{1}{k!}\delta_x^{k-1}(a)\right),$$

from which we obtain (8.8).

Similarly, since we know that

$$(U(a,x),0) = P((a,x),(0,-x)) = P((a,0)(0,x),(0,-x)),$$

where $P$ is as in (1.16) considered in the group in $\mathbf{Laz}(\mathfrak{a}) \rtimes_\lambda \mathbf{Laz}(\mathfrak{g})$, we can apply $\gamma^{-1}$ in order to obtain the equality

$$(U(a,x),0) = \mathrm{BCH}((a,0),(0,x)) + (0,-x)),$$

in $\mathfrak{a} \oplus_\delta \mathfrak{g}$. Applying $\rho$ to this equation yields

$$\rho_{(U(a,x),0)} = \log(\exp(\rho_{(a,0)})\exp(\rho_{(0,x)})) + \rho_{(0,-x)},$$

in the Lazard algebra $\mathrm{End}_f(A,+)$ thus

$$\begin{aligned}(0,U(a,x)) &= \log(\exp(\rho_{(a,0)})\exp(\rho_{(0,x)}))(1,0) + \rho_{(0,-x)}(1,0)\\ &= \log(\exp(\rho_{(a,0)})\exp(\rho_{(0,x)}))(1,0).\end{aligned} \tag{8.10}$$

Since for all $n \in \mathbb{Z}$ and $b \in \mathfrak{a}$ we find $\exp(\rho_{(0,x)})(n,b) = (n,\lambda_x(b))$ and $\exp(\rho_{(a,0)})(n,b) = (1,na)$, we obtain for $k > 0$ that

$$\begin{aligned}(\exp(\rho_{(a,0)})\exp(\rho_{(0,x)}) - \mathrm{id})^k(1,0) &= (\exp(\rho_{(a,0)})\exp(\rho_{(0,x)}) - \mathrm{id})^{k-1}(0,a)\\ &= (0,(\lambda_x - \mathrm{id})^{k-1}(a)).\end{aligned}$$

Combining this with (8.10), we find

$$\begin{aligned}(0,U(a,x)) &= \log(\exp(\rho_{(a,0)})\exp(\rho_{(0,x)}))(1,0)\\ &= \sum_{k=1}\frac{1}{k}(-1)^{k+1}(\exp(\rho_{(a,0)})\exp(\rho_{(0,x)}) - \mathrm{id})^k(1,0)\\ &= \left(0,\sum_{k=1}\frac{1}{k}(-1)^{k+1}(\lambda_x - \mathrm{id}_{\mathfrak{a}})^{k-1}(a)\right)\\ &= \left(0,\sum_{k=1}\frac{1}{k}(\mathrm{id}_{\mathfrak{a}} - \lambda_x)^{k-1}(a)\right),\end{aligned}$$

from which we obtain (8.9). □

We now consider a particular case of the previous setting. Let $\mathfrak{a}$ be a filtered Lie algebra. Define

$$\mathfrak{aff}_f(\mathfrak{a}) := \mathfrak{a} \oplus_\delta \mathfrak{der}_f(\mathfrak{a}),$$

where $\delta$ is the identity map on $\mathfrak{der}_f(\mathfrak{g})$. Similarly, for $A$ a filtered group we define $\mathrm{Hol}_f(A)$ as the semidirect product

$$\mathrm{Hol}_f(A) := A \rtimes_\lambda \mathrm{Aut}_f(A),$$

with $\lambda$ the identity map on $\mathrm{Aut}_f(A)$.

Let us, from now on, assume that $\mathfrak{a}$ is a Lazard Lie algebra. By Proposition 8.3.5, we have a filtered group isomorphism

$$\gamma : \mathbf{Laz}(\mathfrak{aff}_f(\mathfrak{a})) \to \mathbf{Laz}(\mathfrak{a}) \rtimes \mathbf{Laz}(\mathfrak{der}_f(\mathfrak{a})).$$

After identifying $\mathbf{Laz}(\mathfrak{der}_f(\mathfrak{a}))$ with $\mathrm{Aut}_f(\mathfrak{a})$ as in Theorem 8.3.4 and $\mathrm{Aut}_f(\mathfrak{a})$ with $\mathrm{Aut}_f(\mathbf{Laz}(\mathfrak{a}))$ as in Lemma 8.3.2 we find an isomorphism

$$\gamma : \mathbf{Laz}(\mathfrak{aff}_f(\mathfrak{a})) \to \mathrm{Hol}_f(\mathbf{Laz}(\mathfrak{a})),$$

such that $\gamma(a,0) = (a,0)$ and $\gamma(0,\delta) = (0,\exp(\delta))$ for all $a \in \mathfrak{a}$ and $\delta \in \mathfrak{der}_f(\mathfrak{a})$. It then follows from Theorem 1.4.27 and Proposition 8.3.5 that $\gamma$ yields a bijective correspondence between Lazard Lie subrings of $\mathfrak{aff}_f(\mathfrak{a})$ and Lazard subgroups of $\mathrm{Hol}_f(\mathbf{Laz}(\mathfrak{a}))$.

**Proposition 8.3.7.** *Let $\mathfrak{a}$ be a Lazard Lie algebra and let $\mathfrak{g}$ be a Lazard Lie subalgebra of $\mathfrak{aff}_f(\mathfrak{a})$. Then $\mathfrak{g}$ is $t$-injective if and only if the stabilizer of $0$ under the action of $\gamma(\mathfrak{g})$ on $\mathbf{Laz}(\mathfrak{a})$ is trivial.*

*Proof.* Let $\mathfrak{g}$ be as in the statement and assume that $\mathfrak{g}$ is $t$-injective. Any element of $\gamma(\mathfrak{g})$ that fixes $0$ is of the form $(0,\lambda)$, hence $\gamma^{-1}(0,\lambda) = (0,\log(\lambda))$. Since $\mathfrak{g}$ is $t$-injective this implies $\log(\lambda) = 0$ and thus we find that $\lambda = \mathrm{id}_{\mathfrak{a}}$.

Conversely, assume that the stabilizer of $0$ under the action of $\gamma(\mathfrak{g})$ is trivial and let $(a,\delta),(a,\delta') \in \mathfrak{g}$. Then $(0,\delta-\delta') \in \mathfrak{g}$ hence $\gamma(0,\delta-\delta') = (0,\exp(\delta-\delta')) \in \gamma(\mathfrak{g})$. Since this element clearly fixes $0$, we conclude that $\exp(\delta-\delta') = \mathrm{id}_{\mathfrak{a}}$ and thus $\delta = \delta'$. □

**Proposition 8.3.8.** *Let $\mathfrak{a}$ be a Lazard Lie algebra and let $\mathfrak{g}$ be a Lazard Lie subalgebra of $\mathfrak{aff}_f(\mathfrak{a})$. Then $\mathfrak{g}$ is $t$-surjective if and only if $\gamma(\mathfrak{g})$ is transitive.*

*Proof.* Assume that $\mathfrak{g}$ is $t$-surjective. Recall that $V$ is by definition the composition of the projection

$$\mathrm{pr}_{\mathbf{Laz}(\mathfrak{a})} : \mathrm{Hol}_f(\mathbf{Laz}(\mathfrak{a})) \to \mathbf{Laz}(\mathfrak{a}),$$

with $\gamma$, hence it suffices to prove that $V(\mathfrak{g}) = \mathfrak{a}$. If this is not the case, there exists some $a \in \mathfrak{a}$ and $i \geq 1$ such that $V(\mathfrak{g}) \cap (a+\mathfrak{a}_i) \neq \varnothing$ but $V(\mathfrak{g}) \cap (a+\mathfrak{a}_{i+1}) = \varnothing$. Let $(b,\delta) \in \mathfrak{g}$ such that $V(b,\delta) \in a+\mathfrak{a}_i$ and set $c = a - V(b,\delta)$. Since $\mathfrak{g}$ is $t$-surjective, there exists some $\delta' \in \mathfrak{der}_f(\mathfrak{a})$ such that $(c,\delta') \in \mathfrak{g}$ . We find

$$\begin{aligned} c + \mathfrak{a}_{i+1} &= V(c,\delta') + \mathfrak{a}_{i+1} \\ &= \exp(\delta)(V(c,\delta')) + \mathfrak{a}_{i+1}. \end{aligned}$$

Also, since $\gamma$ is a group isomorphism between $\mathbf{Laz}(\mathfrak{aff}_f(\mathfrak{a}))$ and $\mathrm{Hol}_f(\mathbf{Laz}(\mathfrak{a}))$ we find

$$\begin{aligned} (V(\mathrm{BCH}((b,\delta),(c,\delta'))),\exp(\delta)\exp(\delta')) &= \gamma(\mathrm{BCH}((b,\delta),(c,\delta'))) \\ &= \gamma(b,\delta)\gamma(c,\delta') \\ &= (V(b,\delta),\exp(\delta))(V(c,\delta'),\exp(\delta')) \\ &= (\mathrm{BCH}(V(b,\delta),\exp(\delta)(V(c,\delta'))),\exp(\delta)\exp(\delta')). \end{aligned}$$

Putting these two equalities together, we obtain

$$\begin{aligned} V(\mathrm{BCH}((b,\delta),(c',\delta'))) + \mathfrak{a}_{i+1} &= \mathrm{BCH}(V(b,\delta),\exp(\delta)V(c',\delta')) + \mathfrak{a}_{i+1} \\ &= \mathrm{BCH}(V(b,\delta),c) + \mathfrak{a}_{i+1} \\ &= V(b,\delta) + c + \mathfrak{a}_{i+1} \\ &= a + \mathfrak{a}_{i+1}. \end{aligned}$$

We conclude that $V(\mathfrak{g}) \cap (a+\mathfrak{a}_{i+1})$ is non-empty, which contradicts the earlier assumption.

Conversely, assume that $V(\mathfrak{g}) = \mathfrak{a}$. If $\mathrm{pr}_{\mathfrak{a}}(\mathfrak{g}) \neq \mathfrak{a}$ then there exists some $a \in \mathfrak{a}$ and $i \geq 1$ such that $\mathrm{pr}_{\mathfrak{a}}(\mathfrak{g}) \cap (a + \mathfrak{a}_i) \neq \varnothing$ but $\mathrm{pr}_{\mathfrak{a}}(\mathfrak{g}) \cap (a + \mathfrak{a}_{i+1}) = \varnothing$. Choose $(b, \delta) \in \mathfrak{g}$ such that $b \in a + \mathfrak{a}_i$. By assumption there exists some $(b', \delta') \in \mathfrak{g}$ such that $V(b', \delta') = a - b$. If $j$ is such that $b' \in \mathfrak{a}_j \setminus \mathfrak{a}_{j+1}$, then

$$b = V(b', \delta') = b' + \frac{1}{2}\delta'(b') + \ldots \in b' + \mathfrak{a}_{j+1},$$

which implies that $j = i$. We find

$$\begin{aligned} a - b + \mathfrak{a}_{i+1} &= V(b', \delta') + \mathfrak{a}_{i+1} \\ &= b' + \mathfrak{a}_{i+1}, \end{aligned}$$

and thus

$$\mathrm{pr}_{\mathfrak{a}}((b, \delta) + (b', \delta')) + \mathfrak{a}_{i+1} = a + \mathfrak{a}_{i+1}.$$

This contradicts the choice of $a$ and $i$ and thus we obtain that $\mathrm{pr}_{\mathfrak{a}}(\mathfrak{g}) = \mathfrak{a}$. □

From Propositions 8.3.7 and 8.3.8 we now obtain the main result of this section.

**Theorem 8.3.9.** *Let $\mathfrak{a}$ be a Lazard Lie algebra and let $\mathfrak{g}$ be a Lazard Lie subalgebra of $\mathfrak{aff}_f(\mathfrak{a})$. Then $\mathfrak{g}$ is $t$-bijective if and only if $\gamma(\mathfrak{g})$ is regular.*

*Remark* 8.3.10. As discussed in Section 1.5.3, transitive subgroups of the holomorph of a finite group play an essential role in the theory of Hopf–Galois structures on separable field extensions. Let us shortly discuss a potential application for Proposition 8.3.8 in Hopf–Galois theory.

Let $A$ be a finite $p$-group for some prime $p$ and let $G$ be a Sylow $p$-subgroup of $\mathrm{Aut}(A)$. Since the semidirect product $A \rtimes G$ is still a $p$-group, its lower central series

$$\gamma^1(A \rtimes G) \supseteq \gamma^2(A \rtimes G) \supseteq \ldots$$

terminates at some point. In particular, $A$ has the structure of a filtered group for the filtration $A_i = A \cap \gamma^i(A \rtimes G)$ for $i \geq 1$. Alternatively this filtration can be obtained by setting $A_1 = A$ and defining $A_{i+1}$ as the subgroup of $A$ generated by

$$\{[a, b], g(a)a^{-1} \mid a \in A_i, b \in A, g \in G\}.$$

This choice of filtration guarantees that $G$ is a subgroup of $\mathrm{Aut}_f(A)$. Since $\mathrm{Hol}_f(A)$ has a finite filtration, it is, in particular, nilpotent. Therefore, any element $g \in \{1\} \rtimes \mathrm{Aut}_f(A)$ of prime order $q \neq p$ centralizes the $p$-subgroup $A \rtimes \{1\}$, which implies that $g$ is the identity automorphism. We conclude that $\mathrm{Aut}_f(A)$ is a $p$-group and thus $\mathrm{Aut}_f(A) = G$.

If $A_p = \{1\}$, which is for example always the case if $|A| < p^p$, then $A$ and $\mathrm{Hol}_f(A)$ are Lazard. In that case, Proposition 8.3.8 states that transitive subgroups of $\mathrm{Hol}_f(A)$ are in a one-to-one correspondence with $t$-surjective Lie subrings of $\mathfrak{aff}_f(\mathbf{Laz}^{-1}(A))$. This potentially opens the door to structural or classification results on Hopf–Galois structures on separable extensions of degree $p^n$ whose type is a $p$-group, where $n < p$.

## 8.4 The correspondence

Recall the correspondence described in Proposition 1.3.22 between post-Lie algebra structures on a Lie algebra $\mathfrak{a}$ and $t$-bijective Lie subalgebras of $\mathfrak{aff}(\mathfrak{a})$. We now define filtered post-Lie algebras in such a way that this correspondence restricts to one between filtered post-Lie algebras and $t$-bijective Lie subalgebras of $\mathfrak{aff}_f(\mathfrak{a})$.

**Definition 8.4.1.** A *filtration* on a post-Lie algebra $(\mathfrak{a}, \triangleright)$ is a descending chain of left ideals

$$\mathfrak{a} = \mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \dots$$

such that $\mathfrak{a}$ is a filtered Lie algebra with respect to this filtration and $\mathfrak{a} \triangleright \mathfrak{a}_i \subseteq \mathfrak{a}_{i+1}$ for all $i \geq 1$.

**Proposition 8.4.2.** *Let $\mathfrak{a}$ be a filtered Lie algebra. Then there is a bijective correspondence between operations $\triangleright$ such that $(\mathfrak{a}, \triangleright)$ is a filtered post-Lie algebra with respect to the filtration on $\mathfrak{a}$, and $t$-bijective Lie subalgebras of $\mathfrak{aff}_f(\mathfrak{a})$.*

*Proof.* Let $\mathfrak{a}$ be a filtered Lie algebra and let $(\mathfrak{a}, \triangleright)$ be a post-Lie algebra structure. Recall that its corresponding Lie subalgebra of $\mathfrak{aff}(\mathfrak{a})$ is $\mathfrak{g} = \{(a, \mathcal{L}_a) \mid a \in \mathfrak{a}\}$. We then see that $\mathfrak{g}$ is contained in $\mathfrak{aff}_f(\mathfrak{a})$ if and only if $\mathcal{L}_a \in \mathfrak{der}_f(\mathfrak{a})$ for all $a \in \mathfrak{a}$. This happens precisely if $\mathfrak{a} \triangleright \mathfrak{a}_i \subseteq \mathfrak{a}_{i+1}$ for all $i \geq 1$. □

Recall from Section 1.3 that for a post-Lie algebra $(\mathfrak{a}, \triangleright)$ we obtained the sub-adjacent Lie algebra structure $\mathfrak{a}^\circ$ on the module $\mathfrak{a}$ whose Lie bracket is given by

$$\{a, b\} = [a, b] + a \triangleright b - b \triangleright a,$$

for $a, b \in \mathfrak{a}$. Moreover, the map

$$\mathfrak{a}^\circ \to \mathfrak{aff}(\mathfrak{a}) : a \mapsto (a, \mathcal{L}_a),$$

induces an isomorphism between $\mathfrak{a}^\circ$ and the $t$-bijective Lie subalgebra of $\mathfrak{aff}(\mathfrak{a})$ associated to the post-Lie algebra $(\mathfrak{a}, \triangleright)$.

**Lemma 8.4.3.** *Let $(\mathfrak{a}, \triangleright)$ be a post-Lie algebra. Then $\mathfrak{a}^\circ$ is a filtered Lie algebra for the filtration*

$$\mathfrak{a}_i^\circ = \{a \in \mathfrak{a}_i \mid a \triangleright \mathfrak{a}_j \subseteq \mathfrak{a}_{i+j} \text{ for all } j \geq 1\}.$$

*Proof.* This follows directly by transferring the filtration of the associated $t$-bijective Lie subalgebra of $\mathfrak{aff}_f(\mathfrak{a})$ onto $\mathfrak{a}^\circ$. □

**Definition 8.4.4.** A *Lazard* post-Lie algebra is a filtered post-Lie algebra $(\mathfrak{a}, \triangleright)$ such that both $\mathfrak{a}$ and $\mathfrak{a}^\circ$ are Lazard Lie algebras, where the filtration on $\mathfrak{a}$ is the same one as on $(\mathfrak{a}, \triangleright)$ and the filtration on $\mathfrak{a}^\circ$ is as in Lemma 8.4.3. A map $f : (\mathfrak{a}, \triangleright) \to (\mathfrak{b}, \triangleright)$ between filtered post-Lie algebras is a *homomorphism* of filtered post-Lie algebras if it is a post-Lie algebra homomorphism such that moreover $f(\mathfrak{a}_i) \subseteq \mathfrak{b}_i$ and $f(\mathfrak{a}_i^\circ) \subseteq \mathfrak{b}_i^\circ$ for all $i \geq 1$.

Next, we follow a similar approach for skew braces. Here we recall the correspondence between skew braces of the form $(A, \cdot, \circ)$ and regular subgroups of $\mathrm{Hol}(A, \cdot)$ as described in Proposition 1.1.9. The definition of a filtered skew brace is now chosen in order to preserve this correspondence in the filtered setting.

**Definition 8.4.5.** A *filtration* on a skew brace $(A, \cdot, \circ)$ is a descending chain of strong left ideals

$$A = A_1 \supseteq A_2 \supseteq \dots,$$

such that $(A, \cdot)$ is a filtered group for the given chain of ideals and $A * A_i \subseteq A_{i+1}$ for all $i \geq 1$.

**Proposition 8.4.6.** *Let $(A,\cdot)$ be a filtered group. Then there is a bijective correspondence between operations $\circ$ such that $(A,\cdot,\circ)$ is a filtered skew brace for the filtration on $A$, and regular subgroups of $\mathrm{Hol}_f(A,\cdot)$.*

*Proof.* Let $(A,\cdot)$ be a filtered group and $(A,\cdot,\circ)$ a skew brace structure. Recall that its corresponding regular subgroup of $\mathrm{Hol}(A,\cdot)$ is given by $G=\{(a,\lambda_a)\mid a\in A\}$. We find that $G$ is contained in $\mathrm{Hol}_f(A,\cdot)$ if and only if $\lambda_a\in\mathrm{Aut}_f(A,\cdot)$ for all $a\in A$. This happens precisely if $a*b=\lambda_a(b)\cdot b^{-1}\in A_{i+1}$ for all $a\in A$ and $b\in A_i$. □

**Lemma 8.4.7.** *Let $(A,\cdot,\circ)$ be a filtered skew brace. Then $(A,\circ)$ is a filtered group for the filtration*

$$(A,\circ)_i=\{a\in A_i\mid \lambda_a(b)b^{-1}\in A_{i+j}\text{ for all } j\geq 1, b\in A_i\}.$$

*Proof.* This follows from transferring the filtration of the associated regular subgroup of $\mathrm{Hol}_f(A,\cdot)$ onto the group $(A,\circ)$, through the group isomorphism $(A,\circ)\to\{(a,\lambda_a)\mid a\in A\}$. □

**Definition 8.4.8.** A *Lazard* skew brace is a filtered skew brace $(A,\cdot,\circ)$ such that both $(A,\cdot)$ and $(A,\circ)$ are Lazard groups, where the filtration $(A,\cdot)$ is the same as on the skew brace and the filtration on $(A,\circ)$ is as in Lemma 8.4.7. A map $f:(A,\cdot,\circ)\to(B,\cdot,\circ)$ between filtered skew braces is a *homomorphism* of filtered skew braces if it is a skew brace homomorphism such that moreover the inclusions $f(A_i)\subseteq B_i$ and $f((A,\circ)_i)\subseteq(B,\circ)_i$ hold for all $i\geq 1$.

**Proposition 8.4.9.** *Let $(\mathfrak{a},\triangleright)$ be a Lazard post-Lie ring. Then*

$$W:\mathfrak{a}\to\mathfrak{a}:a\mapsto V(a,\mathcal{L}_a)$$

*is a bijective map and $\mathbf{B}(\mathfrak{a},\triangleright)=(\mathfrak{a},\cdot,\circ)$ with*

$$\begin{aligned}a\cdot b&=\mathrm{BCH}(a,b),\\ a\circ b&=a\cdot\exp(\mathcal{L}_{\Omega(a)})(b),\end{aligned}$$

*and $\Omega:=W^{-1}$, is a Lazard skew brace with respect to the filtration of $(\mathfrak{a},\triangleright)$.*

*Proof.* Let $\mathfrak{g}$ be the $t$-bijective Lie subring of $\mathfrak{aff}_f(\mathfrak{a})$ associated to $(\mathfrak{a},\triangleright)$, which is Lazard since $\mathfrak{a}^\circ$ is assumed to be Lazard. As in the statement, we define $W$ as the composition of the bijection

$$\mathfrak{a}\to\mathfrak{g}:a\mapsto(a,\mathcal{L}_a),$$

and the map $V:\mathfrak{aff}_f(\mathfrak{a})\to\mathfrak{a}$ as defined in Section 8.3. Since $\mathfrak{g}$ is $t$-bijective and Lazard, it follows from Theorem 8.3.9 that $\gamma(\mathfrak{g})$ is regular and thus $V$ induces a bijection between $\gamma(\mathfrak{g})$ and $\mathfrak{a}$. We conclude that $W$ is a bijection.

Since $\gamma(\mathfrak{g})$ is a regular subgroup of $\mathrm{Hol}_f(\mathbf{Laz}(\mathfrak{a}))$, we can consider its corresponding Lazard skew brace $(\mathfrak{a},\cdot,\circ)$ where $(\mathfrak{a},\cdot)=\mathbf{Laz}(\mathfrak{a})$. For $a,b\in\mathfrak{a}$, we have $a\circ b=a\cdot\lambda_a(b)$ where $\lambda_a\in\mathrm{Aut}(\mathfrak{a})$ is uniquely determined by the fact that $(a,\lambda_a)\in\gamma(\mathfrak{g})$. Since

$$\gamma(\mathfrak{g})=\{(W(a),\exp(\mathcal{L}_a))\mid a\in\mathfrak{a}\},$$

we find that $\lambda_a=\exp(\mathcal{L}_{\Omega(a)})$. □

From (8.6) we obtain

$$W(a) = a + \frac{1}{2}(a \triangleright a) + \frac{1}{6}(a \triangleright (a \triangleright a)) + \frac{1}{12}[a, a \triangleright a] + \frac{1}{24}([a, a \triangleright (a \triangleright a)] + a \triangleright (a \triangleright (a \triangleright a)) + \dots \quad (8.11)$$

where further terms are of order at least 5. If we restrict Proposition 8.4.9 to pre-Lie rings, the following more explicit statement follows from Lemma 8.3.6.

**Proposition 8.4.10.** *Let $(\mathfrak{a}, \triangleright)$ be a Lazard pre-Lie ring. Then*

$$W : \mathfrak{a} \to \mathfrak{a} : a \mapsto \sum_{k=1}^{\infty} \frac{1}{k!} \mathcal{L}_a^{k-1}(a)$$

*is a bijective map and $\mathbf{B}(\mathfrak{a}, \triangleright) = (\mathfrak{a}, +, \circ)$ with*

$$a \circ b = a \cdot \exp(\mathcal{L}_{\Omega(a)})(b),$$

*and $\Omega := W^{-1}$, is a Lazard brace with respect to the filtration of $(\mathfrak{a}, \triangleright)$.*

**Proposition 8.4.11.** *Let $(\mathfrak{a}, \triangleright)$ be a Lazard post-Lie ring and set $(\mathfrak{a}, \cdot, \circ) = \mathbf{B}(\mathfrak{a}, \triangleright)$. Then the map $W : \mathbf{Laz}(\mathfrak{a}^\circ) \to (\mathfrak{a}, \circ)$ is an isomorphism of filtered groups.*

*Proof.* It suffices to note that $W$ is the composition of the filtered group isomorphisms

$$\mathbf{Laz}(\mathfrak{a}^\circ) \to \mathbf{Laz}(\mathfrak{g}) : a \mapsto (a, \mathcal{L}_a),$$

$\gamma : \mathbf{Laz}(\mathfrak{g}) \to \gamma(\mathfrak{g})$ and $\mathrm{pr}_{\mathbf{Laz}(\mathfrak{a})} : \gamma(\mathfrak{g}) \to (\mathfrak{a}, \circ)$. □

**Proposition 8.4.12.** *Let $(A, \cdot, \circ)$ be a Lazard skew brace. Then*

$$\Omega : A \mapsto A : a \mapsto U(a, \lambda_a)$$

*is a bijection and $\mathbf{L}(A, \cdot, \circ) = (\mathbf{Laz}^{-1}(A, \cdot), \triangleright)$ with*

$$a \triangleright b = \log(\lambda_{W(a)})(b),$$

*and $W := \Omega^{-1}$, is a Lazard post-Lie ring with respect to the filtration on $(A, \cdot, \circ)$.*

*Proof.* Let $G$ be the regular subgroup of $\mathrm{Hol}_f(A, \cdot)$ associated to the skew brace structure $(A, \cdot, \circ)$. Then $G$ is Lazard since we assumed that $(A, \circ)$ is Lazard. Note that $\Omega$ is the composition of the bijection $A \to G : a \mapsto (a, \lambda_a)$ and the map $U : \mathrm{Hol}(A, \cdot) \to A$ with $U$ as in Section 8.3. The map $U$ induces a bijection between $G$ and $A$, since $\gamma^{-1}(G)$ is a $t$-bijective Lie subring of $\mathfrak{aff}_f(\mathbf{Laz}^{-1}(A, \cdot))$, see Theorem 8.3.9. We conclude that $\Omega$ is a bijection.

Since $\gamma^{-1}(G)$ is a $t$-bijective Lazard Lie subring of $\mathfrak{aff}_f(\mathbf{Laz}^{-1}(A, \cdot))$, we can consider its associated Lazard post-Lie ring $(\mathbf{Laz}^{-1}(A, \cdot), \triangleright)$. For $a, b \in A$, we find that $a \triangleright b = \mathcal{L}_a(b)$ where $\mathcal{L}_a$ is uniquely determined by the fact that $(a, \mathcal{L}_a) \in \gamma^{-1}(G)$. Since

$$\gamma^{-1}(G) = \{(\Omega(a), \log(\lambda_a)) \mid a \in A\},$$

we find that $\mathcal{L}_a = \log(\lambda_{\Omega^{-1}(a)})$. □

From (8.7) we obtain

$$\begin{aligned}\Omega(a) =& a(a \circ \lambda_a^{-1}(\overline{a}))^{\circ -\frac{1}{2}}(a \circ \lambda_a(a)a^{\circ -2} \circ \lambda_a^{-1}(a) \circ \overline{a})^{\circ \frac{1}{12}} \\ &\circ (a \circ \lambda_a(a) \circ \lambda_a^2(a) \circ \lambda_x(a^{-2}) \circ a \circ \lambda_a(\overline{a}) \circ \lambda_a^{-1}(\overline{a}) \circ a^{\circ 2} \circ \lambda_a(\overline{a}) \circ \overline{a})^{\circ -\frac{1}{24}} \\ &\circ (\lambda_a^{-2}(a) \circ \lambda_a^{-3}(\overline{a}) \circ \lambda_a^{-2}(a) \circ \lambda_a^{-1}(\overline{a}) \circ a \circ \lambda_a^{-1}(\overline{a}) \circ \lambda_a^{-2}(a) \circ \lambda_a^{-1}(\overline{a}))^{\circ \frac{1}{24}} \cdots,\end{aligned} \tag{8.12}$$

where further factors are of degree 5 or more. If we restrict Proposition 8.4.12 to braces, the following more explicit statement follows from Lemma 8.3.6.

**Proposition 8.4.13.** *Let $(A, +, \circ)$ be a Lazard brace. Then*

$$\Omega(a) = \sum_{k=1}^{\infty} \frac{1}{k}(\mathrm{id}_A - \lambda_a)^{k-1}(a),$$

*is a bijection and $\mathbf{L}(A, +, \circ) = (\mathbf{Laz}^{-1}(A, +), \triangleright)$ with*

$$a \triangleright b = \log(\lambda_{W(a)})(b),$$

*and $W := \Omega^{-1}$, is a Lazard pre-Lie ring with respect to the filtration on $(A, \cdot, \circ)$.*

**Theorem 8.4.14.** *The constructions in Proposition 8.4.9 and Proposition 8.4.12 are mutually inverse and functorial, and yield a correspondence between Lazard post-Lie rings and Lazard skew braces. The maps $\Omega$ and $W$ associated to a Lazard post-Lie ring $(\mathfrak{a}, \triangleright)$ coincide with those associated to $\mathbf{B}(\mathfrak{a}, \triangleright)$.*

*Proof.* Since both constructions rely on the correspondence between $t$-bijective Lazard Lie subrings of $\mathfrak{aff}_f(\mathfrak{a})$ and regular Lazard subgroups of $\mathrm{Hol}_f(\mathbf{Laz}(\mathfrak{a}))$ given by $\gamma$ and its inverse, it is clear that they are mutually inverse and that their associated maps $\Omega$ and $W$ coincide.

We prove the functoriality of $\mathbf{B}$, the proof for $\mathbf{L}$ is analogous. Let $(\mathfrak{a}, \triangleright)$ and $(\mathfrak{b}, \triangleright)$ be Lazard post-Lie rings and let $f : (\mathfrak{a}, \triangleright) \to (\mathfrak{b}, \triangleright)$ be a homomorphism of filtered post-Lie rings. Set $(\mathfrak{a}, \cdot, \circ) = \mathbf{B}(\mathfrak{a}, \triangleright)$ and $(\mathfrak{b}, \cdot, \circ) = \mathbf{B}(\mathfrak{b}, \triangleright)$, and let $W_\mathfrak{a}$ and $W_\mathfrak{b}$ denote their respective maps $W$. By Theorem 1.4.27 the map $f : (\mathfrak{a}, \cdot) \to (\mathfrak{b}, \cdot)$ is a group homomorphism. It remains to prove that $f : (\mathfrak{a}, \circ) \to (\mathfrak{b}, \circ)$ is a filtered group homomorphism. From Proposition 8.4.11 we know that it is sufficient to prove the equality $fW_\mathfrak{a} = W_\mathfrak{b} f$. However, this follows from the fact that $f\mathcal{L}_a = \mathcal{L}_{f(a)}f$ for all $a \in \mathfrak{a}$ and the fact that $f$ is a filtered Lie ring homomorphism, which implies that it behaves well with respect to the unique roots of elements. □

*Remark* 8.4.15. Recall that an element $a$ of a skew brace $(A, +, \circ)$ is *square-free* if $a * a = 0$. A skew brace is square-free if all of its elements are square-free. Similarly, we say that an element $a$ of a post-Lie ring $(\mathfrak{a}, \triangleright)$ is *square-free* if $a \triangleright a = 0$, and $(\mathfrak{a}, \triangleright)$ is square-free when all of its elements are square-free. Note that the property of being square-free is preserved by $\mathbf{B}$ and $\mathbf{L}$, and $W = \Omega = \mathrm{id}$ in this case. Therefore, these classes behave particularly well under the correspondence, and most of the computations involved are trivial.

**Proposition 8.4.16.** *Let $(\mathfrak{a}, \triangleright)$ be a Lazard post-Lie ring and let $\mathfrak{b}$ be a Lazard Lie subring of $\mathfrak{a}$. Then $\mathfrak{b}$ is a left ideal, strong left ideal or ideal in $(\mathfrak{a}, \triangleright)$ if and only if it is so in $\mathbf{B}(\mathfrak{a}, \triangleright)$.*

*Proof.* Clearly $\mathfrak{b}$ is a subgroup of $\mathbf{Laz}(\mathfrak{a})$. The statement for left ideals follows directly from the fact that $\mathfrak{b}$, since it is Lazard, is invariant under $\{\mathcal{L}_a \mid a \in \mathfrak{a}\}$ if and only if it is invariant under $\{\exp(\mathcal{L}_a) \mid a \in \mathfrak{a}\}$. This can be extended to the statement regarding strong left ideals if we take into account Lemma 1.4.31.

Before proving the last part of the statement, we prove that if $\mathfrak{b}$ is a left ideal of $(\mathfrak{a}, \triangleright)$ then $\Omega(\mathfrak{b}) = \mathfrak{b}$. We obtain $W(\mathfrak{b}) \subseteq \mathfrak{b}$ since for any $b \in \mathfrak{b}$ the expression of $W(b)$ only involves occurrences of $b$, manipulations internal to the Lie ring $\mathfrak{b}$, and applications of $\mathcal{L}_b$. Similarly, $\Omega(\mathfrak{b}) \subseteq \mathfrak{b}$ since for any $b \in \mathfrak{b}$ the expression for $\Omega(b)$ only involves occurrences of $b$, manipulations internal to the group $\mathbf{Laz}(\mathfrak{b})$ and applications of $\exp(\mathcal{L}_{\Omega(b)})$. Note that we do not need to know $\exp(\mathcal{L}_{\Omega(b)})$ explicitly since we know that $\exp(\mathcal{L}_a)(\mathfrak{b}) \subseteq \mathfrak{b}$ for all $a \in \mathfrak{a}$. We conclude that $\Omega(\mathfrak{b}) = \mathfrak{b}$.

At last, still under the assumption that $\mathfrak{b}$ is a left ideal of $(\mathfrak{a}, \triangleright)$, we use the fact that $W$ is a group isomorphism between $\mathbf{Laz}(\mathfrak{a}^\circ)$ and $(A, \circ)$ to find that $\mathfrak{b}$ is an ideal of $\mathfrak{a}^\circ$ if and only if $W(\mathfrak{b}) = \mathfrak{b}$ is a normal subgroup of $(A, \circ)$. In particular, we can conclude that $\mathfrak{b}$ is an ideal of $(\mathfrak{a}, \triangleright)$ if and only if it is an ideal of $\mathbf{B}(\mathfrak{a}, \triangleright)$. □

**Proposition 8.4.17.** *Let $(\mathfrak{a}, \triangleright)$ be a Lazard post-Lie ring. Then the fix, socle and annihilator of $(\mathfrak{a}, \triangleright)$ coincide with that of $\mathbf{B}(\mathfrak{a}, \triangleright)$. In particular, $(\mathfrak{a}, \triangleright)$ is right nilpotent if and only if $\mathbf{B}(\mathfrak{a}, \triangleright)$ is right nilpotent.*

*Proof.* The first part of the statement follows from the fact that $W(a) = a$ whenever $a \triangleright a = 0$ or $\lambda_a(a) = a$, which in particular is the case when $a$ is contained in the fix or socle. The second part of the statement now follows from [1, Lemma 5.3 and 5.4] and the analogous statement for post-Lie rings. □

**Example 8.4.18.** Let $R$ be a Lazard ring and let $\mathcal{L}_a$ denote left multiplication by $a$. Then $\mathfrak{a} = R_1$ is a Lazard pre-Lie ring for $a \triangleright b = ab$ and filtration $\mathfrak{a}_i = R_i$ for $i \geq 1$. In this case, the operation $\circ$ in $(A, +, \circ) = \mathbf{B}(\mathfrak{a}, \triangleright)$ is given by $a \circ b = a + ab + b$. Indeed, clearly $W(a) = \exp(a) - 1$, hence $\Omega(a) = \log(1 + a)$. We now find

$$a \circ b = a + \exp(\mathcal{L}_{\log(1+a)})(b) = a + ab + b.$$

Conversely, starting from the brace $(A, +, \circ)$ we find $\Omega(a) = \log(1 + a)$ and thus $W(a) = \exp(a) - 1$. We recover the original multiplication as

$$a \triangleright b = \log(\lambda_{W(a)})(b) = \log(\mathcal{L}_{1+W(a)})(b) = a + \log(\mathcal{L}_{\exp(a)})(b) = ab.$$

This is precisely the classical correspondence between two-sided braces and Jacobson radical rings as described by Rump, see Proposition 1.1.14.

## 8.5 $L$-nilpotent post-Lie algebras

In light of Section 8.4, it is natural to ask whether every post-Lie algebra $(\mathfrak{a}, \triangleright)$ admits a filtration and, in particular, whether it admits a finite filtration. The natural candidate for a filtration is the following: we set $L^1(\mathfrak{a}) = \mathfrak{a}$ and for $i \geq 1$ we inductively define $L^{i+1}(\mathfrak{a})$ as the subgroup of $(\mathfrak{a}, +)$ (or equivalently, submodule of $\mathfrak{a}$) generated by the set

$$\{a \triangleright b, [a, b] \mid a \in \mathfrak{a}, b \in L^i(A)\}.$$

We obtain a descending chain of strong left ideals

$$\mathfrak{a} = L^1(\mathfrak{a}) \supseteq L^2(\mathfrak{a}) \supseteq \dots$$

which we call the *$L$-series of* $(\mathfrak{a}, \triangleright)$. If $(\mathfrak{a}, \triangleright)$ is a pre-Lie algebra, then $L^i(\mathfrak{a}) = \mathfrak{a}^i$ so we obtain the left series as defined in Definition 1.3.24.

**Lemma 8.5.1.** *Any post-Lie algebra $(\mathfrak{a}, \triangleright)$ is a filtered post-Lie algebra for the filtration $\mathfrak{a}_i = L^i(\mathfrak{a})$.*

*Proof.* We show that $[L^i(\mathfrak{a}), L^j(\mathfrak{a})] \subseteq L^{i+j}(\mathfrak{a})$ for all $i, j \geq 1$. Consider the Lie subalgebra

$$\mathfrak{h} = \{\mathcal{L}_a \mid a \in \mathfrak{a}\}$$

of $\mathfrak{der}_f(\mathfrak{a})$ and as in Lemma 8.1.3 consider the semidirect sum $\mathfrak{t} = \mathfrak{a} \oplus_\delta \mathfrak{h}$ where $\delta : \mathfrak{h} \to \mathfrak{der}_f(\mathfrak{a})$ is the inclusion map. Then we find

$$[(a, \mathcal{L}_b), (c, 0)] = ([a, c] + b \triangleright c),$$

for all $a, b, c \in \mathfrak{a}$. It follows that $[\mathfrak{t}, \mathfrak{t}] = L^2(\mathfrak{a}) \oplus [\mathfrak{h}, \mathfrak{h}]$ or with the notation as in Lemma 1.4.4, $\gamma^2(\mathfrak{t}) = L^2(\mathfrak{a}) \oplus \gamma^2(\mathfrak{h})$. By induction one finds $\gamma^i(\mathfrak{t}) = L^i(\mathfrak{a}) \oplus \gamma^i(\mathfrak{h})$. From Lemma 1.4.4 we get

$$[L^i(\mathfrak{a}), L^j(\mathfrak{a})] \oplus 0 = [L^i(\mathfrak{a}) \oplus 0, L^j(\mathfrak{a}) \oplus 0] \subseteq L^{i+j}(\mathfrak{a}) \oplus \gamma^{i+j}(\mathfrak{h}),$$

and thus we conclude $[L^i(\mathfrak{a}), L^j(\mathfrak{a})] \subseteq L^{i+j}(\mathfrak{a})$. From the definition it is clear that $\mathfrak{a} \triangleright \mathfrak{a}_i \subseteq \mathfrak{a}_{i+1}$ for all $i \geq 1$, so we have indeed constructed a filtration on $(\mathfrak{a}, \triangleright)$. □

The above constructed filtration is clearly the finest possible one. Therefore, if there exists some finite filtration on $(\mathfrak{a}, \triangleright)$, then also the descending series $L^i(\mathfrak{a})$ terminates at some point.

**Definition 8.5.2.** A post-Lie algebra $(\mathfrak{a}, \triangleright)$ is *$L$-nilpotent* if $L^{k+1}(\mathfrak{a}) = 0$ for some $k \geq 0$. The minimal such $k$, if it exists, is the *$L$-nilpotency class* of $(\mathfrak{a}, \triangleright)$.

**Lemma 8.5.3.** *Let $(\mathfrak{a}, \triangleright)$ be a post-Lie algebra. Then $(\mathfrak{a}, \triangleright)$ is $L$-nilpotent if and only if $(\mathfrak{a}, \triangleright)$ is left nilpotent and $\mathfrak{a}$ is a nilpotent Lie ring.*

*Proof.* From the definition of $L^i(\mathfrak{a})$, it is clear that if $(\mathfrak{a}, \triangleright)$ is $L$-nilpotent then it is left nilpotent and $\mathfrak{a}$ is a nilpotent Lie algebra.

Conversely, assume that $(\mathfrak{a}, \triangleright)$ is left nilpotent and $\mathfrak{a}$ is a nilpotent Lie algebra. Let

$$\mathfrak{a} = \gamma^1(\mathfrak{a}) \supseteq \ldots \supseteq \gamma^{d+1}(\mathfrak{a}) = \{0\}$$

denote the lower central series of $\mathfrak{a}$ and let $c$ be such that $\mathfrak{a}^{c+1} = \{0\}$, recall that this is the $c+1$-th term in the left series of $(\mathfrak{a}, \triangleright)$. Assume that $L^i(\mathfrak{a}) \subseteq \gamma^k(\mathfrak{a})$ for some $i, k \geq 1$, then $[L^i(\mathfrak{a}), \mathfrak{a}] \subseteq \gamma^{k+1}(\mathfrak{a})$ and thus

$$L^{i+1}(\mathfrak{a}) \subseteq (\mathfrak{a} \triangleright L^i(\mathfrak{a})) + \gamma^{k+1}(\mathfrak{a}) \subseteq \mathfrak{a}^2 + \gamma^{k+1}(\mathfrak{a}).$$

By induction on $c$ we find

$$L^{i+c}(\mathfrak{a}) \subseteq \mathfrak{a}^{c+1} + \gamma^{k+1}(\mathfrak{a}) = \gamma^{k+1}(\mathfrak{a}).$$

Since $L^1(A) \subseteq \gamma^1(A)$ we conclude by induction on $k$ that $L^{dc+1}(\mathfrak{a}) \subseteq \gamma^{d+1}(\mathfrak{a}) = \{0\}$. □

**Theorem 8.5.4.** *Let $(\mathfrak{a}, \triangleright)$ be a post-Lie algebra of $L$-nilpotency class $k$. Then $\mathfrak{a}^\circ$ is nilpotent of class at most $k$ and the $k$-th term in the lower central series of $\mathfrak{a}^\circ$ is contained in* $\mathrm{Ann}(\mathfrak{a})$.

*Proof.* Let $(\mathfrak{a}, \triangleright)$ be $L$-nilpotent of class $k$ and consider $(\mathfrak{a}, \triangleright)$ as a filtered post-Lie algebra where its filtration is given by its $L$-series. Recall from Lemma 8.4.3 that this induces a filtration on $\mathfrak{a}^\circ$ explicitly given by

$$\mathfrak{a}_i^\circ = \{a \in L^i(\mathfrak{a}) \mid a \triangleright L^j(\mathfrak{a}) \subseteq L^{i+j}(\mathfrak{a}) \text{ for all } j \geq 1\}.$$

In particular, $\mathfrak{a}_{k+1}^\circ \subseteq L^{k+1}(\mathfrak{a}) = 0$, so indeed $\mathfrak{a}^\circ$ is nilpotent of class at most $k$. Also, for $a \in \mathfrak{a}_k^\circ$ we find that $a \triangleright \mathfrak{a} = a \triangleright L^1(\mathfrak{a}) \subseteq L^{k+1}(\mathfrak{a}) = \{0\}$ hence $\mathfrak{a}_k^\circ$ is contained in the kernel of $\mathcal{L}$. Since also $b \triangleright a, [a, b] \in L^{k+1}(\mathfrak{a}) = 0$ for all $b \in \mathfrak{a}$, we find that $\mathfrak{a}_k^\circ \subseteq Z(\mathfrak{a}) \cap \mathrm{Fix}(\mathfrak{a})$, from which the statement follows. □

**Corollary 8.5.5.** *Let $(\mathfrak{a}, \triangleright)$ be a post-Lie algebra. Then $(\mathfrak{a}, \triangleright)$ is L-nilpotent if and only if the semidirect sum $\mathfrak{a} \oplus_{\mathcal{L}} \mathfrak{a}^{\circ}$ is a nilpotent Lie algebra. Moreover, in this case the L-nilpotency class of $(\mathfrak{a}, \triangleright)$ coincides with the nilpotency class of $\mathfrak{a} \oplus_{\mathcal{L}} \mathfrak{a}^{\circ}$.*

*Proof.* Similar to the lower central series of $\mathfrak{aff}(\mathfrak{a})$ as deduced in Lemma 8.5.1, the lower central series of $\mathfrak{a} \oplus_{\mathcal{L}} \mathfrak{a}^{\circ}$ is given by

$$\gamma^i(\mathfrak{a} \oplus_{\mathcal{L}} \mathfrak{a}^{\circ}) = L^i(\mathfrak{a}) \oplus_{\mathcal{L}} \gamma^i(\mathfrak{a}^{\circ}).$$

The equivalence then follows from Theorem 8.5.4. □

## 8.6 $L$-nilpotent skew braces

Similar to the previous section, we are interested in, whether given a skew brace $(A, \cdot, \circ)$, there exists a finite filtration on it.

Set $L^1(A) = A$ and let $L^{i+1}(A)$ be the subgroup of $(A, \cdot)$ generated by

$$\{a * b, [a, b] \mid a \in A, b \in L_i(A)\},$$

where we recall that $a * b := a^{-1} \cdot (a \circ b) \cdot b^{-1}$ and the commutator is to be interpreted in $(A, \cdot)$. We obtain a descending series of strong left ideals

$$A = L^1(A) \supseteq L^2(A) \supseteq \dots$$

which we call the *L-series of* $(A, \cdot, \circ)$. Note that this series is the left-hand version of the series $R_n(A, A)$ as defined in [1]. Also, note that if $A$ is a brace, then $L^i(A) = A^i$, so we recover the left series as defined in Definition 1.1.23.

**Lemma 8.6.1.** *Any skew brace $(A, \cdot, \circ)$ is a filtered skew brace for the filtration $A_i = L^i(A)$.*

*Proof.* We show that the commutator $[L^i(A), L^j(A)]$ is contained in $L^{i+j}(A)$ for all $i, j \geq 1$. Let

$$H = \{\lambda_a \mid a \in A\} \subseteq \mathrm{Aut}(A, \cdot),$$

and consider the semidirect product $T = (A, \cdot) \rtimes_{\beta} H$ where $\beta : H \to \mathrm{Aut}(A, \cdot)$ is the inclusion map. Since

$$[(1, \lambda_a), (b, 1)] = (a * b, 1),$$

for all $a, b \in A$, it follows that $[T, T] = L^2(A) \times [H, H]$, or with the notation as in Lemma 1.4.2 $\gamma^2(T) = L^2(A) \times \gamma^2(H)$. By induction one finds $\gamma^i(T) = L^i(A) \times \gamma^i(H)$. By Lemma 1.4.2 we know that $[\gamma^i(T), \gamma^j(T)] \subseteq \gamma^{i+j}(T)$, so in particular

$$[L^i(A), L^j(A)] \times \{0\} = [L^i(A) \times \{0\}, L^j(A) \times \{0\}] \subseteq L^{i+j}(A) \times \gamma^{i+j}(H),$$

thus $[L^i(\mathfrak{a}), L^j(\mathfrak{a})] \subseteq L^{i+j}(A)$. At last, it is clear from the definition that $a * L^i(A) \subseteq L^{i+1}(A)$ for all $a \in A$. We conclude that the $L$-series indeed yields a filtration on $(A, \cdot, \circ)$. □

Note that the above filtration is the finest filtration one can consider. So if there exists some finite filtration on a skew brace $(A, \cdot, \circ)$, then the descending series $L^i(A)$ terminates at some point.

**Definition 8.6.2.** A skew brace $(A, \cdot, \circ)$ is *L-nilpotent* if $L^{k+1}(A) = \{1\}$ for some $k \geq 0$. The minimal such $k$, if it exists, is the *L-nilpotency class* of $A$.

**Lemma 8.6.3.** *Let $(A, \cdot, \circ)$ be a skew brace. Then $A$ is $L$-nilpotent if and only if $A$ is left nilpotent and $(A, \cdot)$ is a nilpotent group.*

*Proof.* From the definition of $L^i(A)$ it is clear that if $(A, \cdot, \circ)$ is $L$-nilpotent, then it is left nilpotent and $A$ is a nilpotent group.

Conversely, assume that $(A, \cdot, \circ)$ is left nilpotent and that $(A, \cdot)$ is a nilpotent group. Let

$$A = \gamma^1(A, \cdot) \supseteq \ldots \supseteq \gamma^{d+1}(A, \cdot) = \{0\}$$

be the lower central series of $(A, \cdot)$. Also, let $c$ such that $A^{c+1} = \{0\}$, recall that this is the $c+1$-th term in the left series. Assume that $L^i(A) \subseteq \gamma^k(A, \cdot)$ for some $i, k \geq 1$, then $[L^i(A), A] \subseteq \gamma^{k+1}(A, \cdot)$ hence

$$L^{i+1}(A) \subseteq (A * L^i(\mathfrak{a}))\gamma^{k+1}(A, \cdot) \subseteq A^2\gamma^{k+1}(A, \cdot).$$

By induction on $c$, we find

$$L^{i+c}(A) \subseteq A^{c+1}\gamma^{k+1}(A, \cdot) = \gamma^{k+1}(A).$$

Since $L^1(A) \subseteq \gamma^1(A)$, we conclude by induction on $k$ that $L^{dc+1}(A) \subseteq \gamma^{d+1}(A) = \{0\}$. □

**Corollary 8.6.4.** *Every skew brace of prime power size is $L$-nilpotent.*

*Proof.* Let $(A, \cdot, \circ)$ be a skew brace of size $p^n$. The group $(A, \cdot)$ is nilpotent since it is a finite $p$-group. Also from Theorem 1.1.24 it follows that $A$ is left nilpotent. The statement is now a consequence of Lemma 8.6.3. □

*Remark* 8.6.5. Contrary to skew braces, post-Lie rings of prime power size are not automatically $L$-nilpotent. Indeed, the trivial Lie ring structure on $\mathbb{Z}/p$ with $n \triangleright m = nm$ yields an example of a pre-Lie ring of size $p$ that is neither left nor right nilpotent.

**Theorem 8.6.6.** *Let $(A, \cdot, \circ)$ be an $L$-nilpotent skew brace of class $k$. Then $(A, \circ)$ is nilpotent of class at most $k$ and the $k$-th term in the lower central series of $(A, \circ)$ is contained in* $\mathrm{Ann}(A)$.

*Proof.* Let $(A, \cdot, \circ)$ be an $L$-nilpotent skew brace of class $k$ and consider it as a filtered skew brace with the filtration given by the $L$-series. As in Lemma 8.4.7, we find a filtration on $(A, \circ)$ explicitly given by

$$(A, \circ)_i = \{a \in L^i(A) \mid a * L^j(A) \subseteq L^{i+j}(A) \text{ for all } j \geq 1\}.$$

Since $(A, \circ)_{k+1} \subseteq L^{k+1}(A) = \{1\}$ we find that $(A, \circ)$ is indeed nilpotent of class at most $k$. Also, for $a \in (A, \circ)_k$ we find $a * A = a * L^1(A) \subseteq L^{k+1}(A) = \{1\}$ hence $(A, \circ)_k$ is contained in the socle of $A$. Since moreover $L^k(A) \subseteq Z(A, \cdot) \cap \mathrm{Fix}(A)$ we conclude that $(A, \circ)_k \subseteq \mathrm{Ann}(A)$. □

**Corollary 8.6.7.** *Let $(A, \cdot, \circ)$ be a skew brace. Then $A$ is $L$-nilpotent if and only if the semidirect product $(A, \cdot) \rtimes_\lambda (A, \circ)$ is a nilpotent group. Moreover, in this case the $L$-nilpotency class of $(A, \cdot, \circ)$ coincides with the nilpotency class of $(A, \cdot) \rtimes_\lambda (A, \circ)$.*

*Proof.* Similar to the lower central series of $\mathrm{Hol}(A, \cdot)$ as deduced in Lemma 8.6.1, the lower central series of $(A, \cdot) \rtimes_\lambda (A, \circ)$ is given by

$$\gamma^i((A, \cdot) \rtimes_\lambda (A, \circ)) = L^i(A) \rtimes_\lambda \gamma^i(A, \circ).$$

The equivalence then follows from Theorem 8.6.6. □

## 8.7 Finite $L$-nilpotent skew braces

Let $(A, \cdot, \circ)$ be a finite $L$-nilpotent skew brace, then by Proposition 1.1.25 we know that $A$ is isomorphic to a direct product of skew braces of prime power order. For this reason, we consider in this section only structures of prime power order.

**Theorem 8.7.1.** *Let $p^n$ be a prime power. The correspondence described in Theorem 8.4.14 yields a correspondence between post-Lie rings of size $p^n$ and $L$-nilpotency class smaller than $p$ and skew braces of size $p^n$ and $L$-nilpotency class smaller than $p$, where all structures are considered with the filtration coming from their $L$-series.*

*Proof.* Recall from Proposition 1.4.33 that a filtered Lie ring or group of order $p^n$ is Lazard if and only if the $p$-th term in its filtration is trivial. Assume we are given a post-Lie ring $(\mathfrak{a}, \triangleright)$ of size $p^n$ and $L$-nilpotency class smaller than $p$. We consider it with its filtration coming from the $L$-series, then $\mathfrak{a}^\circ_p \subseteq \mathfrak{a}_p = L^p(\mathfrak{a}) = \{0\}$ hence both $\mathfrak{a}$ and $\mathfrak{a}^\circ$ are Lazard, meaning that $(\mathfrak{a}, \triangleright)$ itself is Lazard. Therefore, we can apply Proposition 8.4.9 in order to obtain a skew brace $\mathbf{B}(\mathfrak{a}, \triangleright)$ whose $L$-nilpotency class is smaller than $p$.

Conversely, given a skew brace $(A, \cdot, \circ)$ of size $p^n$ and $L$-nilpotency class smaller than $p$ we can also consider it with its filtration coming from the $L$-series. Since $(A, \circ)_p \subseteq A_p = L^p(A) = \{1\}$ we find that $(A, \cdot, \circ)$ is Lazard hence Proposition 8.4.12 can be applied to obtain a Lie ring $\mathbf{L}(A, \cdot, \circ)$ whose $L$-nilpotency class is smaller than $p$. □

**Proposition 8.7.2.** *Let $(\mathfrak{a}, \triangleright)$ be a post-Lie ring of prime power size $p^n$ and $L$-nilpotency class smaller than $p$. Then post-Lie subrings of $(\mathfrak{a}, \triangleright)$ and skew subbraces of $\mathbf{B}(\mathfrak{a}, \triangleright)$ coincide. Similarly, left ideals, strong left ideals and ideals of $(\mathfrak{a}, \triangleright)$ and $\mathbf{B}(\mathfrak{a}, \triangleright)$ coincide.*

*Proof.* This is a direct consequence of Proposition 8.4.16 and the fact that the $L$-nilpotency class of a post-Lie subalgebra of $(\mathfrak{a}, \triangleright)$ is at most the $L$-nilpotency class of $(\mathfrak{a}, \triangleright)$. □

**Corollary 8.7.3.** *Let $p$ be a prime and $1 \leq n < p$. The correspondence described in Theorem 8.4.14 yields a correspondence between $L$-nilpotent post-Lie rings of size $p^n$ and skew braces of size $p^n$, where all structures are considered with the filtration coming from their $L$-series.*

*Proof.* Clearly, if $(\mathfrak{a}, \triangleright)$ is an $L$-nilpotent post-Lie ring of size $p^n$, then $L^{n+1}(\mathfrak{a}) = \{0\}$ and a similar statement holds for $L$-nilpotent skew braces of size $p^n$. The statement now follows from Theorem 8.7.1, taking into account Corollary 8.6.4. □

Let $(A, \cdot, \circ)$ be a skew brace and $a \in A$. Recall that for an integer $n$ we denote the $n$-th power of $a$ in $(A, \cdot)$ by $a^n$ and its $n$-th power in $(A, \circ)$ by $a^{\circ n}$. The following result extends Proposition 15 and Lemma 17 of [148] (note that these only appear in the preprint version and not in the published version [147]).

**Proposition 8.7.4.** *Let $(A, \cdot, \circ)$ be a skew brace of prime-power size $p^n$ and $L$-nilpotency class smaller than $p$. Then for any $k$*

$$\{a^{p^k} \mid a \in A\} = \{a^{\circ p^k} \mid a \in A\},$$

*and*

$$\{a \in A \mid a^{p^k} = 1\} = \{a \in A \mid a^{\circ p^k} = 1\},$$

*and these sets are ideals of $(A, \cdot, \circ)$.*

*Proof.* We prove the first part of the statement; the second part is analogous. By Theorem 8.7.1 we know that there exists a Lazard post-Lie ring $(\mathfrak{a}, \triangleright)$ such that $(A, \cdot, \circ) = \mathbf{B}(\mathfrak{a}, \triangleright)$. It follows from Proposition 8.7.2 that $p^k\mathfrak{a}$ is an ideal of $(A, \cdot, \circ)$. Since $(A, \cdot) = \mathbf{Laz}(\mathfrak{a})$, we find $p^k\mathfrak{a} = \{a^{p^k} \mid a \in A\}$. Also, from Proposition 8.4.11 we obtain

$$W(p^k\mathfrak{a}) = \{a^{\circ p^k} \mid a \in A\},$$

but since $W(p^k\mathfrak{a}) = p^k\mathfrak{a}$ (see proof of Proposition 8.4.16), we get the desired equality. □

### 8.7.1 IYB groups

Recall that a group $G$ is an *involutive Yang–Baxter (IYB) group* if it is isomorphic to the permutation group of an involutive finite set-theoretical solution of the YBE. Equivalently, a group $(G, \circ)$ is IYB if there exists some abelian group structure $(G, +)$ such that $(G, +, \circ)$ is a brace. It is an open problem to characterize all such groups. It is well-known that finite IYB groups are solvable, see [73]. Many classes of finite groups are known to be IYB. Examples of such classes are groups of nilpotency class 2 or $A$-groups, see [48, 51]. Conversely, if a group $G$ is IYB, then so are its Sylow subgroups. In [10], Bachiller proved that for all but a finite number of primes $p$ there exists a $p$-group of order $p^{10}$ that is not IYB. The main tools here were a counterexample by Burde to a conjecture of Milnor [23] and the Lazard correspondence. Actually, he even proved the stronger statement that for all but a finite number of primes $p$ there exists a $p$-group of order $p^{10}$ and exponent $p$ that does not embed into the matrix group $\mathrm{GL}_{11}(\mathbb{F}_p)$. Together with the fact that for a brace $(A, +, \circ)$ of order $p^{10}$ and $p \geq 11$ the exponent of $(A, +)$ and $(A, \circ)$ coincide, see Proposition 8.7.4, this indeed implies the earlier statement. Theorem 8.7.1 could be useful in the study of IYB $p$-groups, as we can easily deduce the following statement from it.

**Corollary 8.7.5.** *Let $p$ be a prime and $n < p$. Then a group $G$ of order $p^n$ is IYB if and only if $\mathbf{Laz}^{-1}(G)$ is isomorphic to the sub-adjacent Lie ring of some left nilpotent pre-Lie algebra.*

The underlying philosophy here is precisely the same as that of Bachiller, but it allows us to be more precise since there might be groups of order $p^n$ and exponent $p$ that are not IYB but are embeddable in $\mathrm{GL}_{n+1}(\mathbb{F}_p)$.

### 8.7.2 Differentiation using primitive roots of unity

At last, we shortly discuss and extend [147, Theorems 12 and 13]. Recall that, for $n \geq 1$, a *primitive $n$-th root of unity* of a ring $R$ is an element $\xi \in R$ such that $\xi^n = 1$ and $\xi^k - 1$ is not a zero divisor for $1 \leq k < n$. Since the group of invertible elements of a finite field of prime power order $\mathbb{F}_{p^n}$ is cyclic, it has a primitive $(p^n - 1)$-th root of unity. The same holds for $\mathbb{Z}/p^n$; indeed, any element of order $p - 1$ in $(\mathbb{Z}/p^n)^\times$ is a primitive $(p - 1)$-th root of unity since its image in $\mathbb{Z}/p$ is a primitive $(p - 1)$-th root of unity. Recall that [147, Theorems 12 and 13] states:

**Theorem 8.7.6.** *Let $(A, +, \circ)$ be a strongly nilpotent brace of prime power size $p^n$ and strong nilpotency class $k$, with $k, n < p - 1$. Let $\xi \in \mathbb{Z}$ be a primitive $(p - 1)$-th root of unity modulo $p^n$. Then $(\mathfrak{a}, \triangleright)$ with $\mathfrak{a}$ the trivial Lie ring on the abelian group $(A, +)$ and*

$$a \triangleright b = -(1 + p + p^2 + \ldots + p^{n-1}) \sum_{i=0}^{p-2} ((\xi^i a) * b)$$

*is a pre-Lie ring such that $\mathbf{B}(\mathfrak{a}, \triangleright) = (A, +, \circ)$.*

Therefore, in the setting of Theorem 8.7.6, it follows that

$$-(1+p+p^2+\ldots+p^{n-1})\sum_{i=0}^{p-2}((\xi^i a)*b)=\log(\lambda_{W(a)})(b),$$

for all $a,b\in A$, since $\mathbf{B}$ provides an inverse construction of $\mathbf{L}$. Before explaining why this equality holds, we consider a similar phenomenon in a more general context. As usual, let $R$ be a commutative ring.

**Definition 8.7.7.** A map $f:M\to N$ between $R$-modules is:

- *homogeneous polynomial of degree $k$* if $f(rm)=r^kf(m)$ for all $r\in R$, $m\in M$.
- *polynomial of degree less than $k$* if it can be written as a sum $f=\sum_{i=0}^{k-1}f_i$ where $f_i$ is a homogeneous polynomial of degree $i$.

**Lemma 8.7.8.** *Let $R$ be a ring and let $M,N$ be $R$-modules. Let $\xi\in R$ be a primitive $n$-th root of unity where $n$ is invertible in $R$ and let $f:M\to N$ be polynomial of degree less than $n$, with homogeneous decomposition $f=\sum_{i=0}^{n-1}f_i$. Then*

$$\frac{1}{n}\sum_{j=0}^{n-1}\xi^{jk}f(\xi^{-j}m)=f_k(m)$$

*for all $0\leq k<n$ and $m\in M$.*

*Proof.* Let $0\leq k<n$, then

$$\frac{1}{n}\sum_{j=0}^{n-1}\xi^{jk}f(\xi^{-j}m)=\frac{1}{n}\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}\xi^{j(k-i)}f_i(m)=f_k(m),$$

since $\frac{1}{n}\sum_{j=0}^{n-1}\xi^{j(k-i)}$ equals $0$ if $i\neq k$ and it equals $1$ if $i=k$. □

For $k=1$, it makes sense to see the above manipulation as taking the directional derivative of $f$ through $m$ and subsequently evaluating at $0$. Therefore, in the above setting, it is justified to introduce the notation

$$df:M\to N:m\mapsto\frac{1}{n}\sum_{i=0}^{n-1}\xi^i f(\xi^{-i}m).$$

Although the previous analogy is not explicitly mentioned, this technique plays a prominent role throughout [146, 147]. We are now ready to prove an extension of [147, Theorems 12 and 13].

**Proposition 8.7.9.** *Let $p^k$ be a prime power, $\xi\in\mathbb{Z}$ a primitive $(p-1)$-th root of unity modulo $p^k$. Let $(A,\cdot,\circ)$ be a filtered skew brace of order $p^k$ such that $A_p=\{1\}$ and such that $A_i*A_j\subseteq A_{i+j}$ for all $i,j\geq 1$. Set $(\mathfrak{a},\triangleright)=\mathbf{L}(A,\cdot,\circ)$. Then*

$$a\triangleright b=-(1+p+p^2+\ldots+p^{k-1})\sum_{i=0}^{p-2}\xi^i\lambda_{\xi^{-i}a}(b),$$

*where the sum is taken in $\mathbf{Laz}^{-1}(A,\cdot)$.*

*Proof.* By Theorem 8.7.1 we know that $(A, \cdot, \circ) = \mathbf{B}(\mathfrak{a}, \triangleright)$ for some Lazard post-Lie ring $(\mathfrak{a}, \triangleright)$ of size $p^k$. In particular, $\mathfrak{a}$ has a natural structure of a $\mathbb{Z}/p^k$-module. Since $W(\mathfrak{a}_i) = \mathfrak{a}_i$, it follows from Theorem 8.3.4 that the assumption on the filtration translates to $\mathfrak{a}_i \triangleright \mathfrak{a}_j \subseteq \mathfrak{a}_{i+j}$ for all $i, j \geq 1$.

Consider the map $\lambda : \mathfrak{a} \to \mathrm{End}(\mathfrak{a}) : a \mapsto \lambda_a$. We claim that $\lambda$ is polynomial of degree less than $p-1$ and that, moreover, its degree 1 component is $\mathcal{L}_a$. Indeed, from Proposition 8.4.9 we find

$$\lambda_{ta} = \exp(\mathcal{L}_{W(ta)}) = \sum_{k=0}^{\infty}\sum_{i=1}^{\infty} \frac{1}{k!i!}\mathcal{L}^k_{\mathcal{L}^{i-1}_{ta}(ta)} = \sum_{k=0}^{\infty}\sum_{i=1}^{\infty} \frac{1}{k!i!}t^{ki}\mathcal{L}^k_{\mathcal{L}^{i-1}_{a}(a)}.$$

Clearly $\mathcal{L}^{i-1}_a(a) \in \mathfrak{a}_i$. By the earlier mentioned condition on the filtration we have $\mathcal{L}^k_{\mathcal{L}^{i-1}_a(a)}(b) \in A^{ki+1}$ for all $b \in \mathfrak{a}$ and thus $\mathcal{L}^k_{\mathcal{L}^{i-1}_a(a)} = 0$ for $ki \geq p-1$. Therefore, $\lambda$ is polynomial of degree less than $p-1$ and its degree 1 component is $\mathcal{L}_a$. From Lemma 8.7.8 we obtain $d\lambda(a) = \mathcal{L}_a$ which concludes the proof. □

*Remark* 8.7.10. A filtration as in Proposition 8.7.9 exists precisely if $A^{\{p\}} = \{1\}$ where $A^{\{1\}} = A$ and $A^{\{k+1\}}$ is the subgroup of $(A, \cdot)$ generated by

$$\{a * b, a \cdot b \cdot a^{-1} \cdot b^{-1} \mid a \in A^{\{i\}}, b \in A^{\{k+1-i\}}\}.$$

For braces, this is precisely the chain of ideals $A^{[k]}$ used to define strong nilpotency as in Definition 1.1.29.

When $R$ has characteristic $p^n$, the degrees of the polynomial functions considered in Lemma 8.7.8 are not directly bounded by $p$. On the other hand, in the formulae for $\exp$ and $\log$ no terms of degree $p$ or more are allowed in this case. It is therefore natural to ask whether the nilpotency condition in Proposition 8.7.9 can be relaxed under the assumption that an appropriate root of unity is present.

*Question* 8.7.11. Let $(A, +, \circ)$ be an $\mathbb{F}_{p^n}$-brace (as in [46, Definition 2]) such that $A^{[p^n]} = 1$ and let $\xi \in \mathbb{F}_{p^n}$ be a primitive $(p^n-1)$-th root of unity. Does the operation

$$a \triangleright b = \frac{1}{p^n - 1}\sum_{i=0}^{p^n-2} \xi^i \lambda_{\xi^{-i}a}(b)$$

yield a pre-Lie $\mathbb{F}_{p^n}$-algebra structure on the trivial Lie algebra $(A, +)$?

## 8.8 $L$-nilpotent post-Lie algebras over $\mathbb{R}$

In [98], it is explained how one can differentiate a regular affine action of a Lie group on $\mathbb{R}^n$ in order to obtain a pre-Lie algebra. A similar construction appears in [27] for a nilpotent Lie group acting affinely on a nilpotent Lie group in order to obtain a $t$-bijective subgroup of the affine Lie algebra on the associated Lie algebra. In [15], differentiation is used to obtain a post-Lie algebra from a post-Lie group. All of these constructions coincide, up to the correspondences discussed in Sections 1.1.5 and 1.3.1, and the philosophy is precisely the same as the one present in Sections 8.3 and 8.4.

Let $G, A$ be connected Lie groups with associated Lie algebras $\mathfrak{g}, \mathfrak{a}$. Recall that $\mathrm{Hol}^\infty(A)$ denotes the semidirect product $A \rtimes \mathrm{Aut}^\infty(A)$ where $\mathrm{Aut}^\infty(A)$ are the Lie group automorphisms of $A$. Since every Lie group automorphism of $A$ yields an automorphism of $\mathfrak{a}$ and $\mathfrak{Der}(\mathfrak{a})$ is the Lie algebra associated to $\mathrm{Aut}^\infty(\mathfrak{a})$, we find that the Lie algebra associated to $\mathrm{Hol}^\infty(A)$ can be identified with a Lie subalgebra of $\mathfrak{aff}(\mathfrak{a})$. In particular, any smooth group homomorphism $f : G \to \mathrm{Hol}^\infty(A)$ yields a Lie algebra homomorphism

$df : \mathfrak{g} \to \mathfrak{aff}(\mathfrak{a})$. If we assume that $f$ corresponds to a regular action, then also $df$ is injective and $df(\mathfrak{g})$ is a $t$-bijective Lie subalgebra of $\mathfrak{aff}(\mathfrak{a})$.

If we assume that $G, A$ are also simply connected, then $\mathrm{Aut}^\infty(A) \cong \mathrm{Aut}(\mathfrak{a})$ and thus $\mathfrak{aff}(\mathfrak{a})$ is precisely the Lie algebra associated to $\mathrm{Hol}^\infty(A)$. For every Lie algebra homomorphism $\psi : \mathfrak{g} \to \mathfrak{aff}(\mathfrak{a})$ there exists a unique smooth group homomorphism $f : G \to \mathrm{Hol}(A)$ such that $df = \psi$. In other words, there is a bijective correspondence between group homomorphism $f : G \to \mathrm{Hol}(A)$ and Lie algebra homomorphisms $\psi : \mathfrak{g} \to \mathfrak{aff}(\mathfrak{a})$.

$$\begin{array}{ccc} G & \xrightarrow{f} & \mathrm{Hol}^\infty(A) \\ {\scriptstyle\exp}\uparrow & & \uparrow{\scriptstyle\exp} \\ \mathfrak{g} & \xrightarrow[\psi]{} & \mathfrak{aff}(\mathfrak{a}) \end{array}$$

As before, we know that injectivity of $f$ coincides with that of $\psi$. Also, if $f(G)$ is regular, then $\psi(\mathfrak{g})$ is $t$-bijective. However, it is generally not true that the inverse holds. As proved by Kim in [98], for $A \cong (\mathbb{R}^n, +)$ the inverse holds precisely when the pre-Lie algebra determined by $\psi(\mathfrak{g})$ is transitive; recall that this means that the map $x \mapsto x \triangleright y + x$ is bijective for all $y \in \mathfrak{a}$. Burde, Dekimpe and Deschamps proved the following result in [27, Theorem 3.1].

**Theorem 8.8.1.** *Let $G, A$ be connected, simply connected nilpotent Lie groups. Then, using the same notation as above, the following are equivalent for a smooth group homomorphism $f : G \to \mathrm{Hol}^\infty(A)$:*

1. *$f$ is injective and $f(G)$ is a regular subgroup of $\mathrm{Hol}^\infty(A)$,*
2. *$df$ is injective and $df(\mathfrak{g})$ is a $t$-bijective Lie subalgebra of $\mathfrak{aff}(\mathfrak{a})$ such that the corresponding post-Lie algebra is left nil.*

Which, using Proposition 1.3.26 and Lemma 8.5.3, can be reinterpreted as a statement about post-Lie algebras and skew Lie braces.

**Theorem 8.8.2.** *There is a bijective correspondence between $L$-nilpotent finite dimensional real post-Lie algebras $(\mathfrak{a}, \triangleright)$, and connected, simply-connected skew Lie braces $(A, \cdot, \circ)$ such that $(A, \cdot)$ and $(A, \circ)$ are nilpotent.*

We now explain how the above construction is related to Theorem 8.4.14. Let $G$ and $A$ be connected, simply connected nilpotent Lie groups and let $f : G \to \mathrm{Hol}^\infty(A)$ be a smooth group homomorphism satisfying the equivalent properties of Theorem 8.8.1. Let $\mathfrak{g}$ and $\mathfrak{a}$ be the Lie algebras associated to $G$ and $A$ respectively. On $\mathfrak{a}$ we consider the filtration $\mathfrak{a}_i = L^i(\mathfrak{a})$, coming from the post-Lie algebra associated to $df(\mathfrak{g})$. In this way, $df(\mathfrak{g})$ is contained in $\mathfrak{aff}_f(\mathfrak{a})$. Keep in mind that from Proposition 1.3.26 we know that the $L$-series terminates and thus $\mathfrak{a}$ is Lazard with respect to this filtration, since we are working over $\mathbb{R}$. On $\mathfrak{g}$ we consider the filtration $\mathfrak{g}_i = (df)^{-1}(\mathfrak{aff}_f(\mathfrak{a})_i)$, which also makes $\mathfrak{g}$ into a Lazard Lie algebra. As in Proposition 1.4.39, we identify $G$ with $\mathbf{Laz}(\mathfrak{g})$ and $A$ with $\mathbf{Laz}(\mathfrak{a})$ through their respective exponential maps. As in Proposition 8.3.5 we have the isomorphism $\gamma : \mathbf{Laz}(\mathfrak{aff}_f(\mathfrak{a})) \cong \mathrm{Hol}_f(\mathbf{Laz}(\mathfrak{a}))$ where $\mathfrak{a}$ is considered as a post-Lie ring. However, we want to consider $\mathfrak{a}$ as a post-Lie algebra over $\mathbb{R}$. If we do so, then we see that $\gamma$ restricts to a bijection between $\mathfrak{aff}_f(\mathfrak{a})$ (with $\mathfrak{a}$ considered here as a post-Lie algebra over $\mathbb{R}$) and

$$\mathrm{Hol}_f^\infty(\mathbf{Laz}(\mathfrak{a})) := \mathrm{Hol}_f(\mathbf{Laz}(\mathfrak{a})) \cap \mathrm{Hol}^\infty(\mathbf{Laz}(\mathfrak{a})).$$

This means that we can extend the previous commutative diagram to the following one, which shows that indeed the correspondence in Theorem 8.8.2 is a specialized case of Theorem 8.4.14.

$$\begin{array}{ccccc} \mathbf{Laz}(\mathfrak{g}) & \xrightarrow{f} & \mathrm{Hol}_f^{\infty}(\mathbf{Laz}(\mathfrak{a})) & \hookrightarrow & \mathrm{Hol}^{\infty}(\mathbf{Laz}(\mathfrak{a})) \\ {\scriptstyle \mathrm{id}}\uparrow & & \uparrow{\scriptstyle \gamma} & & \uparrow{\scriptstyle \exp} \\ \mathfrak{g} & \xrightarrow[df]{} & \mathfrak{aff}_f(\mathfrak{a}) & \hookrightarrow & \mathfrak{aff}(\mathfrak{a}) \end{array}$$

Here we used the fact that the identity $\mathfrak{g} \to \mathbf{Laz}(\mathfrak{g})$ plays the role of the exponential map, see Proposition 1.4.39. Note that a priori, the assumptions on the skew Lie braces in Theorem 8.8.2 differ from the ones imposed in Theorem 8.4.14. Since both constructions coincide and the conditions on the post-Lie algebras are the same, we can deduce the following counterpart of Theorem 1.1.24. Alternatively, this can also be obtained from [27, Theorem 2.1].

**Theorem 8.8.3.** *Let $(A, \cdot, \circ)$ be a connected, simply connected skew Lie brace such that $(A, \cdot)$ is nilpotent. Then $(A, \cdot, \circ)$ is left nilpotent if and only if $(A, \circ)$ is nilpotent.*

## 8.9 Complete post-Lie rings and skew braces

As discussed in Section 1.4, the Lazard correspondence can be extended to completions of Lazard Lie rings and completions of Lazard groups. Similarly, in [2] and [15], the notion of completeness appears for pre-Lie and post-Lie algebras over a field of characteristic 0. In this section, we use the Lazard correspondence obtained in Section 8.4 to also provide a correspondence between certain complete post-Lie algebras and skew braces. Before we can give sense to the notion of completeness in this context, we prove that the categories of filtered post-Lie rings and filtered skew braces are complete.

**Proposition 8.9.1.** *The category of filtered post-Lie rings is complete.*

*Proof.* It is sufficient to prove that it has all equalizers and small products. Let $f, g : (\mathfrak{a}, \triangleright) \to (\mathfrak{b}, \triangleright)$ be homomorphisms of filtered post-Lie algebras. Then

$$\{a \in \mathfrak{a} \mid f(a) = g(a)\},$$

is a post-Lie subalgebra of $(\mathfrak{a}, \triangleright)$. Together with the filtration coming from $(\mathfrak{a}, \triangleright)$ and the inclusion map, this is easily seen to indeed be the equalizer of the pair $f, g$.

Next, let $(\mathfrak{a}_i, \triangleright)_{j \in J}$ be a small family of filtered post-Lie algebras. Then the product of sets $\prod_{j \in J} \mathfrak{a}_j$ with pointwise operations and the filtration $(\prod_{j \in J} \mathfrak{a}_j)_i = \prod_{j \in J} (\mathfrak{a}_j)_i$ is, together with the projection maps the categorical product of $(\mathfrak{a}_i, \triangleright)_{j \in J}$. □

As a specific case, let $(\mathfrak{a}_i, \triangleright)_{i \geq 1}$ be a family of post-Lie algebras and $(f_i : \mathfrak{a}_{i+1} \to \mathfrak{a}_i)_{i \geq 1}$ a family of homomorphisms, then the limit of a diagram

$$\ldots \longrightarrow (\mathfrak{a}_3, \triangleright) \xrightarrow{f_2} (\mathfrak{a}_2, \triangleright) \xrightarrow{f_1} (\mathfrak{a}_1, \triangleright)$$

can be explicitly realized as

$$\varprojlim (\mathfrak{a}_i, \triangleright) = \{(a_i)_{i \geq 1} \mid a_i \in \mathfrak{a}_i, f_i(a_{i+1}) = a_i \text{ for all } i \geq 1\},$$

with the pointwise operations and filtration, together with the homomorphisms

$$\varprojlim (\mathfrak{a}_i, \triangleright) \to (\mathfrak{a}_k, \triangleright) : (a_i)_{i \geq 1} \mapsto a_k.$$

**Proposition 8.9.2.** *The category of filtered skew braces is complete.*

*Proof.* It is sufficient to prove that it has all equalizers and small products. Let $f, g : (A, \cdot, \circ) \to (B, \cdot, \circ)$ be homomorphisms of filtered post-Lie algebras. Then

$$\{a \in A \mid f(a) = g(a)\},$$

is a skew subbrace of $(A, \cdot, \circ)$. Together with the filtration coming from $(A, \cdot, \circ)$ and the inclusion map, this is easily seen to indeed be the equalizer of the pair $f, g$.

Next, let $(A_i, \cdot, \circ)_{j\in J}$ be a small family of filtered post-Lie algebras. Then the product of sets $\prod_{j\in J} A_j$ with pointwise operations and the filtration $(\prod_{j\in J} A_j) = \prod_{j\in J}(A_j)_i$ is, together with the projection maps, the categorical product of $((A_i, \cdot, \circ))_{j\in J}$. □

Let $(A_i, \cdot, \circ)_{i\geq 1}$ be a family of filtered skew braces and let $(f_i : (A_{i+1}, \cdot, \circ) \to (A_i, \cdot, \circ))_{i\geq 1}$ be a family of homomorphisms, then the limit of the diagram

$$\ldots \longrightarrow (A_3, \cdot, \circ) \xrightarrow{f_2} (A_2, \cdot, \circ) \xrightarrow{f_1} (A_1, \cdot, \circ)$$

can be explicitly realized as

$$\varprojlim(A_i, \cdot, \circ) = \{(a_i)_{i\geq 1} \mid a_i \in A_i, f_i(a_{i+1}) = a_i \text{ for all } i \geq 1\},$$

with the pointwise operations and filtration, together with the homomorphisms

$$\varprojlim(A_i, \cdot, \circ) \to (A_k, \cdot, \circ) : (a_i)_{i\geq 1} \mapsto a_k.$$

**Definition 8.9.3.** Let $(\mathfrak{a}, \triangleright)$ be a filtered post-Lie algebra and let

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \ldots$$

be a descending chain of ideals of $(\mathfrak{a}, \triangleright)$. Then $(\mathfrak{a}, \triangleright)$ is *complete* with respect to this chain if the canonical homomorphism $(\mathfrak{a}, \triangleright) \to \varprojlim(\mathfrak{a}, \triangleright)/I_i$ is an isomorphism.

**Definition 8.9.4.** Let $(A, \cdot, \circ)$ be a filtered skew brace and let

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \ldots$$

be a descending chain of ideals of $(A, \cdot, \circ)$. Then $(A, \cdot, \circ)$ is *complete* with respect to this chain if the canonical homomorphism $(A, \cdot, \circ) \to \varprojlim(A, \cdot, \circ)/I_i$ is an isomorphism.

Let $(\mathfrak{a}, \triangleright)$ be a filtered post-Lie algebra and let $I_k$, $k \geq 1$, be a descending chain of ideals of $(\mathfrak{a}, \triangleright)$. Assume that $(\mathfrak{a}, \triangleright)$ is complete with respect to this chain of ideals and that, moreover, $(\mathfrak{a}, \triangleright)/I_k$ is Lazard for each $k \geq 1$. We identify $(\mathfrak{a}, \triangleright)$ with $\varprojlim(A, \cdot, \circ)/I_k$ and define

$$\hat{\mathbf{B}}(\varprojlim(A, \cdot, \circ)/I_k) = \varprojlim \mathbf{B}((A, \cdot, \circ)/I_k),$$

so explicitly

$$(a_k + I_k)_{k\geq 1} \cdot (b_k + I_k)_{k\geq 1} = ((a_k + I_k) \cdot (b_k + I_k))_{k\geq 1},$$
$$(a_k + I_k)_{k\geq 1} \circ (b_k + I_k)_{k\geq 1} = ((a_k + I_k) \circ (b_k + I_k))_{k\geq 1},$$

where the operations on the right are taken in $\mathbf{B}((\mathfrak{a}, \triangleright)/I_k)$. In this way we obtain a filtered skew brace $\hat{\mathbf{B}}(\mathfrak{a}, \triangleright)$ with a descending chain of ideals $I_k$, $k \geq 1$, such that $\hat{\mathbf{B}}(\mathfrak{a}, \triangleright)/I_k = \mathbf{B}((\mathfrak{a}, \triangleright)/I_k)$ for all $k \geq 1$.

Conversely, let $(A, \cdot, \circ)$ be a filtered skew brace together with a descending chain of ideals $I_k$, $k \geq 1$. Assume that $(A, \cdot, \circ)$ is complete with respect to this chain of ideals and that moreover $(A, \cdot, \circ)/I_k$ is Lazard for all $k \geq 1$. We identify $(A, \cdot, \circ)$ with $\varprojlim (A, \cdot, \circ)/I_k$ and define

$$\hat{\mathbf{L}}(\varprojlim (A, \cdot, \circ)/I_k) = \varprojlim \mathbf{L}((A, \cdot, \circ)/I_k),$$

so explicitly

$$\begin{aligned}
(a_k I_k)_{k\geq 1} + (b_k I_k)_{i\geq 1} &= ((a_k I_k) + (b_k I_k))_{k\geq 1}, \\
[(a_k I_k)_{k\geq 1}, (b_k I_k)_{i\geq 1}] &= ([(a_k I_k), (b_k I_k)])_{k\geq 1}, \\
(a_k I_k)_{k\geq 1} \triangleright (b_k I_k)_{i\geq 1} &= ((a_k I_k) \triangleright (b_k I_k))_{k\geq 1},
\end{aligned}$$

where the operations on the right are taken in $\mathbf{L}((A, \cdot, \circ)/I_k)$. In this way we obtain a complete post-Lie ring $\mathbf{L}(A, \cdot, \circ)$ such that the $I_k$ form a descending chain of ideals and $\hat{\mathbf{L}}(A, \cdot, \circ)/I_k = \mathbf{L}((A, \cdot, \circ)/I_k)$ for all $k \geq 1$. These two constructions are clearly inverse.

**Theorem 8.9.5.** *The constructions $\hat{\mathbf{B}}$ and $\hat{\mathbf{L}}$ as defined above yield a correspondence between:*

- *filtered post-Lie algebras $(\mathfrak{a}, \triangleright)$ together with a descending chain of ideals $I_k$, $k \geq 1$, such that $(\mathfrak{a}, \triangleright)$ is complete with respect to this chain and such that $(\mathfrak{a}, \triangleright)/I_k$ is Lazard for all $k \geq 1$.*
- *filtered skew braces $(A, \cdot, \circ)$ together with a descending chain of ideals $I_k$, $k \geq 1$, such that $(A, \cdot, \circ)$ is complete with respect to this chain and such that $(A, \cdot, \circ))/I_k$ is Lazard for all $k \geq 1$.*

### 8.9.1 Group of formal flows

Let $K$ be a field of characteristic $0$. In [2] Agrachev and Gamkrelidze define a *graded chronological algebra* as a graded vector space $L = \bigoplus_{i=1}^{\infty} L_i$ over $K$ with an operation $\triangleright$ such that $(L, \triangleright)$ is a pre-Lie algebra satisfying $L_i \triangleright L_j \subseteq L_{i+j}$ for all $i, j \geq 1$. Starting from a graded chronological algebra $L$, the authors construct the *group of formal flows of $L$* in the following way. First the product $\triangleright$ is extended to the completed vector space

$$\hat{L} := \prod_{i=1}^{\infty} L_i,$$

as

$$\left(\sum_{i=1}^{\infty} x_i\right) \triangleright \left(\sum_{i=1}^{\infty} y_i\right) = \sum_{i=2}^{\infty} \left(\sum_{j=1}^{i-1} x_j \triangleright y_{i-j}\right).$$

Then the bijective map $W : \hat{L} \to \hat{L}$ is defined as

$$W(x) = \sum_{k=1}^{\infty} \frac{1}{k!} \mathcal{L}_x^{k-1}(x),$$

where as usual $\mathcal{L}_x$ denotes left multiplication by $x$ in $\hat{L}$. This infinite sum is well-defined since on every component $L_i$ it restricts to a finite sum. Next, $\Omega$ is defined as $W^{-1}$ and at last the group operation on $\hat{L}$ is given by the map

$$x \circ y = x + \exp(\mathcal{L}_{\Omega(x)})(y).$$

We now explain how this construction is related to the one given in Theorem 8.9.5. First of all, note that $(\hat{L}, \triangleright)$ is a pre-Lie algebra over $K$. For every $k \geq 1$, the product $I_k = \prod_{i=k}^{\infty} L_i$ is an ideal of $\hat{L}$ since $\hat{L} \triangleright I_k \subseteq I_{k+1} \subseteq I_k$ and similarly $I_k \triangleright \hat{L} \subseteq I_{k+1} \subseteq I_k$. Moreover, $(\hat{L}, \triangleright)$ is complete with respect to the ideals $I_k$. Since we have observed that $\hat{L} \triangleright I_k \subseteq I_{k+1}$, the ideals $I_k$ also yield a filtration on $\mathfrak{a}$ such that the induced filtration on the quotient $(\hat{L}, \triangleright)/I_k$ is finite and thus $(\hat{L}, \triangleright)/I_k$ is Lazard. Since $(\hat{L}, \circ)/I_i$ is the multiplicative group of $\mathbf{Laz}((\hat{L}, \triangleright)/I_i)$ for all $i \geq 1$, we find that $(\hat{L}, \circ)$ as constructed by Agrachev and Gamkrelidze is the second group operation of $\hat{\mathbf{B}}(\hat{L}, \triangleright)$.

### 8.9.2 Formal integration of post-Lie algebras

It requires some more work to see how Theorem 8.9.5 is related to the formal integration as described by Bai, Guo, Sheng and Tang [15]. Again, let $K$ be a field of characteristic 0. Bai, Guo, Sheng and Tang associate a skew brace to any connected complete post-Lie algebra $(\mathfrak{a}, \triangleright)$ over $K$. In our terminology, their notion of a connected complete post-Lie algebra over $K$ is a filtered post-Lie algebra $(\mathfrak{a}, \triangleright)$ that satisfies two additional conditions: the first one is that

$$\mathfrak{a}_i \triangleright \mathfrak{a}_j \subseteq \mathfrak{a}_{i+j}, \tag{8.13}$$

for all $i, j \geq 0$, which implies that $\mathfrak{a}_i$ is an ideal. Secondly, $(\mathfrak{a}, \triangleright)$ must be complete with respect to the chain of ideals $\mathfrak{a}_i$. Note that (8.13) is the same condition that also appeared in Proposition 8.7.9 and in the construction of the group of flows, and is equivalent to demanding that the filtration on $\mathfrak{a}^\circ$ coincides with the one on $\mathfrak{a}$.

We explicitly recall the construction given in [15]: Let $(\mathfrak{a}, \triangleright)$ be a filtered post-Lie algebra satisfying the above assumptions. We consider the universal enveloping algebra $\mathcal{U}(\mathfrak{a})$ as a filtered algebra as explained in Example 1.4.12. On $\mathcal{U}(\mathfrak{a})$ we define a new multiplication $\star$ which for $a \in \mathfrak{a}$, $b \in \mathcal{U}(\mathfrak{a})$ is given by

$$a \star b = ab + \mathcal{L}_a(b),$$

where $\mathcal{L}_a$ is the unique extension of the derivation $\mathcal{L}_a \in \mathfrak{der}_f(\mathfrak{a})$ to a derivation of the algebra $\mathcal{U}(\mathfrak{a})$. In this way, $(\mathcal{U}(\mathfrak{a}), \star)$ becomes a filtered algebra, where the filtration on $\mathcal{U}(\mathfrak{a})$ is the same as before. This operation is then extended to the completion $\hat{\mathcal{U}}(\mathfrak{a}) = \varprojlim \mathcal{U}(\mathfrak{a})/\mathcal{U}(\mathfrak{a})_i$ in order to obtain a complete filtered algebra $(\hat{\mathcal{U}}(\mathfrak{a}), \star)$. Since $\mathfrak{a}$ is assumed to be complete and $\mathfrak{a} \cap \mathcal{U}(\mathfrak{a})_i = \mathfrak{a}_i$ for all $i \geq 1$, we find that $\mathfrak{a}$ still embeds into $\hat{\mathcal{U}}(\mathfrak{a})$. Define

$$\Omega : \mathfrak{a} \to \mathfrak{a} : a \mapsto (\log_\star \exp(a_i + \hat{\mathcal{U}}(\mathfrak{a})_i))_{i \geq 1},$$

where $\log_\star \exp(a_i + \mathfrak{a}_i)$ denotes the element obtained by first taking the exponential map with respect to the usual multiplication in $\mathcal{U}(\mathfrak{a})/\mathcal{U}(\mathfrak{a})_i$, followed by the logarithmic map in $(\mathcal{U}(\mathfrak{a}), \star)/\mathcal{U}(\mathfrak{a})_i$. Note that here we identify $\mathfrak{a}$ with its image in $\hat{\mathcal{U}}(\mathfrak{a})$. The resulting skew brace is then $(\mathfrak{a}, \cdot, \circ)$ where

$$\begin{aligned} a \cdot b &= \mathrm{BCH}(a, b), \\ a \circ b &= a \cdot \exp(\mathcal{L}_{\Omega(a)})(b). \end{aligned}$$

We claim that this is precisely the one obtained in Theorem 8.9.5 from the post-Lie algebra $(\mathfrak{a}, \triangleright)$ and descending chain of ideals $I_i = \mathfrak{a}_i$. To see this, it is sufficient to prove that for any $a \in \mathfrak{a}$ and $i \geq 1$, the element $\log_\star \exp(a + \hat{\mathcal{U}}(\mathfrak{a})_i)$, seen in the quotient algebra $\mathcal{U}(\mathfrak{a})/\mathcal{U}(\mathfrak{a})_i$, coincides with $\Omega(a + \mathfrak{a}_i)$ with $\Omega_i$ the map associated to the post-Lie algebra $(\mathfrak{a}, \triangleright)/\mathfrak{a}_i$ as in Proposition 8.4.9.

As discussed in example Example 1.3.19, we have

$$\rho : \mathfrak{aff}(\mathfrak{a}) \to \mathrm{End}(\mathcal{U}(\mathfrak{a}), +) : (a, \delta) \mapsto \rho_{(a,\delta)},$$

where $\rho_{(a,\delta)}(b) = ab + \delta(b)$, is a homomorphism of Lie algebras. As before, we do not distinguish between a derivation of $\mathfrak{a}$ and its unique extension to a derivation of the algebra $\mathcal{U}(\mathfrak{a})$. Note that if $a \in \mathfrak{a}_i$ and $\delta \in \mathfrak{der}_f(\mathfrak{a})_i$, then also $\rho_{(a,\delta)}(b) \in \mathcal{U}(\mathfrak{a})_i$ for all $b \in \mathfrak{a}$. Therefore, $\rho$ restricts to a filtered Lie algebra homomorphism

$$\rho : \mathfrak{aff}_f(\mathfrak{a}) \to \mathrm{End}_f(\mathcal{U}(\mathfrak{a}), +) : (a, \delta) \mapsto \rho_{(a,\delta)}.$$

This then yields a homomorphism of filtered Lie algebras

$$\rho' : \mathfrak{aff}_f(\mathfrak{a})/\,\mathfrak{aff}_f(\mathfrak{a})_i \to \mathrm{End}_f(\mathcal{U}(\mathfrak{a})/\mathcal{U}(\mathfrak{a})_i) : (a,\delta) + \mathfrak{aff}_f(\mathfrak{a})_i \mapsto \rho'_{(a,\delta)+\mathfrak{aff}_f(\mathfrak{a})_i},$$

with

$$\rho'_{(a,\delta)+\mathfrak{aff}_f(\mathfrak{a})_i}(b + \mathcal{U}(\mathfrak{a})_i) = \rho_{(a,\delta)}(b) + \mathcal{U}(\mathfrak{a})_i.$$

Recall that the operation $\star$ is defined by

$$a \star b = ab + \mathcal{L}_a(b) = \rho_{(a,\mathcal{L}_a)}(b),$$

for all $a \in \mathfrak{a}$ and $b \in \mathcal{U}(\mathfrak{a})$. Working in the quotient ring $(\mathcal{U}(\mathfrak{a}), \star)/\mathcal{U}(\mathfrak{a})_i$ we then find

$$(a + \mathcal{U}(\mathfrak{a})_i) \star (b + \mathcal{U}(\mathfrak{a})_i) = \rho'_{(a,\mathcal{L}_a)+\mathfrak{aff}_f(\mathfrak{a})_i}(b + \mathcal{U}(\mathfrak{a})_i),$$

and therefore

$$\exp_\star(a + \mathcal{U}(\mathfrak{a})_i) = \exp\left(\rho'_{(a,\mathcal{L}_a)+\mathfrak{aff}_f(\mathfrak{a})_i}\right)(1).$$

Since derivations map $1$ to $0$, also

$$\exp_\star(a + \mathcal{U}(\mathfrak{a})_i) = \exp\left(\rho'_{(a,\mathcal{L}_a)+\mathfrak{aff}_f(\mathfrak{a})_i}\right)\exp\left(\rho'_{(0,-\mathcal{L}_a)+\mathfrak{aff}_f(\mathfrak{a})_i}\right)(1).$$

By Proposition 1.4.24 we find

$$\begin{aligned}\exp\left(\rho'_{(a,\mathcal{L}_a)+\mathfrak{aff}_f(\mathfrak{a})_i}\right)\exp\left(\rho'_{(0,-\mathcal{L}_a)+\mathfrak{aff}_f(\mathfrak{a})_i}\right) &= \exp\left(\rho'_{\mathrm{BCH}((a,\mathcal{L}_a)+\mathfrak{aff}_f(\mathfrak{a})_i,(0,-\mathcal{L}_a)+\mathfrak{aff}_f(\mathfrak{a})_i)}\right)\\ &= \exp\left(\rho_{(W_i(a+\mathfrak{a}_i),0)}\right),\end{aligned}$$

where $W_i$ is the map constructed on the Lazard skew brace $(\mathfrak{a}, \triangleright)/\mathfrak{a}_i$ as in Proposition 8.4.9. Putting everything together, we find

$$\exp_\star(a + \mathcal{U}(\mathfrak{a})_i) = \exp\left(\rho_{(W_i(a+\mathfrak{a}_i),0)}\right)(1) = \exp(W_i(a + \mathfrak{a}_i)),$$

which proves the claim.

*Remark* 8.9.6. Not every Lazard post-Lie algebra can be given a filtration satisfying the properties that make it a connected complete post-Lie algebra in the sense of Bai, Guo, Sheng and Tang. Indeed, in the finite dimensional case, a pre-Lie algebra admits such a filtration if and only if it is strongly nilpotent, see also Remark 8.7.10. The pre-Lie algebra given in Example 1.3.31 gives a concrete example of a left nilpotent pre-Lie algebra that is not strongly nilpotent.

# Chapter 9

# Skew braces of order $p^3$

In this chapter, we classify all skew braces of order $p^3$ for primes $p > 3$. A crucial tool here is Corollary 8.7.3, from which it follows that this classification can be achieved by first classifying $L$-nilpotent post-Lie rings of size $p^3$ and then computing their corresponding skew braces through the Lazard correspondence.

Note that this classification is not new and was achieved by Zenouz in 2018 [124, 125], albeit his classification is given in the form of generating sets of the corresponding regular subgroups of the holomorph. The author chose to include this classification in order to showcase concrete examples where the theory developed in Chapter 8 is applied and to provide a more explicit list of skew braces of order $p^3$, in the hope that they will prove useful to others.

The classification of braces of size $p^3$ was achieved by Bachiller in [9]. Puljić, Smoktunowicz and Zenouz constructed all braces on the elementary abelian group of order $p^4$, for $p > 3$, that are not right nilpotent [128]. Subsequently, Puljić proved that these are the only non-right nilpotent braces of order $p^4$ when $p > 5$ [126]. Later, in [127], Puljić constructed all strongly nilpotent post-Lie rings of order $p^4$, for $p > 5$, meaning that, modulo applying the group of flows construction, all right nilpotent braces of order $p^4$, for $p > 5^5$, are obtained. It should be noted that the very strong condition $p > 5^5$ stems from Theorem 8.7.6, since the strong nilpotency index of a brace or order $p^n$ is only bounded from above by $(n+1)^{n+1}$, see [147, Corollary 19]. However, since the conditions of Corollary 8.7.3 are less strict than those of [147, Corollary 19], the strongly nilpotent post-Lie rings described in [127] actually yield all right nilpotent braces of order $p^4$ for $p > 5$.

On a related note, regular affine actions of connected, simply connected Lie groups on $\mathbb{R}^2$ were classified by Kuiper [109]. For $\mathbb{R}^3$, the abelian group case was done by Baverman in his PhD thesis [22] and Fried and Goldman obtained the general classification of those groups where the action factors through $\mathbb{R}^3 \rtimes \mathrm{SL}_3(\mathbb{R})$ [76], this includes the general case for nilpotent groups since these always act through unipotent matrices [141, Theorem 1]. Regular affine actions of connected, simply connected nilpotent Lie groups on $\mathbb{R}^4$ were classified by Kim in [98, 99], this was done through the classification of left nilpotent pre-Lie algebras.

For regular affine actions on non-abelian Lie groups, less explicit classification results are known. Let us say that a pair $(G, N)$, with $G, N$ connected, simply connected Lie groups, is *admissible* if there exists a regular affine action of $G$ on $N$, or equivalently, if there exists a skew Lie brace $(A, \cdot, \circ)$ with $(A, \cdot)$ isomorphic to $N$ and $(A, \circ)$ isomorphic to $G$. Since $N$ is homeomorphic to its corresponding Lie algebra $\mathfrak{n}$ (through the exponential map), also $G$ must be homeomorphic to $\mathfrak{n}$. Also $\mathrm{Hol}^{\infty}(N)$ has a faithful linear representation, one can for example adapt the argument in [24, Proposition 6] (see also Proposition 1.4.39) in order to conclude that the canonical faithful linear representation on $\mathcal{U}(\mathfrak{n})$ descends to a faithful linear

representation on the finite dimensional space $\mathcal{U}(\mathfrak{n})/\mathcal{U}(\mathfrak{n})_{c+1}$, with $c$ the nilpotency class of $N$. Therefore, $G$ has a faithful linear representation and it is homeomorphic to $\mathbb{R}^n$, which by [25, Proposition 5.2] implies that it is solvable. By a result of Dekimpe [69], for any solvable $G$ there exists a nilpotent $N$ such that $(G, N)$ is admissible. For $1 \leq n \leq 5$ and $G, N$ nilpotent of dimension $n$, the pair $(G, N)$ is admissible by the results in [27]. In [70], it is more generally proved which pairs $(G, N)$ with $G$ solvable and $N$ nilpotent are admissible in dimensions 3 and 4. Both of these results rely on solving the analogous question for post-Lie algebras. Further, in [26, 28, 29, 31, 32] results are obtained relating the structure of the Lie algebra $\mathfrak{a}$ and the Lie algebra $\mathfrak{a}^\circ$ for a post-Lie algebra $(\mathfrak{a}, \triangleright)$. In [32], a classification is given of all post-Lie algebra structures $(\mathfrak{a}, \triangleright)$ on the Heisenberg Lie algebra $\mathfrak{a}$ such that also $\mathfrak{a}^\circ$ is isomorphic to the Heisenberg Lie algebra, although one should note that this is not up to post-Lie algebra isomorphism.

As mentioned before, an explicit classification of braces of size $p^3$ was obtained by Bachiller. Therefore, we will restrict to skew braces with non-abelian additive groups and thus also to post-Lie rings on non-trivial (but nilpotent) Lie rings. As discussed in Examples 1.4.36 and 1.4.37 there are two such non-abelian nilpotent Lie rings of size $p^3$, corresponding through the Lazard correspondence with the two extraspecial groups of this size. The extraspecial group of exponent $p$ corresponds to the Heisenberg Lie algebra, which can be considered over any field $K$. Therefore, we give in Section 9.1 a general classification of $L$-nilpotent post-Lie algebra structures on the Heisenberg Lie algebra over an arbitrary field $K$ of characteristic different from 2, together with their automorphism groups. In Section 9.2 we classify $L$-nilpotent post-Lie ring structures on the extraspecial Lie ring of size $p^3$ and characteristic $p^2$. The classification from Section 9.1 is then used to obtain a classification of skew brace structures on the Heisenberg group over prime fields whose characteristic is not 2 or 3, and similarly also skew Lie brace structures on the real Heisenberg group. Similarly, in Section 9.4 we use the classification in Section 9.2 in order to obtain a complete classification of skew braces on the extraspecial group of size $p^3$ and exponent $p^2$ for $p > 3$. All of the obtained skew braces have underlying set $(\mathbb{Z}/p)^3$ or $\mathbb{Z}/p \times \mathbb{Z}/p^2$ and the operations are expressed as polynomial functions.

Throughout the whole section, we consider the elements of the vector space $K^n$ as column vectors. Linear endomorphisms of $K^n$ are seen as $n \times n$-matrices.

## 9.1 $L$-nilpotent post-Lie algebras on the Heisenberg Lie algebra

The following lemma is well-known for $K$ a field of characteristic 0, but holds generally over any field. We give a short proof.

**Lemma 9.1.1.** *Let $K$ be a field. Then, up to isomorphism, there exists precisely two left nilpotent pre-Lie algebras of dimension 2.*

1. *The trivial pre-Lie algebra $(K^2, \triangleright)$ where $\triangleright$ is given by*

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

   *with automorphism group $\mathrm{GL}_2(K)$.*

2. *The pre-Lie algebra $(K^2, \triangleright)$ where $\triangleright$ is given by*

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 \\ x_1 x_2 \end{pmatrix},$$

*with automorphism group*

$$\mathrm{Aut}(K^2,\triangleright) = \left\{ \begin{pmatrix} a & 0 \\ b & a^2 \end{pmatrix} \mid a,b \in K, a \neq 0 \right\}.$$

*Proof.* It is clear that the automorphism group of the trivial pre-Lie algebra on $K^2$ is $\mathrm{GL}_2(K)$. It is easily seen that also the non-trivial operation as described in 2 yields a pre-Lie algebra since (P1) and (P2) are trivially satisfied. If $\phi$ is an automorphism of this pre-Lie algebra, then it is at least of the form

$$\phi = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix},$$

for $a,b,c \in K$ with $ac \neq 0$. We find

$$\phi \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \triangleright \phi \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 \\ a^2 x_1 x_2 \end{pmatrix},$$

and

$$\phi \left( \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \right) = \begin{pmatrix} 0 \\ c x_1 x_2 \end{pmatrix},$$

which forces $c = a^2$.

Now, let us show that any non-trivial two-dimensional left nilpotent pre-Lie algebra is isomorphic to the one given in the statement. Let $(K^2,\triangleright)$ be a non-trivial left nilpotent pre-Lie algebra. Then necessarily $L^3(K^2,\triangleright) = \{0\}$ and $L^2(K^2,\triangleright) = \mathrm{Fix}(K^2,\triangleright)$ is 1-dimensional. Also, by Theorem 8.5.4 the sub-adjacent Lie algebra is nilpotent hence abelian, implying that $x \triangleright y = y \triangleright x$ for all $x,y \in K^2$. Let $e_1, e_2 \in K^2$ be a basis with $e_2 \in L^2(K^2,\triangleright)$. It follows that $e_2 \triangleright e_2 = e_1 \triangleright e_2 = e_2 \triangleright e_1 = 0$ and there exists a non-zero $a \in K$ such that $e_1 \triangleright e_1 = a e_2$. With respect to the basis $e_1, a e_2$, the pre-Lie algebra structure is then the non-trivial one given in the statement. □

Let $K$ be an arbitrary field. Recall that the Heisenberg Lie algebra is the unique nilpotent non-abelian Lie algebra of dimension 3. We will always implicitly assume it to have underlying vector space $K^3$ and Lie bracket

$$\left[ \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} \right] = \begin{pmatrix} 0 \\ 0 \\ x_1 y_2 - x_2 y_1, \end{pmatrix}. \tag{9.1}$$

The following lemma is well-known; we give a short proof for completeness' sake.

**Lemma 9.1.2.** *Let $\mathfrak{a}$ be the Heisenberg Lie algebra over a field $K$. Then*

$$\mathrm{Aut}(\mathfrak{a}) = \left\{ \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ e & f & ad-bc \end{pmatrix} \mid a,b,c,d,e,f \in K, ad-bc \neq 0 \right\}.$$

*Proof.* Let $\mathfrak{a}$ be the Heisenberg Lie algebra over a field $K$, then any automorphism $\phi$ of $\mathfrak{a}$ maps its center to itself. Therefore, a necessary condition is that $\phi$ is given by a matrix of the form

$$\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ e & f & g \end{pmatrix},$$

for some $a, b, c, d, e, f, g \in K$. We find

$$\phi\left[\begin{pmatrix}x_1\\y_1\\z_1\end{pmatrix},\begin{pmatrix}x_2\\y_2\\z_2\end{pmatrix}\right] = \phi\begin{pmatrix}0\\0\\x_1y_2-y_1x_2\end{pmatrix} = \begin{pmatrix}0\\0\\g(x_1y_2-y_1x_2)\end{pmatrix},$$

and

$$\begin{aligned}\left[\phi\begin{pmatrix}x_1\\y_1\\z_1\end{pmatrix},\phi\begin{pmatrix}x_2\\y_2\\z_2\end{pmatrix}\right] &= \left[\begin{pmatrix}ax_1+by_1\\cx_1+dy_1\\ex_1+fy_1+gz_1\end{pmatrix},\begin{pmatrix}ax_2+by_2\\cx_2+dy_2\\ex_2+fy_2+gz_2\end{pmatrix}\right]\\ &= \begin{pmatrix}0\\0\\(ax_1+by_1)(cx_2+dy_2)-(cx_1+dy_1)(ax_2+by_2)\end{pmatrix}\\ &= \begin{pmatrix}0\\0\\adx_1y_2+bcy_1x_2-bcx_1y_2-ady_1x_2\end{pmatrix}.\end{aligned}$$

Both expressions coincide precisely when $g = ad - bc$, from which the statement follows. □

**Proposition 9.1.3.** *Let $\mathfrak{a}$ be the Heisenberg Lie algebra over a field $K$ whose characteristic is different from 2.*

1. *For any $0 \neq \alpha_{31} \in K$, the operation*

$$\begin{pmatrix}x_1\\y_1\\z_1\end{pmatrix} \triangleright \begin{pmatrix}x_2\\y_2\\z_2\end{pmatrix} = \begin{pmatrix}0\\\alpha_{31}z_1x_2\\\frac{1}{2}(y_1x_2-x_1y_2)\end{pmatrix},$$

*defines a post-Lie algebra $(\mathfrak{a}, \triangleright)$ with automorphism group*

$$\mathrm{Aut}(\mathfrak{a},\triangleright) = \left\{\begin{pmatrix}(-1)^i & 0 & 0\\ c & d & 0\\ 0 & 0 & (-1)^i d\end{pmatrix} \mid c, d \in K, d \neq 0, i \in \mathbb{Z}\right\}.$$

*Two such post-Lie algebras, with parameters $\alpha_{31}$ and $\alpha'_{31}$ respectively, are isomorphic if and only if $\alpha_{31}^{-1}\alpha'_{31}$ is a square in $K$.*

2. *For any $0 \neq \alpha_{31} \in K$, the operation*

$$\begin{pmatrix}x_1\\y_1\\z_1\end{pmatrix} \triangleright \begin{pmatrix}x_2\\y_2\\z_2\end{pmatrix} = \begin{pmatrix}0\\\alpha_{31}z_1x_2\\x_1x_2+\frac{1}{2}(y_1x_2-x_1y_2)\end{pmatrix},$$

*defines a post-Lie algebra $(\mathfrak{a}, \triangleright)$ with automorphism group*

$$\mathrm{Aut}(\mathfrak{a},\triangleright) = \left\{\begin{pmatrix}(-1)^i & 0 & 0\\ c & (-1)^i & 0\\ 0 & 0 & 1\end{pmatrix} \mid c \in K, i \in \mathbb{Z}\right\}.$$

*Two such post-Lie algebras, with parameters $\alpha_{31}$ and $\alpha'_{31}$ respectively, are isomorphic if and only if $\alpha_{31}^{-1}\alpha'_{31}$ is a square in $K$.*

*All of the described post-Lie algebras are $L$-nilpotent and have a zero socle. Up to isomorphism, every $L$-nilpotent post-Lie algebra on $\mathfrak{a}$ with zero socle is contained in precisely one of the two above families.*

*Proof.* Let $K$ be a field whose characteristic is different from 2 and let $(\mathfrak{a}, \triangleright)$ be an $L$-nilpotent post-Lie algebra on the Heisenberg Lie algebra with zero socle. We consider this as a filtered post-Lie algebra with the filtration given by its $L$-series. Note that $\mathfrak{a}^\circ$ can not be abelian since otherwise

$$\{0\} \neq \mathrm{Fix}(\mathfrak{a}, \triangleright) \cap Z(\mathfrak{a}) \subseteq \mathrm{Soc}(\mathfrak{a}, \triangleright),$$

so $\{\mathfrak{a}, \mathfrak{a}\} = Z(\mathfrak{a}^\circ)$ is a subspace of dimension 1. As $\{\mathfrak{a}, \mathfrak{a}\} \subseteq \mathfrak{a}_2^\circ$ we find that $\mathfrak{a}_3 \neq 0$ since otherwise

$$\{\mathfrak{a}, \mathfrak{a}\} \triangleright \mathfrak{a} \subseteq \mathfrak{a}_2^\circ \triangleright \mathfrak{a}_1 \subseteq \mathfrak{a}_3 = \{0\},$$

which implies that the socle is non-trivial. It follows that $\dim \mathfrak{a}_2 = 2$, $\dim \mathfrak{a}_3 = 1$ and $\dim \mathfrak{a}_4 = 0$. Let $0 \neq e_2 \in Z(\mathfrak{a}^\circ)$, then $e_2$ can not be contained in $\mathfrak{a}_3$ since this would mean that $e_2 \in \mathrm{Soc}(\mathfrak{a})$. Since $\mathfrak{a}_3 \subseteq Z(\mathfrak{a})$, we can find $e_3 \in \mathfrak{a}_3$ and $e_1 \in \mathfrak{a} \setminus \mathfrak{a}_2$ such that $[e_1, e_2] = e_3$. Also, we find

$$e_1 \triangleright e_3 = e_2 \triangleright e_3 = e_3 \triangleright e_3 = 0,$$

and

$$0 = \{e_2, e_3\} = [e_2, e_3] + e_2 \triangleright e_3 - e_3 \triangleright e_2 = -e_3 \triangleright e_2.$$

Since $e_2 \in \{\mathfrak{a}, \mathfrak{a}\} = Z(\mathfrak{a}^\circ)$, we know that

$$e_3 \triangleright e_1 = e_3 \triangleright e_1 - e_1 \triangleright e_3 + [e_3, e_1] = \{e_3, e_1\} \in \{\mathfrak{a}, \mathfrak{a}\} = Ke_2.$$

Hence $e_3 \triangleright e_1 = \alpha_{31} e_2$ for some $\alpha_{31} \in K$. Since $\mathfrak{a}^\circ$ is non-abelian and $\{e_1, e_2, e_3\}$ is a basis of $\mathfrak{a}$, we find that $\alpha_{31} \neq 0$.

We know that $e_1 \triangleright e_1 = \alpha_{11} e_2 + \beta_{11} e_3$ for some $\alpha_{11}, \beta_{11} \in K$. If $\alpha_{11} \neq 0$, then by replacing $e_1$ by $e_1 - \alpha_{31}^{-1} \alpha_{11} e_3$ all of the earlier observations still hold but $e_1 \triangleright e_1 = \beta_{11} e_3$. If $\beta_{11} \neq 0$, then replacing $e_3$ by $\beta_{11} e_3$ and $e_2$ by $\beta_{11} e_2$ does also not change the earlier observations but ensures that $e_1 \triangleright e_1 = e_3$. So without loss of generality $\beta_{11} \in \{0, 1\}$. At last, we know that $e_1 \triangleright e_2 = \beta_{12} e_3$ for some $\beta_{12} \in K$ and since $e_2 \in \mathfrak{a}_2^\circ$ we find $e_2 \triangleright e_1 = \beta_{21} z$ for some $\beta_{21} \in K$ and $e_2 \triangleright e_2 = e_2 \triangleright e_1 = 0$.

Taking coordinates with respect to the basis $e_1, e_2, e_3$ we find that

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ \alpha_{31} z_1 x_2 \\ \beta_{21} y_1 x_2 + \beta_{12} x_1 y_2 + \beta_{11} x_1 x_2 \end{pmatrix}.$$

Since we have ensured that $[e_1, e_2] = e_3$, the Lie bracket with respect to this basis is still the one given in (9.1).

We now determine for which choices of parameters $\alpha_{31}, \beta_{12}, \beta_{21}, \beta_{11}$ the above operation yields a post-Lie algebra. We find

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \left[ \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix}, \begin{pmatrix} x_3 \\ y_3 \\ z_3 \end{pmatrix} \right] = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

and

$$\begin{aligned}\left[\begin{pmatrix}x_1\\y_1\\z_1\end{pmatrix}\triangleright\begin{pmatrix}x_2\\y_2\\z_2\end{pmatrix},\begin{pmatrix}x_3\\y_3\\z_3\end{pmatrix}\right] &= \left[\begin{pmatrix}0\\\alpha_{31}z_1x_2\\\beta_{21}y_1x_2+\beta_{12}x_1y_2+\beta_{11}x_1x_2\end{pmatrix},\begin{pmatrix}x_3\\y_3\\z_3\end{pmatrix}\right]\\ &= \begin{pmatrix}0\\0\\-\alpha_{31}z_1x_2x_3\end{pmatrix}\\ &= -\left[\begin{pmatrix}x_2\\y_2\\z_2\end{pmatrix},\begin{pmatrix}0\\\alpha_{31}z_1x_3\\\beta_{21}y_1x_3+\beta_{12}x_1y_3+\beta_{11}x_1x_3\end{pmatrix}\right]\\ &= -\left[\begin{pmatrix}x_2\\y_2\\z_2\end{pmatrix},\begin{pmatrix}x_1\\y_1\\z_1\end{pmatrix}\triangleright\begin{pmatrix}x_3\\y_3\\z_3\end{pmatrix}\right].\end{aligned}$$

We conclude that (P1) is satisfied independently of the choice of parameters. Also,

$$\begin{aligned}\left(\begin{pmatrix}x_1\\y_1\\z_1\end{pmatrix}\triangleright\begin{pmatrix}x_2\\y_2\\z_2\end{pmatrix}\right)\triangleright\begin{pmatrix}x_3\\y_3\\z_3\end{pmatrix} &= \begin{pmatrix}0\\\alpha_{31}z_1x_2\\\beta_{21}y_1x_2+\beta_{12}x_1y_2+\beta_{11}x_1x_2\end{pmatrix}\triangleright\begin{pmatrix}x_3\\y_3\\z_3\end{pmatrix}\\ &= \begin{pmatrix}0\\\alpha_{31}(\beta_{21}y_1x_2+\beta_{12}x_1y_2+\beta_{11}x_1x_2)x_3\\\beta_{21}\alpha_{31}z_1x_2x_3\end{pmatrix},\end{aligned}$$

and

$$\begin{pmatrix}x_1\\y_1\\z_1\end{pmatrix}\triangleright\left(\begin{pmatrix}x_2\\y_2\\z_2\end{pmatrix}\triangleright\begin{pmatrix}x_3\\y_3\\z_3\end{pmatrix}\right)=\begin{pmatrix}x_1\\y_1\\z_1\end{pmatrix}\triangleright\begin{pmatrix}0\\\alpha_{31}z_2x_3\\\beta_{21}y_2x_3+\beta_{12}x_2y_3+\beta_{11}x_2x_3\end{pmatrix}=\begin{pmatrix}0\\0\\\beta_{12}\alpha_{31}x_1z_2x_3\end{pmatrix}.$$

We find that (P2) is satisfied if and only if

$$\begin{aligned}\begin{pmatrix}0\\\alpha_{31}(x_1y_2-y_1x_2)x_3\\0\end{pmatrix} &= \begin{pmatrix}0\\-\alpha_{31}(\beta_{21}y_1x_2+\beta_{12}x_1y_2+\beta_{11}x_1x_2)x_3\\\beta_{12}\alpha_{31}x_1z_2x_3-\beta_{21}\alpha_{31}z_1x_2x_3\end{pmatrix}\\ &\quad-\begin{pmatrix}0\\-\alpha_{31}(\beta_{21}y_2x_1+\beta_{12}x_2y_1+\beta_{11}x_2x_1)x_3\\\beta_{12}\alpha_{31}x_2z_1x_3-\beta_{21}\alpha_{31}z_2x_1x_3\end{pmatrix}\\ &= \begin{pmatrix}0\\\alpha_{31}(\beta_{12}-\beta_{21})y_1x_2x_3+\alpha_{31}(\beta_{21}-\beta_{12})x_1y_2x_3\\-\alpha_{31}(\beta_{21}+\beta_{12})z_1x_2x_3+\alpha_{31}(\beta_{12}+\beta_{21})x_1z_2x_3\end{pmatrix}.\end{aligned}$$

The third components agree if and only if $\beta_{12}=-\beta_{21}$ and the second components agree if and only if $\beta_{21}-\beta_{12}=1$, or $\beta_{21}=\frac{1}{2}$. We conclude that for any choice of $0\neq\alpha_{31}\in K$, $\beta_{11}\in\{0,1\}$, the operation

$$\begin{pmatrix}x_1\\y_1\\z_1\end{pmatrix}\triangleright\begin{pmatrix}x_2\\y_2\\z_2\end{pmatrix}=\begin{pmatrix}0\\\alpha_{31}z_1x_2\\\frac{1}{2}(y_1x_2-x_1y_2)+\beta_{11}x_1x_2\end{pmatrix}.$$

yields an $L$-nilpotent post-Lie algebra with zero socle on the Heisenberg Lie algebra, and that up to isomorphism any such post-Lie algebra is of this form.

It remains to determine for which choices of parameters we obtain isomorphic post-Lie algebras. Let $(\mathfrak{a}, \triangleright)$ be the post-Lie algebra determined by parameters $\alpha_{31}, \beta_{11}$, and let $(\mathfrak{a}, \triangleright')$ be the post-Lie algebra determined by parameters $\alpha'_{31}, \beta'_{11}$. Assume that $\phi : (\mathfrak{a}, \triangleright) \to (\mathfrak{a}, \triangleright')$ is an isomorphism of post-Lie algebras. Then in particular $\phi$ is an automorphism of $\mathfrak{a}$ which maps $\mathfrak{a}_2$ to itself, so by Lemma 9.1.2 we have

$$\phi \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} ax \\ cx + dy \\ ex + fy + adz \end{pmatrix},$$

for $a, c, d, e, f \in K$ with $ad \neq 0$. We find

$$\begin{aligned} \phi \left( \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} \right) &= \phi \begin{pmatrix} 0 \\ \alpha_{31} x_1 z_2 \\ \frac{1}{2}(y_1 x_2 - x_1 y_2) + \beta_{11} x_1 x_2 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ d\alpha_{31} z_1 x_2 \\ f\alpha_{31} z_1 x_2 + ad\left(\frac{1}{2}(y_1 x_2 - x_1 y_2) + \beta_{11} x_1 x_2\right) \end{pmatrix}, \end{aligned}$$

and

$$\begin{aligned} \phi \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright' \phi \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} &= \begin{pmatrix} ax_1 \\ cx_1 + dy_1 \\ ex_1 + fy_1 + adz_1 \end{pmatrix} \triangleright' \begin{pmatrix} ax_2 \\ cx_2 + dy_2 \\ ex_2 + fy_2 + adz_2 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ \alpha'_{31}(ex_1 + fy_1 + adz_1) ax_2 \\ \frac{1}{2}((cx_1 + dy_1) ax_2 - ax_1(cx_2 + dy_2)) + \beta'_{11} a^2 x_1 x_2 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ \alpha'_{31}(ex_1 + fy_1 + adz_1) ax_2 \\ \frac{1}{2} ad(y_1 x_2 - x_1 dy_2) + \beta'_{11} a^2 x_1 x_2 \end{pmatrix}. \end{aligned}$$

Looking at the second components of these expressions, we find that they coincide if and only if $a^2 = \alpha_{31}(\alpha'_{31})^{-1}$ and $e = f = 0$. Substituting this and comparing the third components, we obtain the equality

$$\frac{1}{2} ad(y_1 x_2 - x_1 y_2) + ad\beta_{11} x_1 x_2 = \frac{1}{2} ad(y_1 x_2 - x_1 y_2) + \beta'_{11} a^2 x_1 x_2.$$

If $\beta_{11} = 1$, this forces $\beta'_{11} \neq 0$ thus $\beta'_{11} = 1$ and $d = a$. If $\beta_{11} = 0$ then it forces $\beta'_{11} = 0$ with no further restrictions on $d$. We conclude that $(\mathfrak{a}, \triangleright)$ and $(\mathfrak{a}, \triangleright')$ are isomorphic if and only if $\beta_{11} = \beta'_{11}$ and $\alpha_{31}(\alpha'_{31})^{-1}$ is a square. Also, the automorphism groups for both the case $\beta_{11} = 1$ and $\beta_{11} = 0$ follow. □

**Corollary 9.1.4.** *Let $K$ be a field of characteristic 2. Then every $L$-nilpotent post-Lie algebra on the Heisenberg Lie algebra has non-zero socle.*

*Proof.* This follows directly from the proof of Proposition 9.1.3 since the condition $2\beta_{21} = 1$ appears as a necessary condition. □

**Proposition 9.1.5.** *Let $\mathfrak{a}$ be the Heisenberg Lie algebra over a field $K$.*

1. *For any $\beta_{12} \in K$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \beta_{12}(x_1y_2 - y_1x_2) \end{pmatrix}$$

*defines a post-Lie algebra $(\mathfrak{a}, \triangleright)$ with automorphism group*

$$\mathrm{Aut}(\mathfrak{a}, \triangleright) = \left\{ \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ e & f & ad - bc \end{pmatrix} \mid a, b, c, d, e, f \in K, ad - bc \neq 0 \right\}.$$

*Different choices of $\beta_{12}$ yield non-isomorphic post-Lie algebras.*

2. *For any $\beta_{12} \neq \beta_{21} \in K$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \beta_{12}x_1y_2 - \beta_{21}y_1x_2 \end{pmatrix}$$

*defines a post-Lie algebra $(\mathfrak{a}, \triangleright)$ with automorphism group*

$$\mathrm{Aut}(\mathfrak{a}, \triangleright) = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & d & 0 \\ e & f & ad \end{pmatrix} \mid a, d, e, f \in K, ad \neq 0 \right\}.$$

*Two such post-Lie algebras, with parameters $\beta_{12}, \beta_{21}$ and $\beta'_{12}, \beta'_{21}$ respectively, are isomorphic if and only if $\{\beta_{12}, \beta_{21}\} = \{\beta'_{12}, \beta'_{21}\}$.*

3. *For any $\beta \in K$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ x_1x_2 + \beta_{12}(x_1y_2 - y_1x_2) \end{pmatrix}$$

*defines a post-Lie algebra $(\mathfrak{a}, \triangleright)$ with automorphism group*

$$\mathrm{Aut}(\mathfrak{a}, \triangleright) = \left\{ \begin{pmatrix} a & 0 & 0 \\ c & a & 0 \\ e & f & a^2 \end{pmatrix} \mid a, c, e, f \in K, a \neq 0 \right\}.$$

*Different choices of $\beta_{12}$ yield non-isomorphic post-Lie algebras.*

4. *For any $\beta_{22}, \beta_{12} \in K$ such that the equation $t^2 + \beta_{12}t + \beta_{22}$ has no solutions over $K$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ x_1x_2 + \beta_{12}x_1y_2 + \beta_{22}y_1y_2 \end{pmatrix}$$

*defines a post-Lie algebra $(\mathfrak{a}, \triangleright)$ with automorphism group*

$$\mathrm{Aut}(\mathfrak{a}, \triangleright) = \left\{ \begin{pmatrix} a & -c\beta_{22} & 0 \\ c & a + c\beta_{12} & 0 \\ e & f & a^2 + ac\beta_{12} + c^2\beta_{22} \end{pmatrix} \mid a, c, e, f \in K \right\}.$$

*Different choices of $\beta_{12}, \beta_{22}$ yield non-isomorphic post-Lie algebras.*

*All of the described post-Lie algebras are $L$-nilpotent, have a non-zero socle, and their retract is a trivial post-Lie algebra. Up to isomorphism, every post-Lie algebra $(\mathfrak{a}, \triangleright)$ with these properties is contained in precisely one of the above families.*

*Proof.* Let $\mathfrak{a}$ be the Heisenberg Lie algebra over $K$ and let $(\mathfrak{a}, \triangleright)$ be an $L$-nilpotent post-Lie algebra with non-zero socle such that $(\mathfrak{a}, \triangleright)/\operatorname{Soc}(\mathfrak{a}, \triangleright)$ is a trivial post-Lie algebra. Since the socle is contained in $Z(\mathfrak{a})$, we know that its dimension is 1. The $L$-nilpotency of $(\mathfrak{a}, \triangleright)$ implies that $\mathfrak{a} \triangleright \operatorname{Soc}(\mathfrak{a}, \triangleright)$ is a strict subspace of $\operatorname{Soc}(\mathfrak{a}, \triangleright)$ and thus $\mathfrak{a} \triangleright \operatorname{Soc}(\mathfrak{a}, \triangleright) = \{0\}$. It follows that $\operatorname{Soc}(\mathfrak{a}, \triangleright) = \operatorname{Ann}(\mathfrak{a}, \triangleright)$. Let $e_1, e_2, e_3$ be a basis of $\mathfrak{a}$ such that $[e_1, e_2] = e_3$. With respect to this basis, the operation $\triangleright$ is necessarily given by

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \beta_{11}x_1x_2 + \beta_{12}x_1y_2 - \beta_{21}y_1x_2 + \beta_{22}y_1y_2 \end{pmatrix},$$

for some $\beta_{11}, \beta_{12}, \beta_{21}, \beta_{22} \in K$. Note that the minus sign in front of the term $\beta_{21}y_1x_2$ is deliberate; the reason for this will become clear later in the proof. In this case, since $[\mathfrak{a}, \mathfrak{a}] = \operatorname{Ann}(\mathfrak{a}) = L^2(\mathfrak{a})$, both (P1) and (P2) trivially hold. We now distinguish different disjoint cases:

1. $(\mathfrak{a}, \triangleright)$ **is square-free**: In this case we know that $\beta_{11} = \beta_{22} = 0$ since $e_1 \triangleright e_1 = e_2 \triangleright e_2 = 0$ and $\beta_{21} = \beta_{12}$ since also $(e_1 + e_2) \triangleright (e_1 + e_2) = 0$. We find that

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \beta_{12} \left[ \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} \right],$$

   hence $\beta_{12}$ is an invariant of the post-Lie algebra. It also follows that every automorphism of the Lie algebra $\mathfrak{a}$ is also an automorphism of $(\mathfrak{a}, \triangleright)$.

2. $(\mathfrak{a}, \triangleright)$ **is not square-free but is generated (as a vector space) by its square-free elements**: Without loss of generality, $\beta_{11} = \beta_{22} = 0$. Note that $\beta_{21} \neq \beta_{12}$ since otherwise we are in the previous case. Also, for all $a, b, c \in K$:

$$(ae_1 + be_2 + ce_3) \triangleright (ae_1 + be_2 + ce_3) = ab(\beta_{12} + \beta_{21}),$$

   hence the set of square-free elements is $(Ke_1 + Ke_3) \cup (Ke_2 + Ke_3)$. Moreover, the set $\{\beta_{12}, \beta_{21}\}$ is an invariant of $(\mathfrak{a}, \triangleright)$ since it is precisely the set

$$\{\beta \in K \mid \text{ there exists some } a \in \mathfrak{a} \setminus \operatorname{Soc}(\mathfrak{a}, \triangleright) \text{ such that } a \triangleright b = \beta[a, b] \text{ for all } b \in \mathfrak{a}\}.$$

   On the other hand, by swapping $e_1$ and $e_2$, also the roles of $\beta_{12}$ and $\beta_{21}$ swap. We therefore conclude that up to isomorphism $(\mathfrak{a}, \triangleright)$ is given by

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \beta_{12}x_1y_2 - \beta_{21}y_1x_2 \end{pmatrix},$$

   for a unique choice of two-element subset $\{\beta_{12}, \beta_{21}\} \subseteq K$.

   Since

$$Ke_1 + Ke_3 = \{a \in \mathfrak{a} \mid a \triangleright b = \beta_{12}[a, b]\},$$

and

$$Ke_2 + Ke_3 = \{a \in \mathfrak{a} \mid a \triangleright b = \beta_{21}[a, b]\},$$

any automorphism $\phi$ of $(\mathfrak{a}, \triangleright)$ maps $Ke_1 + Ke_3$ and $Ke_2 + Ke_3$ into themselves and is therefore of the form

$$\phi \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} ax \\ dy \\ ex + fy + adx \end{pmatrix},$$

where $a, d, e, f \in K$ and $ad \neq 0$. We find

$$\phi \left( \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} \right) = \begin{pmatrix} 0 \\ 0 \\ ad(\beta_{12} x_1 y_2 - \beta_{21} y_1 x_2) \end{pmatrix},$$

and

$$\begin{aligned} \phi \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \phi \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} &= \begin{pmatrix} ax_1 \\ dy_1 \\ ex_1 + fy_1 + adx_1 \end{pmatrix} \triangleright \begin{pmatrix} ax_2 \\ dy_2 \\ ex_2 + fy_2 + adx_2 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 0 \\ \beta_{12} adx_1 y_2 - \beta_{21} ady_1 x_2 \end{pmatrix}. \end{aligned}$$

We conclude that

$$\mathrm{Aut}(\mathfrak{a}, \triangleright) = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & d & 0 \\ e & f & ad \end{pmatrix} \mid a, d, e, f \in K, ad \neq 0 \right\}.$$

3. **The square-free elements of $(\mathfrak{a}, \triangleright)$ generate a subspace of dimension 2**: Without loss of generality, we may assume that $e_1$ is not square-free but $e_2$ is square-free, meaning that $\beta_{11} \neq 0$ and $\beta_{22} = 0$. If $\beta_{12} \neq \beta_{21}$, then

$$\begin{aligned} &(e_1 - (\beta_{12} - \beta_{21})^{-1} e_2) \triangleright (e_1 - (\beta_{12} - \beta_{21})^{-1} e_2) \\ &\quad = e_3 - (\beta_{12} - \beta_{21})^{-1} \beta_{12} e_3 + (\beta_{12} - \beta_{21})^{-1} \beta_{21} e_3 \\ &\quad = 0, \end{aligned}$$

which contradicts the assumption on the square-free elements. Therefore, $\beta_{12} = \beta_{21}$. With respect to the basis $e_1, \beta_{11} e_2, \beta_{11} e_3$ we find that the operation is given by

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ x_1 x_2 + \beta_{12}(x_1 y_2 - y_1 x_2) \end{pmatrix},$$

for some $\beta_{12} \in K$. Moreover, $\beta_{12}$ is characteristic since it is the unique element satisfying $a \triangleright b = \beta_{12}[a, b]$ for all $a, b \in \mathfrak{a}$ with $b \triangleright b = 0$.

By Lemma 9.1.2, combined with the fact that the square-free elements are precisely the subspace spanned by $e_2$ and $e_3$, we know that any automorphism $\phi$ of $(\mathfrak{a}, \triangleright)$ is of the form

$$\phi \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} ax \\ cx + dy \\ ex + fy + adx \end{pmatrix},$$

where $a, c, d, e, f \in K$ and $ad \neq 0$. For such a map $\phi$ we find

$$\phi \left( \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} \right) = \begin{pmatrix} 0 \\ 0 \\ ad(x_1x_2 + \beta_{12}(x_1y_2 - y_1x_2)) \end{pmatrix},$$

and

$$\begin{aligned} \phi \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \phi \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} &= \begin{pmatrix} ax_1 \\ cx_1 + dy_1 \\ ex_1 + fy_1 + adx_1 \end{pmatrix} \triangleright \begin{pmatrix} ax_2 \\ cx_2 + dy_2 \\ ex_2 + fy_2 + adx_2 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 0 \\ a^2x_1x_2 + \beta_{12}a(x_1(cx_2 + dy_2) - (cx_1 + dy_1)x_2) \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 0 \\ a^2x_1x_2 + \beta_{12}ad(x_1y_2 - y_1x_2) \end{pmatrix}. \end{aligned}$$

We conclude that $\phi$ is an automorphism if and only if $a = d$ and thus

$$\mathrm{Aut}(\mathfrak{a}, \triangleright) = \left\{ \begin{pmatrix} a & 0 & 0 \\ c & a & 0 \\ e & f & a^2 \end{pmatrix} \mid a, c, e, f \in K, a \neq 0 \right\}.$$

4. **The only square-free elements are those contained in** $\mathrm{Soc}(\mathfrak{a}, \triangleright)$: In this case, both $\beta_{11}$ and $\beta_{22}$ are non-zero. Consider the basis $e_1' = e_1$, $e_2' = \beta_{11}e_2 - \beta_{21}e_1$, $e_3' = \beta_{11}e_3$. Then still $[e_1', e_2'] = e_3'$ but also

$$e_2' \triangleright e_1' = \beta_{11}\beta_{21}e_3 - \beta_{21}\beta_{11}e_3 = 0,$$

and $e_1' \triangleright e_1' = e_3'$. We can therefore assume that $(\mathfrak{a}, \triangleright)$ is of the form

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ x_1x_2 + \beta_{12}x_1y_2 + \beta_{22}y_1y_2 \end{pmatrix},$$

for $\beta_{12}, \beta_{22} \in K$ and $\beta_{22} \neq 0$. Such a post-Lie algebra contains a square-free element that is not contained in the socle if and only if the equation $t^2 + \beta_{12}t + \beta_{22} = 0$ has a solution, since $(e_1' + te_2') \triangleright (e_1' + te_2') = t^2 + \beta_{12}t + \beta_{22}e_3$.

Let $(\mathfrak{a}, \triangleright)$ and $(\mathfrak{a}, \triangleright')$ be two such post-Lie algebras with parameters $\beta_{12}, \beta_{22}$ and $\beta_{12}', \beta_{22}'$ respectively. We determine when $\phi \in \mathrm{Aut}(\mathfrak{a})$ yields an isomorphism $\phi : (\mathfrak{a}, \triangleright) \to (\mathfrak{a}, \triangleright')$. By Lemma 9.1.2 we know that

$$\phi \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \\ ex + fy + (ad - bc)x \end{pmatrix},$$

where $a, b, c, d, e, f \in K$ with $ad - bc \neq 0$. We compute

$$\phi\left(\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix}\right) = \begin{pmatrix} 0 \\ 0 \\ (ad-bc)(x_1x_2 + \beta_{12}x_1y_2 + \beta_{22}y_1y_2) \end{pmatrix},$$

and

$$\begin{aligned}\phi\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright' \phi\begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} &= \begin{pmatrix} ax_1 + by_1 \\ cx_1 + dy_1 \\ ex_1 + fy_1 + (ad-bc)x_1 \end{pmatrix} \triangleright' \begin{pmatrix} ax_2 + by_2 \\ cx_2 + dy_2 \\ ex_2 + fy_2 + (ad-bc)x_2 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 0 \\ (ax_1+by_1)(ax_2+by_2) + \beta'_{12}(ax_1+by_1)(cx_2+dy_2) + \beta'_{22}(cx_1+dy_1)(cx_2+dy_2) \end{pmatrix}.\end{aligned}$$

Comparing the coefficients of $y_1x_2$, $x_1y_2$, $x_1x_2$ and $y_1y_2$ we find the system of equations

$$\begin{cases} 0 = ab + bc\beta'_{12} + cd\beta'_{22} \\ (ad-bc)\beta_{12} = ab + ad\beta'_{12} + cd\beta'_{22} \\ ad - bc = a^2 + ac\beta'_{12} + c^2\beta'_{22} \\ (ad-bc)\beta_{22} = b^2 + bd\beta'_{12} + d^2\beta'_{22} \end{cases}$$

From the first two equations we obtain $(ad - bc)\beta_{12} = (ad - bc)\beta'_{12}$ thus $\beta_{12} = \beta'_{12}$.

If $c = 0$, then from the first equation we get $ab = 0$, hence $b = 0$ since otherwise this would contradict the condition $ad - bc \neq 0$. The third and fourth equation reduce to $ad = a^2$ and $ad\beta_{22} = d^2\beta'_{22}$, hence $a = d$ and $\beta_{22} = \beta'_{22}$.

Next, assume that $c \neq 0$. Note that all equations are quadratic in $a, b, c, d$. This means that if we find a solution $(a, b, c, d)$, then also $(\kappa a, \kappa b, \kappa c, \kappa d)$ is a valid solution for $\kappa \in K$. Therefore, we can search for solutions with $c = 1$ and subsequently rescale them to obtain all solutions with $c \neq 0$. We can use the first equation and solve to $d$ to obtain

$$d = -\frac{b(a + \beta_{12})}{\beta'_{22}}.$$

Note that this implies

$$ad - b = -b\frac{a^2 + a\beta_{12} + \beta'_{22}}{\beta'_{22}}.$$

Substituting this into the third equation, we find

$$-b\left(\frac{a^2 + a\beta_{12} + a\beta'_{22}}{\beta'_{22}}\right) = a^2 + a\beta_{12} + \beta'_{22},$$

and thus, using $ad - b \neq 0$, we find $b = -\beta'_{22}$ and thus $d = a + \beta_{12}$. Substituting the expressions for $b$ and $d$ in the last equation we then obtain

$$\begin{aligned}\beta_{22}(a^2 + a\beta_{12} + \beta'_{22}) &= (\beta'_{22})^2 - \beta'_{22}(a + \beta_{12})\beta_{12} + (a + \beta_{12})^2\beta'_{22} \\ &= \beta'_{22}(\beta'_{22} + a\beta_{12} + a^2).\end{aligned}$$

Since $\beta'_{22} + a\beta_{12} + a^2 = ad - b \neq 0$, we conclude that $\beta_{22} = \beta'_{22}$. Therefore, after rescaling, we find that if $c \neq 0$ then the system of equations is equivalent to

$$\begin{cases} \beta_{12} = \beta'_{12} \\ \beta_{22} = \beta'_{22} \\ b = -c\beta_{22} \\ d = a + c\beta_{12} \end{cases}.$$

If we allow $c = 0$ then we obtain the solutions obtained earlier. We conclude that $\beta_{12}, \beta_{22}$ are invariants and

$$\mathrm{Aut}(\mathfrak{a}, \triangleright) = \left\{ \begin{pmatrix} a & -c\beta_{22} & 0 \\ c & a + c\beta_{12} & 0 \\ e & f & a^2 + ac\beta_{12} + c^2\beta_{22} \end{pmatrix} \mid a, c, e, f \in K \right\}.$$

Note that we do not need an assumption on the parameters $a, c, e, f$ in order to guarantee invertibility of the matrices, since we are working under the assumption that $t^2 + t\beta_{12} + \beta_2 2$ has no solutions over $K$. □

**Proposition 9.1.6.** *Let $\mathfrak{a}$ be the Heisenberg Lie algebra over a field $K$. For any $\beta_{12}, \beta_{21} \in K$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ x_1x_2 \\ \beta_{12}x_1y_2 + \beta_{21}y_1x_2 \end{pmatrix}$$

*defines a post-Lie algebra with*

$$\mathrm{Aut}(\mathfrak{a}, \triangleright) = \left\{ \begin{pmatrix} a & 0 & 0 \\ c & a^2 & 0 \\ e & ac(\beta_{12} + \beta_{21}) & a^3 \end{pmatrix} \mid a, c, e \in K, a \neq 0 \right\}.$$

*All of these post-Lie algebras $(\mathfrak{a}, \triangleright)$ are $L$-nilpotent, have a non-zero socle, and their retract is not a trivial post-Lie algebra. Every post-Lie algebra with these properties is isomorphic to one of the above post-Lie algebras for a unique choice of parameters $\beta_{12}, \beta_{21} \in K$.*

*Proof.* Let $\mathfrak{a}$ be the Heisenberg Lie algebra on $K$ and let $(\mathfrak{a}, \triangleright)$ be an $L$-nilpotent post-Lie algebra with non-zero socle such that its retract $(\mathfrak{a}, \triangleright)/\operatorname{Soc}(\mathfrak{a}, \triangleright)$ is non-trivial. Similar to the proof of Proposition 9.1.5, we find $[\mathfrak{a}, \mathfrak{a}] = Z(\mathfrak{a}) = \mathrm{Ann}(\mathfrak{a}, \triangleright)$. Combining this with Lemma 9.1.1, we know that we can find a basis $e_1, e_2, e_3$ of $\mathfrak{a}$ such that $[e_1, e_2] = e_3$ and such that the operation $\triangleright$ with respect to this basis is given by

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ x_1x_2 \\ \beta_{11}x_1x_2 + \beta_{12}x_1y_2 + \beta_{21}y_1x_2 + \beta_{22}y_1y_2 \end{pmatrix},$$

for some $\beta_{11}, \beta_{12}, \beta_{21}, \beta_{22} \in K$. If $\beta_{11} \neq 0$, then we can instead consider the basis $e_1, e'_2 := e_2 + \beta_{11}e_3, e_3$ over which $e_1 \triangleright e_1 = e'_2$ hence we can assume that $\beta_{11} = 0$.

We find that (P1) is trivially satisfied since all terms equal 0. We find

$$\begin{aligned}\left(\begin{pmatrix}x_1\\y_1\\z_1\end{pmatrix}\triangleright\begin{pmatrix}x_2\\y_2\\z_2\end{pmatrix}\right)\triangleright\begin{pmatrix}x_3\\y_3\\z_3\end{pmatrix} &= \begin{pmatrix}0\\x_1x_2\\\beta_{12}x_1y_2+\beta_{21}y_1x_2+\beta_{22}y_1y_2\end{pmatrix}\triangleright\begin{pmatrix}x_3\\y_3\\z_3\end{pmatrix}\\ &= \begin{pmatrix}0\\0\\\beta_{21}x_1x_2x_3+\beta_{22}x_1x_2y_3\end{pmatrix},\end{aligned}$$

and

$$\begin{aligned}\begin{pmatrix}x_1\\y_1\\z_1\end{pmatrix}\triangleright\left(\begin{pmatrix}x_2\\y_2\\z_2\end{pmatrix}\triangleright\begin{pmatrix}x_3\\y_3\\z_3\end{pmatrix}\right) &= \begin{pmatrix}x_1\\y_1\\z_1\end{pmatrix}\triangleright\begin{pmatrix}0\\x_2x_3\\\beta_{12}x_2y_3+\beta_{21}y_2x_3+\beta_{22}y_2y_3\end{pmatrix}\\ &= \begin{pmatrix}0\\0\\\beta_{12}x_1x_2x_3+\beta_{22}y_1x_2x_3\end{pmatrix}.\end{aligned}$$

Therefore, (P2) is satisfied if and only if

$$\beta_{22}y_1x_2x_3 = \beta_{22}y_2x_1x_3,$$

which holds if and only if $\beta_{22}=0$. Now let $(\mathfrak{a},\triangleright)$ and $(\mathfrak{a},\triangleright')$ be post-Lie algebras given by the parameters $\beta_{12},\beta_{21}$ and $\beta'_{12},\beta'_{21}$ respectively. We will study when an automorphism of $\mathfrak{a}$ is an isomorphism $\phi:(\mathfrak{a},\triangleright)\to(\mathfrak{a},\triangleright')$. Since necessarily $\phi(L^2(\mathfrak{a}))=L^2(\mathfrak{a})$, it follows from Lemma 9.1.2 that

$$\phi\begin{pmatrix}x\\y\\z\end{pmatrix} = \begin{pmatrix}ax\\cx+dy\\ex+fy+adz\end{pmatrix},$$

for $a,c,d,e,f\in K$ and $ad\neq 0$. We now compute

$$\phi\left(\begin{pmatrix}x_1\\y_1\\z_1\end{pmatrix}\triangleright\begin{pmatrix}x_2\\y_2\\z_2\end{pmatrix}\right) = \phi\begin{pmatrix}0\\x_1x_2\\\beta_{12}x_1y_2+\beta_{21}y_1x_2\end{pmatrix} = \begin{pmatrix}0\\dx_1x_2\\fx_1x_2+ad(\beta_{12}x_1y_2+\beta_{21}y_1x_2)\end{pmatrix},$$

and

$$\begin{aligned}\phi\begin{pmatrix}x_1\\y_1\\z_1\end{pmatrix}\triangleright'\phi\begin{pmatrix}x_2\\y_2\\z_2\end{pmatrix} &= \begin{pmatrix}ax_1\\cx_1+dy_1\\ex_1+fy_1+adz_1\end{pmatrix}\triangleright'\begin{pmatrix}ax_2\\cx_2+dy_2\\ex_2+fy_2+adz_2\end{pmatrix}\\ &= \begin{pmatrix}0\\a^2x_1x_2\\a\beta'_{12}x_1(cx_2+dy_2)+a\beta'_{21}(cx_1+dy_1)x_2\end{pmatrix}\\ &= \begin{pmatrix}0\\a^2x_1x_2\\ad(\beta'_{12}x_1y_2+\beta'_{21}y_1x_2)+ac(\beta'_{12}+\beta'_{21})x_1x_2\end{pmatrix},\end{aligned}$$

which holds if and only if $a^2 = d$, $\beta_{12} = \beta'_{12}$, $\beta_{21} = \beta'_{21}$ and $f = ac(\beta_{12} + \beta_{21})$. We therefore conclude that different choices of $\beta_{12}, \beta_{21}$ provide non-isomorphic solutions and

$$\mathrm{Aut}(\mathfrak{a}, \triangleright) = \left\{ \begin{pmatrix} a & 0 & 0 \\ c & a^2 & 0 \\ e & ac(\beta_{12} + \beta_{21}) & a^3 \end{pmatrix} \mid a, c, e \in K, a \neq 0 \right\}. \qquad \square$$

**Corollary 9.1.7.** *Let $\mathfrak{a}$ be the Heisenberg Lie algebra over $\mathbb{F}_q$, for $q$ an odd prime power. Then there are precisely $2q^2 + q + 4$ isomorphism classes of $L$-nilpotent post-Lie algebras of the form $(\mathfrak{a}, \triangleright)$. Among those, there are:*

- *4 isomorphism classes of post-Lie algebras whose socle is zero.*
- *$q^2 + q$ isomorphism classes of post-Lie algebras with non-zero socle whose retract is a trivial post-Lie algebra.*
- *$q^2$ isomorphism classes of post-Lie algebras with non-zero socle whose retract is a non-trivial post-Lie algebra.*

*Proof.* The first and third parts follow directly from Proposition 9.1.3 and Proposition 9.1.6.

For the second part, we find that the first three families described in Proposition 9.1.5 yield $q$, $\frac{q(q-1)}{2}$, and $q$ isomorphism classes respectively. Let us now determine for how many pairs $(a, b) \in \mathbb{F}_q^2$, the equation $t^2 + at + b$ has no solutions over $\mathbb{F}_q$. This equation has a solution if and only if the discriminant $a^2 - 4b$ is a square. Since by assumption 4 is invertible in $\mathbb{F}_q$, we find that for any $c \in \mathbb{F}_q$ there are precisely $q$ different pairs $(a, b)$ such that $a^2 - 4b = c$. Indeed, every choice of $a \in \mathbb{F}_q$ yields a unique $b \in \mathbb{F}_q$ such that this holds. Since $\mathbb{F}_q$ contains $\frac{q-1}{2}$ elements that are not a square, we find $\frac{q(q-1)}{2}$ choices of pairs $(a, b)$ such that the given equation has no solutions. $\square$

*Remark* 9.1.8. Let $(\mathfrak{a}, \triangleright)$ be an post-Lie algebra over $\mathbb{Q}$ and let $B = \{x_1, \ldots, x_n\}$ be a basis of $\mathfrak{a}$. Express the operations with respect to this basis and let $k$ be a common multiple of all of the denominators appearing in these expressions. Then, with respect to the basis $kB = \{kx_1, \ldots, kx_n\}$, all operations are expressible using only coefficients in $\mathbb{Z}$. This means that the $\mathbb{Z}$-linear span of $kB$, which we denote by $P$, is a post-Lie subring of $(\mathfrak{a}, \triangleright)$. For any prime $p$, we can consider the quotient $(P, \triangleright)/pK$ in order to obtain a post-Lie algebra over $\mathbb{F}_p$. It would be interesting to better understand which post-Lie algebras over $\mathbb{F}_p$ can occur in this way. Clearly, the post-Lie algebras over $\mathbb{F}_p$ in Propositions 9.1.3, 9.1.5 and 9.1.6 can all be obtained in such a way. Considering the discussion in Section 8.7.1, a better understanding of this phenomenon could help in the search for a counterexample of minimal dimension to Milnor's conjecture [120].

## 9.2 $L$-nilpotent post-Lie rings on the extraspecial Lie ring of characteristic $p^2$

Let $p$ be a prime. Recall that the extraspecial Lie ring of order $p^3$ and characteristic $p^2$ is the Lie ring on the abelian group $\mathfrak{a} = \mathbb{Z}/p \times \mathbb{Z}/p^2$ with Lie bracket

$$\left[ \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \right] = \begin{pmatrix} 0 \\ p(x_1 y_2 - y_1 x_2) \end{pmatrix}.$$

Any group endomorphism $\phi$ of $\mathbb{Z}/p \times \mathbb{Z}/p^2$ is of the form

$$f\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ pcx + dy \end{pmatrix},$$

where $a, b, c \in \mathbb{Z}/p$ and $d \in \mathbb{Z}/p^2$, note that $pc$ is indeed a well-defined element in $\mathbb{Z}/p^2$. We denote such an endomorphism by the matrix

$$\begin{pmatrix} a & b \\ pc & d \end{pmatrix}.$$

Such an endomorphism is bijective if it induces a bijection modulo $p$, meaning that $ad \not\equiv 0 \mod p$. Recall that we use the notation $(\mathbb{Z}/p^2)^\times$ for the set of invertible elements of the ring $\mathbb{Z}/p^2$.

**Lemma 9.2.1.** *Let $\mathfrak{a}$ be the extraspecial Lie ring of size $p^3$ and characteristic $p^2$. Then*

$$\mathrm{Aut}(\mathfrak{a}) = \left\{ \begin{pmatrix} 1 & b \\ pc & d \end{pmatrix} \mid b, c \in \mathbb{Z}/p, d \in (\mathbb{Z}/p^2)^\times \right\}.$$

*Proof.* Let $\phi$ be an automorphism of the group $(\mathfrak{a}, +)$, so given as above with $a, b, c \in \mathbb{Z}/p$, $d \in \mathbb{Z}/p^2$ and $ad \neq 0$ modulo $p$. For it to be an automorphism of the Lie ring $\mathfrak{a}$, we need that

$$\phi\left[\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}\right] = \begin{pmatrix} 0 \\ dp(x_1y_2 - y_1x_2) \end{pmatrix}$$

is equal to

$$\begin{aligned} \left[\phi\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \phi\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}\right] &= \left[\begin{pmatrix} ax_1 + by_1 \\ pcx_1 + dy_1 \end{pmatrix}, \begin{pmatrix} ax_2 + by_2 \\ pcx_2 + dy_2 \end{pmatrix}\right] \\ &= \begin{pmatrix} 0 \\ p((ax_1 + by_1)(pcx_2 + dy_2) - (pcx_1 + dy_1)(ax_2 + by_2)) \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ pad(x_1y_2 - y_1x_2) \end{pmatrix}. \end{aligned}$$

This happens if and only if $a = 1$. □

**Proposition 9.2.2.** *Let $p$ be a prime and let $\mathfrak{a}$ be the extraspecial Lie ring of size $p^3$ and characteristic $p^2$.*

1. *For any $\alpha_{12} \in \mathbb{Z}/p$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 \\ p\alpha_{12}(x_1y_2 - y_1x_2) \end{pmatrix}$$

*defines a post-Lie ring $(\mathfrak{a}, \triangleright)$ with*

$$\mathrm{Aut}(\mathfrak{a}, \triangleright) = \left\{ \begin{pmatrix} 1 & b \\ cp & d \end{pmatrix} \mid b, c \in \mathbb{Z}/p, d \in (\mathbb{Z}/p^2)^\times \right\}.$$

*Different choices of $\alpha_{12}$ yield non-isomorphic post-Lie rings.*

2. *For any $\alpha_{12} \in \mathbb{Z}/p$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 \\ p(\alpha_{12}(x_1y_2 - y_1x_2) + y_1y_2) \end{pmatrix}$$

*defines a post-Lie ring $(\mathfrak{a}, \triangleright)$ with*

$$\mathrm{Aut}(\mathfrak{a}, \triangleright) = \left\{ \begin{pmatrix} 1 & b \\ cp & 1 + dp \end{pmatrix} \mid b, c, d \in \mathbb{Z}/p \right\}.$$

*Different choices of $\alpha_{12}$ yield non-isomorphic post-Lie rings.*

3. *For any $\alpha_{12} \neq \alpha_{21} \in \mathbb{Z}/p$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 \\ p(\alpha_{12}x_1y_2 - \alpha_{21}y_1x_2) \end{pmatrix}$$

*defines a post-Lie ring $(\mathfrak{a}, \triangleright)$ with*

$$\mathrm{Aut}(\mathfrak{a}, \triangleright) = \left\{ \begin{pmatrix} 1 & 0 \\ cp & 1 + pd \end{pmatrix} \mid c, d \in \mathbb{Z}/p \right\}.$$

*Different choices of $\alpha_{12}$ yield non-isomorphic post-Lie rings.*

4. *For any $\alpha_{12}, \alpha_{22} \in \mathbb{Z}/p$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 \\ p(x_1x_2 + \alpha_{12}x_1y_2 + \alpha_{22}y_1y_2) \end{pmatrix}$$

*defines a post-Lie ring $(\mathfrak{a}, \triangleright)$ with*

$$\mathrm{Aut}(\mathfrak{a}, \triangleright) = \left\{ \begin{pmatrix} 1 & 0 \\ cp & 1 + dp \end{pmatrix} \mid c, d \in \mathbb{Z}/p \right\}.$$

*Different choices of $\alpha_{12}, \alpha_{22} \in \mathbb{Z}/p$ yield non-isomorphic post-Lie rings.*

*All of the described post-Lie rings are $L$-nilpotent and satisfy the condition that $\mathfrak{a}/(p\mathfrak{a})$ is a trivial post-Lie ring. Up to isomorphism, every post-Lie ring on $\mathfrak{a}$ with these properties is contained in precisely one of the above families.*

*Proof.* Let $\mathfrak{a}$ be the extraspecial Lie ring of size $p^3$ and characteristic $p^2$, and let $(\mathfrak{a}, \triangleright)$ be an $L$-nilpotent post-Lie ring such that $(\mathfrak{a}, \triangleright)/(p\mathfrak{a})$ is a trivial post-Lie ring. Let $e_1, e_2 \in \mathfrak{a}$ be a linearly independent generating set of $(\mathfrak{a}, +)$ such that $pe_1 = p^2e_2 = 0$. We can always rescale $e_1$ in order to ensure that $[e_1, e_2] = pe_2$. With respect to this basis, we have

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 \\ p(\alpha_{11}x_1x_2 + \alpha_{12}x_1y_2 - \alpha_{21}y_1x_2 + \alpha_{22}y_1y_2) \end{pmatrix}$$

for some $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in \mathbb{Z}/p$. Axioms (P1) and (P2) hold trivially for any choice of parameters since all terms therein are $0$.

We now determine when two such post-Lie rings $(\mathfrak{a}, \triangleright)$ and $(\mathfrak{a}, \triangleright')$, determined by the parameters $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in \mathbb{Z}/p$ and $\alpha'_{11}, \alpha'_{12}, \alpha'_{21}, \alpha'_{22} \in \mathbb{Z}/p$ respectively, are isomorphic. From Lemma 9.2.1 we know that such an isomorphism $\phi : (\mathfrak{a}, \triangleright) \to (\mathfrak{a}, \triangleright')$ is necessarily of the form

$$\phi \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + by \\ cpx + dy \end{pmatrix},$$

for $b, c \in \mathbb{Z}/p$ and $d \in (\mathbb{Z}/p^2)^\times$. We compute

$$\begin{aligned} \phi\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}\right) &= \phi \begin{pmatrix} 0 \\ p(\alpha_{11}x_1x_2 + \alpha_{12}x_1y_2 - \alpha_{21}y_1x_2 + \alpha_{22}y_1y_2) \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ dp(\alpha_{11}x_1x_2 + \alpha_{12}x_1y_2 - \alpha_{21}y_1x_2 + \alpha_{22}y_1y_2) \end{pmatrix}, \end{aligned}$$

and

$$\begin{aligned} &\phi \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \triangleright' \phi \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 + by_1 \\ cpx_1 + dy_1 \end{pmatrix} \triangleright' \begin{pmatrix} x_2 + by_2 \\ cpx_2 + dy_2 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ p(\alpha'_{11}(x_1 + by_1)(x_2 + by_2) + d\alpha'_{12}(x_1 + by_1)dy_2 - \alpha'_{21}dy_1(x_2 + by_2) + d^2\alpha'_{22}y_1y_2) \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ p(\alpha'_{11}x_1x_2 + (b\alpha'_{11} + d\alpha'_{12})x_1y_2 + (b\alpha_{11} - d\alpha'_{21})y_1x_2 + (b^2\alpha'_{11} + bd\alpha'_{12} - bd\alpha'_{21} + d^2\alpha'_{22})y_1y_2) \end{pmatrix}. \end{aligned}$$

From which we obtain the following equations in $\mathbb{Z}/p$:

$$\begin{cases} d\alpha_{11} = \alpha'_{11}, \\ d\alpha_{12} = d\alpha'_{12} + b\alpha'_{11}, \\ d\alpha_{21} = d\alpha'_{21} - b\alpha'_{11}, \\ d\alpha_{22} = b^2\alpha'_{11} + bd(\alpha'_{12} - \alpha'_{21}) + d^2\alpha'_{22}. \end{cases}$$

We observe first of all that $\alpha_{11} = 0$ if and only if $\alpha'_{11} = 0$, and therefore this yields an invariant of the post-Lie ring. Let us use this invariant to consider two disjoint cases:

1. $\alpha_{11} = 0$: In this case we find that $\alpha_{12} = \alpha'_{12}$ and $\alpha_{21} = \alpha'_{21}$. We further distinguish two disjoint cases:

   (a) $\alpha_{12} = \alpha_{21}$: Under this assumption, we find that $\alpha_{22} = 0$ if and only if $\alpha'_{22} = 0$, which leads to another two disjoint subcases:

      i. $\alpha_{22} = 0$: The system of equations is trivially satisfied and the operation $\triangleright$ equals $\alpha_{12}$ times the Lie bracket, therefore $\mathrm{Aut}(\mathfrak{a}, \triangleright) = \mathrm{Aut}(\mathfrak{a})$.

      ii. $\alpha_{22} \neq 0$: We see that $d = \alpha_{22}$ and $\alpha'_{22} = 1$ yields a solution so without loss of generality, $\alpha_{22} = 1$. We find

$$\mathrm{Aut}(\mathfrak{a}, \triangleright) = \left\{ \begin{pmatrix} 1 & b \\ cp & 1 + dp \end{pmatrix} \mid b, c, d \in \mathbb{Z}/p \right\}.$$

(b) $\alpha_{12} \neq \alpha_{21}$: Since $\alpha_{12} \neq 0$ or $\alpha_{21} \neq 0$, this forces $d \equiv 1 \mod p$. Moreover, when $b = \alpha_{22}(\alpha'_{12} - \alpha'_{21})^{-1}$ and $\alpha'_{22} = 0$ we find a solution of the system of equations. Therefore we may assume that $\alpha_{22} = \alpha'_{22} = 0$, which forces $b = 0$ and we find

$$\mathrm{Aut}(\mathfrak{a}, \triangleright) = \left\{ \begin{pmatrix} 1 & 0 \\ cp & 1 + pd \end{pmatrix} \mid c, d \in \mathbb{Z}/p \right\}.$$

2. $\alpha_{11} \neq 0$: If we let $d = \alpha_{11}^{-1}$, $b = 0$, $\alpha'_{12} = \alpha_{12}$, $\alpha'_{21} = \alpha_{21}$, $\alpha'_{22} = \alpha_{11}\alpha_{22}$ and $\alpha'_{11} = 1$ then the system of equations is satisfied, so without loss of generality we may assume that $\alpha_{11} = \alpha'_{11} = 1$ which forces $d \equiv 1 \mod p$. Setting, $b = -\alpha_{21}$, $\alpha'_{21} = 0$, $\alpha'_{12} = \alpha_{12} + \alpha_{21}$ and $\alpha'_{22} = \alpha_{22} - \alpha_{21}^2 + \alpha_{21}(\alpha_{12} + \alpha_{21})$ also yields a solution, so we can moreover assume that $\alpha_{21} = \alpha'_{21} = 0$. This forces $b = 0$ and thus $\alpha_{12} = \alpha'_{12}$ and $\alpha_{22} = \alpha'_{22}$, and also we find

$$\mathrm{Aut}(\mathfrak{a}, \triangleright) = \left\{ \begin{pmatrix} 1 & 0 \\ cp & 1 + dp \end{pmatrix} \mid c, d \in \mathbb{Z}/p \right\}. \qquad \square$$

**Proposition 9.2.3.** *Let $p$ be a prime and let $\mathfrak{a}$ be the extraspecial Lie ring of size $p^3$ and characteristic $p^2$. For any $\alpha_{22}, \beta_{12}, \beta_{21} \in \mathbb{Z}/p$ with $\alpha_{22} \neq 0$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} \alpha_{22} y_1 y_2 \\ p(\beta_{12} x_1 y_2 - \beta_{21} y_1 x_2) \end{pmatrix},$$

*defines a post-Lie ring $(\mathfrak{a}, \triangleright)$ with*

$$\mathrm{Aut}(\mathfrak{a}, \triangleright) = \left\{ \begin{pmatrix} 1 & b \\ b\alpha_{22}^{-1}(\beta_{12} - \beta_{21})p & (-1)^i + dp \end{pmatrix} \mid b, d \in \mathbb{Z}/p, i \in \mathbb{Z} \right\}.$$

*Different choices of parameters $\alpha_{22}, \beta_{12}, \beta_{21} \in \mathbb{Z}/p$ and $\alpha'_{22}, \beta'_{12}, \beta'_{21} \in \mathbb{Z}/p$ yield isomorphic post-Lie rings if and only if $\beta_{12} = \beta'_{12}$, $\beta_{21} = \beta'_{21}$ and $\alpha_{22}^{-1}\alpha'_{22}$ is a square in $\mathbb{Z}/p$.*

*The above post-Lie rings are $L$-nilpotent and satisfy the condition that $(\mathfrak{a}, \triangleright)/(p\mathfrak{a})$ is a non-trivial post-Lie ring. Every post-Lie ring with these properties is isomorphic to one of the above ones.*

*Proof.* Let $\mathfrak{a}$ be the extraspecial Lie ring of size $p^3$ and characteristic $p^2$ and let $(\mathfrak{a}, \triangleright)$ be an $L$-nilpotent post-Lie ring such that $(\mathfrak{a}, \triangleright)/(p\mathfrak{a})$ is non-trivial. By Lemma 9.1.1 know that we can find a generating set $e_1, e_2$ of $(\mathfrak{a}, +)$ such that $e_2 \triangleright e_2 \in e_1 + p\mathfrak{a}$. Also, since $\mathfrak{a} \triangleright (p\mathfrak{a})$ is a strict subset of $p\mathfrak{a}$ and thus equals $\{0\}$, we find that $p\mathfrak{a}$ is contained in $\mathrm{Fix}(\mathfrak{a}, \triangleright)$. Combining these observations yields

$$0 = e_2 \triangleright (pe_2) = p(e_2 \triangleright e_2) = pe_1,$$

thus $e_1$ has order $p$. This implies that $e_2$ has order $p^2$ and that $e_1, e_2$ is a basis of $(\mathfrak{a}, +)$. If necessary we can rescale $e_1$ in order to ensure $[e_1, e_2] = pe_2$. With respect to the base $e_1, e_2$ we find that the operation $\triangleright$ is given by

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} \alpha_{22} y_1 y_2 \\ p(\beta_{11} x_1 x_2 + \beta_{12} x_1 y_2 - \beta_{21} y_1 x_2 + \beta_{22} y_1 y_2) \end{pmatrix}$$

with $\alpha_{22}, \beta_{11}, \beta_{12}, \beta_{21}, \beta_{22} \in \mathbb{Z}/p$ and $\alpha_{22} \neq 0$. We find

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \triangleright \left[ \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}, \begin{pmatrix} x_3 \\ y_3 \end{pmatrix} \right] = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

and

$$\left[\begin{pmatrix}x_1\\y_1\end{pmatrix}\triangleright\begin{pmatrix}x_2\\y_2\end{pmatrix},\begin{pmatrix}x_3\\y_3\end{pmatrix}\right]+\left[\begin{pmatrix}x_2\\y_2\end{pmatrix},\begin{pmatrix}x_1\\y_1\end{pmatrix}\triangleright\begin{pmatrix}x_3\\y_3\end{pmatrix}\right]=\begin{pmatrix}0\\p\alpha_{22}y_1y_2y_3\end{pmatrix}+\begin{pmatrix}0\\-p\alpha_{22}y_1y_2y_3\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix},$$

hence (P1) is trivially satisfied. Also

$$\begin{aligned}\left(\begin{pmatrix}x_1\\y_1\end{pmatrix}\triangleright\begin{pmatrix}x_2\\y_2\end{pmatrix}\right)\triangleright\begin{pmatrix}x_3\\y_3\end{pmatrix}&=\begin{pmatrix}\alpha_{22}y_1y_2\\p(\beta_{11}x_1x_2+\beta_{12}x_1y_2-\beta_{21}y_1x_2+\beta_{22}y_1y_2)\end{pmatrix}\triangleright\begin{pmatrix}x_3\\y_3\end{pmatrix}\\&=\begin{pmatrix}0\\p\alpha_{22}y_1y_2(\beta_{11}x_3+\beta_{12}y_3)\end{pmatrix},\end{aligned}$$

and

$$\begin{aligned}\begin{pmatrix}x_1\\y_1\end{pmatrix}\triangleright\left(\begin{pmatrix}x_2\\y_2\end{pmatrix}\triangleright\begin{pmatrix}x_3\\y_3\end{pmatrix}\right)&=\begin{pmatrix}x_1\\y_1\end{pmatrix}\triangleright\begin{pmatrix}\alpha_{22}y_2y_3\\p(\beta_{11}x_2x_3+\beta_{12}x_2y_3-\beta_{21}y_2x_3+\beta_{22}y_2y_3)\end{pmatrix}\\&=\begin{pmatrix}0\\p(\beta_{11}x_1+\beta_{21}y_1)\alpha_{22}y_2y_3\end{pmatrix},\end{aligned}$$

from which we obtain that (P2) holds if and only if the following equality holds in $\mathbb{Z}/p$:

$$(\beta_{11}x_1+\beta_{21}y_1)y_2y_3-y_1y_2(\beta_{11}x_3+\beta_{12}y_3)=(\beta_{11}x_2+\beta_{21}y_2)y_1y_3-y_1y_2(\beta_{11}x_3+\beta_{12}y_3).$$

This equation holds if and only if $\beta_{11}=0$. We now determine when two such post-Lie rings $(\mathfrak{a},\triangleright)$ and $(\mathfrak{a},\triangleright')$, determined by the parameters $\alpha_{11},\beta_{12},\beta_{21},\beta_{22}\in\mathbb{Z}/p$ and $\alpha'_{11},\beta'_{12},\beta'_{21},\beta'_{22}\in\mathbb{Z}/p$ respectively, are isomorphic. From Lemma 9.2.1 we know that such an isomorphism $\phi:(\mathfrak{a},\triangleright)\to(\mathfrak{a},\triangleright')$ is of the form

$$\phi\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}x+by\\cpx+dy\end{pmatrix},$$

for $b,c\in\mathbb{Z}/p$ and $d\in(\mathbb{Z}/p^2)^\times$. We calculate

$$\begin{aligned}\phi\left(\begin{pmatrix}x_1\\y_1\end{pmatrix}\triangleright\begin{pmatrix}x_2\\y_2\end{pmatrix}\right)&=\phi\begin{pmatrix}\alpha_{22}y_1y_2\\p(\beta_{12}x_1y_2-\beta_{21}y_1x_2+\beta_{22}y_1y_2)\end{pmatrix}\\&=\begin{pmatrix}\alpha_{22}y_1y_2\\pc\alpha_{22}y_1y_2+dp(\beta_{12}x_1y_2-\beta_{21}y_1x_2+\beta_{22}y_1y_2)\end{pmatrix},\end{aligned}$$

and

$$\begin{aligned}\phi\begin{pmatrix}x_1\\y_1\end{pmatrix}\triangleright'\phi\begin{pmatrix}x_2\\y_2\end{pmatrix}&=\begin{pmatrix}x_1+by_1\\cpx_1+dy_1\end{pmatrix}\triangleright'\begin{pmatrix}x_2+by_2\\cpx_2+dy_2\end{pmatrix}\\&=\begin{pmatrix}\alpha'_{22}d^2y_1y_2\\p(\beta'_{12}(x_1+by_1)dy_2-\beta'_{21}dy_1(x_2+by_2)+\beta'_{22}d^2y_1y_2)\end{pmatrix}\\&=\begin{pmatrix}\alpha'_{22}d^2y_1y_2\\p(d\beta'_{12}x_1y_2+d\beta'_{21}y_1x_2+(b(\beta'_{12}-\beta'_{21})+d^2\beta'_{22})y_1y_2)\end{pmatrix},\end{aligned}$$

from which we get the following system of equations in $\mathbb{Z}/p$:

$$\begin{cases}\alpha_{22}=d^2\alpha'_{22}\\ d\beta_{12}=d\beta'_{12}\\ d\beta_{21}=d\beta'_{12}\\ c\alpha_{22}+d\beta_{22}=b(\beta'_{12}-\beta'_{21})+d^2\beta'_{22}\end{cases}.$$

This immediately implies that $\beta_{12} = \beta'_{12}$ and $\beta_{21} = \beta'_{21}$. Choosing $b = 0$, $d = 1$, $c = -\alpha_{22}^{-1}\beta_{22}$, $\alpha'_{22} = \alpha_{22}$ and $\beta'_{22} = 0$ we find a solution of the system of equations. Therefore, we may assume that $\beta_{22} = \beta'_{22} = 0$. We find that up to isomorphism $(\mathfrak{a}, \triangleright)$ is of the form

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} \alpha_{22} y_1 y_2 \\ p(x_1 x_2 + \beta_{12} x_1 y_2 - \beta_{21} y_1 x_2) \end{pmatrix},$$

for $\alpha_{22}, \beta_{12}, \beta_{21} \in \mathbb{Z}/p$ with $\alpha_{22} \neq 0$. Two such post-Lie rings, with parameters $\alpha_{22}, \beta_{12}, \beta_{21} \in \mathbb{Z}/p$ and $\alpha'_{22}, \beta'_{12}, \beta'_{21} \in \mathbb{Z}/p$ respectively, are isomorphic if and only if $\beta_{12} = \beta'_{12}$, $\beta_{21} = \beta'_{21}$ and $\alpha_{22}^{-1}\alpha'_{22}$ is a square in $\mathbb{Z}/p$. Also, it follows that $\mathrm{Aut}(\mathfrak{a}, \triangleright)$ is as given in the statement. □

**Corollary 9.2.4.** *Let $p$ be a prime and let $\mathfrak{a}$ be the extraspecial Lie ring of size $p^3$ and characteristic $p^2$. Then there are precisely $4p^2 + p$ isomorphism classes of $L$-nilpotent post-Lie rings of the form $(\mathfrak{a}, \triangleright)$. Among those, there are:*

- *$2p^2 + p$ isomorphism classes of post-Lie rings such that $(\mathfrak{a}, \triangleright)/(p\mathfrak{a})$ is a trivial post-Lie ring.*
- *$2p^2$ isomorphism classes of post-Lie rings such that $(\mathfrak{a}, \triangleright)/(p\mathfrak{a})$ is a non-trivial post-Lie ring.*

*Proof.* From Proposition 9.2.2 we find $p + p + p(p-1) + p^2 = 2p^2 + 2$ isomorphism classes and from Proposition 9.2.3 we obtain $2p^2$ equivalence classes. □

## 9.3 Skew braces on the Heisenberg group

Let $K$ be a field and let $\mathfrak{a}$ be the Heisenberg Lie algebra over $K$. Recall from Example 1.4.36 that through the Lazard correspondence we obtain from $\mathfrak{a}$ the Heisenberg group $(K^3, \cdot) = \mathbf{Laz}(\mathfrak{a})$ with

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ z_1 + z_2 + \frac{1}{2}(x_1 y_2 - y_1 x_2) \end{pmatrix}. \tag{9.2}$$

**Proposition 9.3.1.** *Let $K = \mathbb{Q}$ or $K = \mathbb{F}_p$ for a prime $p > 3$ and let $(K^3, \cdot)$ be the Heisenberg group over $K$, with the operation given by* (9.2)*.*

1. *For any $0 \neq \alpha_{31} \in K$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + \alpha_{31} z_1 x_2 \\ z_1 + z_2 \end{pmatrix}$$

*defines a skew brace $(K^3, \cdot, \circ)$ with automorphism group*

$$\mathrm{Aut}(\mathfrak{a}, \triangleright) = \left\{ \begin{pmatrix} (-1)^i & 0 & 0 \\ c & d & 0 \\ 0 & 0 & (-1)^i d \end{pmatrix} \mid c, d \in K, d \neq 0, i \in \mathbb{Z} \right\}.$$

*Two such skew braces, with parameters $\alpha_{31}$ and $\alpha'_{31}$ respectively, are isomorphic if and only if $\alpha_{31}^{-1}\alpha'_{31}$ is a square in $K$.*

2. *For any $0 \neq \alpha_{31} \in K$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + \alpha_{31} z_1 x_2 - \frac{1}{2}\alpha_{31} x_1^2 x_2 \\ z_1 + z_2 + x_1 x_2 \end{pmatrix}$$

*defines a skew brace $(K^3, \cdot, \circ)$ with automorphism group*

$$\mathrm{Aut}(\mathfrak{a}, \triangleright) = \left\{ \begin{pmatrix} (-1)^i & 0 & 0 \\ c & (-1)^i & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid c \in K, i \in \mathbb{Z} \right\}.$$

*Two such skew braces, with parameters $\alpha_{31}$ and $\alpha'_{31}$ respectively, are isomorphic if and only if $\alpha_{31}^{-1}\alpha'_{31}$ is a square in $K$.*

*The socle of the described skew braces is zero and, up to isomorphism, every skew brace $(K^3, \cdot, \circ)$ with this property is contained in precisely one of the above families.*

*Proof.* Let $K = \mathbb{Q}$ or $K = \mathbb{F}_p$ for $p > 3$ and let $\mathfrak{a}$ be the Heisenberg Lie algebra over $K$. Recall that $\mathbf{Laz}(\mathfrak{a}) = (K^3, \cdot)$. Let us consider the two families of $L$-nilpotent post-Lie algebras on $\mathfrak{a}$ given in Proposition 9.1.3 and apply Proposition 8.4.9 to them, where we consider them as filtered Lie algebras with the filtration coming from their $L$-series. Note that the third term in the $L$-series is 0 for all of these post-Lie algebras, so they are indeed Lazard post-Lie algebras since 2 and 3 are invertible in $K$. It is important to remark that the isomorphisms mentioned in Proposition 9.1.3 are isomorphisms of post-Lie algebras over $K$. Since $K$ is a prime field, any additive map $f : \mathfrak{a} \to \mathfrak{a}$ is automatically also $K$-linear. Therefore, when considering post-Lie algebras over $K$, there is no distinction between isomorphisms as post-Lie rings and isomorphisms as post-Lie algebras over $K$. This means that all information about isomorphisms and automorphisms of the obtained skew braces can be directly recovered from Proposition 9.1.3. We now apply explicitly the construction described in Proposition 8.4.9.

1. Consider the post-Lie algebra $(\mathfrak{a}, \triangleright)$ with operation

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ \alpha_{31} z_1 x_2 \\ \frac{1}{2}(y_1 x_2 - x_1 y_2) \end{pmatrix},$$

for some $0 \neq \alpha_{31} \in K$. Then

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \triangleright \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ \alpha_{31} xz \\ 0 \end{pmatrix},$$

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \triangleright \left( \begin{pmatrix} x \\ y \\ z \end{pmatrix} \triangleright \begin{pmatrix} x \\ y \\ z \end{pmatrix} \right) = \begin{pmatrix} 0 \\ 0 \\ -\frac{1}{2}\alpha_{31} x^2 z \end{pmatrix},$$

and

$$\left[ \begin{pmatrix} x \\ y \\ z \end{pmatrix}, \begin{pmatrix} x \\ y \\ z \end{pmatrix} \triangleright \begin{pmatrix} x \\ y \\ z \end{pmatrix} \right] = \begin{pmatrix} 0 \\ 0 \\ \alpha_{31} x^2 z \end{pmatrix}.$$

Using (8.11) we find

$$\begin{aligned} W\begin{pmatrix}x\\y\\z\end{pmatrix} &= \begin{pmatrix}x\\y\\z\end{pmatrix} + \frac{1}{2}\left(\begin{pmatrix}x\\y\\z\end{pmatrix} \triangleright \begin{pmatrix}x\\y\\z\end{pmatrix}\right) + \frac{1}{6}\left(\begin{pmatrix}x\\y\\z\end{pmatrix} \triangleright \left(\begin{pmatrix}x\\y\\z\end{pmatrix} \triangleright \begin{pmatrix}x\\y\\z\end{pmatrix}\right)\right) \\ &\quad + \frac{1}{12}\left[\begin{pmatrix}x\\y\\z\end{pmatrix}, \begin{pmatrix}x\\y\\z\end{pmatrix} \triangleright \begin{pmatrix}x\\y\\z\end{pmatrix}\right] \\ &= \begin{pmatrix}x\\y\\z\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0\\\alpha_{31}xz\\0\end{pmatrix} + \frac{1}{6}\begin{pmatrix}0\\0\\-\frac{1}{2}\alpha_{31}x^2z\end{pmatrix} + \frac{1}{12}\begin{pmatrix}0\\0\\\alpha_{31}x^2z\end{pmatrix} \\ &= \begin{pmatrix}x\\y+\frac{1}{2}\alpha_{31}xz\\z\end{pmatrix}. \end{aligned}$$

The inverse of $W$ is given by

$$\Omega\begin{pmatrix}x\\y\\z\end{pmatrix} = \begin{pmatrix}x\\y-\frac{1}{2}\alpha_{31}xz\\z\end{pmatrix}.$$

Let $\mathcal{L}_{x,y,z}$ denote the left $\triangleright$-multiplication by $\begin{pmatrix}x\\y\\z\end{pmatrix}$, then

$$\begin{aligned} \exp(\mathcal{L}_{x_1,y_1,z_1})\begin{pmatrix}x_2\\y_2\\z_2\end{pmatrix} &= \begin{pmatrix}x_2\\y_2\\z_2\end{pmatrix} + \begin{pmatrix}0\\\alpha z_1x_2\\\frac{1}{2}(y_1x_2-x_1y_2)\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0\\0\\-\frac{1}{2}\alpha x_1z_1x_2\end{pmatrix} \\ &= \begin{pmatrix}x_2\\y_2+\alpha z_1x_2\\z_2+\frac{1}{2}(y_1x_2-x_1y_2)-\frac{1}{4}\alpha x_1z_1x_2\end{pmatrix}. \end{aligned}$$

Therefore we find $\mathbf{B}(\mathfrak{a}, \triangleright) = (K^3, \cdot, \circ)$ with

$$\begin{aligned}
\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} &= \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \cdot \exp(\mathcal{L}_{x_1, y_1 - \frac{1}{2}\alpha_{31}x_1z_1, z_1}) \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} \\
&= \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ y_2 + \alpha_{31}z_1x_2 \\ z_2 + \frac{1}{2}((y_1 - \frac{1}{2}\alpha_{31}x_1z_1)x_2 - x_1y_2) - \frac{1}{4}\alpha_{31}x_1z_1x_2 \end{pmatrix} \\
&= \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ y_2 + \alpha_{31}z_1x_2 \\ z_2 + \frac{1}{2}((y_1 - \alpha_{31}x_1z_1)x_2 - x_1y_2) \end{pmatrix} \\
&= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + \alpha_{31}z_1x_2 \\ z_1 + z_2 + \frac{1}{2}((y_1 - \alpha_{31}x_1z_1)x_2 - x_1y_2) + \frac{1}{2}(x_1(y_2 + \alpha_{31}z_1x_2) - y_1x_2) \end{pmatrix} \\
&= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + \alpha_{31}z_1x_2 \\ z_1 + z_2 \end{pmatrix}.
\end{aligned}$$

2. Now consider the operation

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ \alpha_{31}z_1x_2 \\ x_1x_2 + \frac{1}{2}(y_1x_2 - x_1y_2) \end{pmatrix},$$

for $0 \neq \alpha_{31} \in K$. We find

$$W \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 0 \\ \alpha_{31}xz \\ x^2 \end{pmatrix} + \frac{1}{6} \begin{pmatrix} 0 \\ 0 \\ -\frac{1}{2}\alpha_{31}x^2z \end{pmatrix} + \frac{1}{12} \begin{pmatrix} 0 \\ 0 \\ \alpha_{31}x^2z \end{pmatrix} = \begin{pmatrix} x \\ y + \frac{1}{2}\alpha_{31}xz \\ z + \frac{1}{2}x^2 \end{pmatrix},$$

whose inverse is given by

$$\Omega \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ y - \frac{1}{2}\alpha_{31}xz + \frac{1}{4}\alpha_{31}x^3 \\ z - \frac{1}{2}x^2 \end{pmatrix}.$$

Using the same notation as before, we find

$$\begin{aligned}
\exp(\mathcal{L}_{x_1, y_1, z_1}) \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} &= \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} + \begin{pmatrix} 0 \\ \alpha_{31}z_1x_2 \\ x_1x_2 + \frac{1}{2}(y_1x_2 - x_1y_2) \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 0 \\ 0 \\ -\alpha_{31}x_1z_1x_2 \end{pmatrix} \\
&= \begin{pmatrix} x_2 \\ y_2 + \alpha_{31}z_1x_2 \\ z_2 + x_1x_2 + \frac{1}{2}(y_1x_2 - x_1y_2) - \frac{1}{4}\alpha_{31}x_1z_1x_2 \end{pmatrix}.
\end{aligned}$$

Therefore we find that $\mathbf{B}(\mathfrak{a}, \triangleright) = (K^3, \cdot, \circ)$ is given by

$$\begin{aligned}
&\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \cdot \exp\left(\mathcal{L}_{x_1, y_1 - \frac{1}{2}\alpha_{31}x_1z_1 + \frac{1}{4}\alpha_{31}x_1^3, z_1 - \frac{1}{2}x_1^2}\right) \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} \\
&= \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ y_2 + \alpha_{31}(z_1 - \frac{1}{2}x_1^2)x_2 \\ z_2 + x_1x_2 + \frac{1}{2}((y_1 - \frac{1}{2}\alpha_{31}x_1z_1 + \frac{1}{4}\alpha_{31}x_1^3)x_2 - x_1y_2) - \frac{1}{4}\alpha_{31}x_1(z_1 - \frac{1}{2}x_1^2)x_2 \end{pmatrix} \\
&= \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ y_2 + \alpha_{31}(z_1 - \frac{1}{2}x_1^2)x_2 \\ z_2 + x_1x_2 + \frac{1}{2}(y_1x_2 - x_1y_2 - \alpha_{31}x_1z_1x_2) + \frac{1}{4}\alpha_{31}x_1^3x_2 \end{pmatrix} \\
&= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + \alpha_{31}(z_1 - \frac{1}{2}x_1^2)x_2 \\ z_1 + z_2 + x_1x_2 + \frac{1}{2}(y_1x_2 - x_1y_2 - \alpha_{31}x_1z_1x_2) + \frac{1}{4}\alpha_{31}x_1^3x_2 + \frac{1}{2}(x_1(y_2 + \alpha_{31}(z_1 - \frac{1}{2}x_1^2)x_2) - y_1x_2) \end{pmatrix} \\
&= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + \alpha_{31}z_1x_2 - \frac{1}{2}\alpha_{31}x_1^2x_2 \\ z_1 + z_2 + x_1x_2 \end{pmatrix}. \qquad \square
\end{aligned}$$

**Proposition 9.3.2.** *Let $K = \mathbb{Q}$ or $K = \mathbb{F}_p$ for $p > 2$ and let $(K^3, \cdot)$ be the Heisenberg group over $K$, with the operation given by* (9.2)*.*

1. *For any $\beta_{12} \in K$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ z_1 + z_2 + \beta_{12}(x_1y_2 - y_1x_2) \end{pmatrix}$$

*defines a skew brace $(K^3, \cdot, \circ)$ with automorphism group*

$$\mathrm{Aut}(K^3, \cdot, \circ) = \left\{ \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ e & f & ad - bc \end{pmatrix} \mid a, b, c, d, e, f \in K, ad - bc \neq 0 \right\}.$$

*Different choices of $\beta_{12}$ yield non-isomorphic skew braces.*

2. *For any $\beta_{12} \neq \beta_{21} \in K$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ z_1 + z_2 + \beta_{12}x_1y_2 - \beta_{21}y_1x_2 \end{pmatrix}$$

*defines a skew brace $(K^3, \cdot, \circ)$ with automorphism group*

$$\mathrm{Aut}(K^3, \cdot, \circ) = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & d & 0 \\ e & f & ad \end{pmatrix} \mid a, d, e, f \in K, ad \neq 0 \right\}.$$

*Two such skew braces, with parameters $\beta_{12}, \beta_{21}$ and $\beta'_{12}, \beta'_{21}$ respectively, are isomorphic if and only if $\{\beta_{12}, \beta_{21}\} = \{\beta'_{12}, \beta'_{21}\}$.*

3. *For any $\beta_{12} \in K$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ z_1 + z_2 + x_1x_2 + \beta_{12}(x_1y_2 - y_1x_2) \end{pmatrix}$$

*defines a skew brace $(K^3, \cdot, \circ)$ with automorphism group*

$$\mathrm{Aut}(K^3, \cdot, \circ) = \left\{ \begin{pmatrix} a & 0 & 0 \\ c & a & 0 \\ e & f & a^2 \end{pmatrix} \mid a, c, e, f \in K, a \neq 0 \right\}.$$

*Different choices of $\beta_{12}$ yield non-isomorphic skew braces.*

4. *For any $\beta_{22}, \beta_{12} \in K$ such that $t^2 + (\beta_{12} - \frac{1}{2})t + \beta_{22}$ has no solutions over $K$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ z_1 + z_2 + x_1x_2 + \beta_{12}x_1y_2 - \frac{1}{2}y_1x_2 + \beta_{22}y_1y_2) \end{pmatrix}$$

*defines a skew brace $(K^3, \cdot, \circ)$ with automorphism group*

$$\mathrm{Aut}(K^3, \cdot, \circ) = \left\{ \begin{pmatrix} a & -c\beta_{22} & 0 \\ c & a + c(\beta_{12} - \frac{1}{2}) & 0 \\ e & f & a^2 + a(\beta_{12} - \frac{1}{2}) + \beta_{22} \end{pmatrix} \mid a, c, e, f \in K \right\}.$$

*Different choices of $\beta_{12}, \beta_{22}$ yield non-isomorphic skew braces.*

*All of the above skew braces are L-nilpotent, have non-zero socle, and their retract is a trivial brace. Up to isomorphism, every skew brace $(K^3, \cdot, \circ)$ with these properties is contained in precisely one of the above families.*

*Proof.* Let $K = \mathbb{Q}$ or $K = \mathbb{F}_p$ for $p > 2$ and let $\mathfrak{a}$ be the Heisenberg Lie algebra over $K$. We apply Proposition 8.4.9 to the post-Lie algebras $(\mathfrak{a}, \triangleright)$ described in Proposition 9.1.5. By a similar reasoning as in Proposition 9.1.3, the isomorphisms and automorphisms can be recovered from Proposition 9.4.1. Note that we do not need to explicitly compute $W$ and $\Omega$. Since we are only interested in $\mathcal{L}_{\Omega(a)}$, it is sufficient to know $W$ and $\Omega$ modulo the socle. However, all post-Lie algebras in Proposition 9.1.5 have a trivial retract, so we know that $W$ and $\Omega$ induce the identity map on $(\mathfrak{a}, \triangleright)/\operatorname{Soc}(\mathfrak{a}, \triangleright)$. Therefore, we find $a \circ b = a \cdot \exp(\mathcal{L}_a)(b)$ for all $a, b \in \mathfrak{a}$.

1. Let

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \beta_{12}(x_1y_2 - y_1x_2) \end{pmatrix},$$

with $\beta_{12} \in K$. We find $\mathbf{B}(\mathfrak{a}, \triangleright) = (K^3, \cdot, \circ)$ with

$$\begin{aligned}\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} &= \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \cdot \exp(\mathcal{L}_{x_1,y_1,z_1}) \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ y_2 \\ z_2 + \beta_{12}(x_1y_2 - y_1x_2) \end{pmatrix} \\ &= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ z_1 + z_2 + \beta_{12}(x_1y_2 - y_1x_2) + \frac{1}{2}(x_1y_2 - y_1x_2) \end{pmatrix} \\ &= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ z_1 + z_2 + \beta'_{12}(x_1y_2 - y_1x_2) \end{pmatrix},\end{aligned}$$

where at the end we set $\beta'_{12} = \beta_{12} + \frac{1}{2}$.

2. Let

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \beta_{12}x_1y_2 - \beta_{21}y_1x_2 \end{pmatrix},$$

with $\beta_{12} \neq \beta_{21} \in K$. We find $\mathbf{B}(\mathfrak{a}, \triangleright) = (K^3, \cdot, \circ)$ with

$$\begin{aligned}\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} &= \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \cdot \exp(\mathcal{L}_{x_1,y_1,z_1}) \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ y_2 \\ z_2 + \beta_{12}x_1y_2 - \beta_{21}y_1x_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ z_1 + z_2 + \beta_{12}x_1y_2 - \beta_{21}y_1x_2 + \frac{1}{2}(x_1y_2 - y_1x_2) \end{pmatrix} \\ &= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ z_1 + z_2 + \beta'_{12}x_1y_2 - \beta'_{21}y_1x_2 \end{pmatrix},\end{aligned}$$

where at the end we set $\beta'_{12} = \beta_{12} + \frac{1}{2}$ and $\beta'_{21} = \beta_{21} + \frac{1}{2}$.

3. Let

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ x_1x_2 + \beta_{12}(x_1y_2 - y_1x_2) \end{pmatrix},$$

with $\beta_{12} \in K$. We find $\mathbf{B}(\mathfrak{a}, \triangleright) = (K^3, \cdot, \circ)$ with

$$\begin{aligned}\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} &= \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \cdot \exp(\mathcal{L}_{x_1,y_1,z_1}) \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ y_2 \\ z_2 + x_1x_2 + \beta_{12}(x_1y_2 - y_1x_2) \end{pmatrix} \\ &= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ z_1 + z_2 + x_1x_2 + \beta_{12}(x_1y_2 - y_1x_2) + \frac{1}{2}(x_1y_2 - y_1x_2) \end{pmatrix} \\ &= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ z_1 + z_2 + x_1x_2 + \beta'_{12}(x_1y_2 - y_1x_2) \end{pmatrix},\end{aligned}$$

where at the end we set $\beta'_{12} = \beta_{12} + \frac{1}{2}$.

4. Let

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ x_1x_2 + \beta_{12}x_1y_2 + \beta_{22}y_1y_2 \end{pmatrix},$$

with $\beta_{22}, \beta_{12} \in K$ such that $t^2 + \beta_{12}t + \beta_{22}$ has no solutions over $K$. We find $\mathbf{B}(\mathfrak{a}, \triangleright) = (K^3, \cdot, \circ)$ with

$$\begin{aligned}\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} &= \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \cdot \exp(\mathcal{L}_{x_1,y_1,z_1}) \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ y_2 \\ z_2 + x_1x_2 + \beta_{12}x_1y_2 + \beta_{22}y_1y_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ z_1 + z_2 + x_1x_2 + \beta_{12}x_1y_2 + \beta_{22}y_1y_2 + \frac{1}{2}(x_1y_2 - y_1x_2) \end{pmatrix} \\ &= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ z_1 + z_2 + x_1x_2 + \beta'_{12}x_1y_2 - \frac{1}{2}y_1x_2 + \beta_{22}y_1y_2) \end{pmatrix},\end{aligned}$$

where at the end we set $\beta'_{12} = \beta_{12} + \frac{1}{2}$. □

**Proposition 9.3.3.** *Let $K = \mathbb{Q}$ or $K = \mathbb{F}_p$ for a prime $p > 3$ and let $(K^3, \cdot)$ be the Heisenberg group over $K$, with the operation given by* (9.2)*. Then for any $\beta_{12}, \beta_{21} \in K$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + x_1x_2 \\ z_1 + z_2 + \beta_{12}x_1y_2 + \beta_{21}y_1x_2 + \frac{1}{2}(\beta_{12} - \beta_{21})x_1^2x_2 \end{pmatrix}$$

*defines a skew brace* $(K^3, \cdot, \circ)$ *with*

$$\mathrm{Aut}(K^3, \cdot, \circ) = \left\{ \begin{pmatrix} a & 0 & 0 \\ c & a^2 & 0 \\ e & ac(\beta_{12} + \beta_{21}) & a^3 \end{pmatrix} \mid a, c, e \in K, a \neq 0 \right\}.$$

*These skew braces are L-nilpotent, have a non-zero socle, and their retract is a non-trivial brace. Every skew brace* $(K^3, \cdot, \circ)$ *with these properties is isomorphic to one of the above ones for a unique choice of parameters* $\beta_{12}, \beta_{21} \in K$.

*Proof.* Let $K = \mathbb{Q}$ or $K = \mathbb{F}_p$ for $p > 3$ and let $\mathfrak{a}$ be the Heisenberg algebra over $K$. We consider the family of post-Lie algebra described in Proposition 9.1.6. So $(\mathfrak{a}, \triangleright)$ with

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ x_1 x_2 \\ \beta_{12} x_1 y_2 + \beta_{21} y_1 x_2 \end{pmatrix},$$

where $\beta_{12}, \beta_{21} \in K$. Similar to Proposition 9.3.2, it is sufficient to know $W$ and $\Omega$ modulo the socle. We find that the maps $W'$ and $\Omega'$ associated to $(\mathfrak{a}, \triangleright)/\operatorname{Soc}(\mathfrak{a}, \triangleright)$ are

$$W' \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 0 \\ x^2 \end{pmatrix} = \begin{pmatrix} x \\ y + \frac{1}{2} x^2 \end{pmatrix},$$

and

$$\Omega' \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y - \frac{1}{2} x^2 \end{pmatrix}.$$

It follows that $\mathbf{B}(\mathfrak{a}, \triangleright) = (\mathfrak{a}, \cdot, \circ)$ is given by

$$\begin{aligned}
\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} &= \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \cdot \exp(\mathcal{L}_{x_1, y_1 - \frac{1}{2} x_1^2, z_1}) \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} \\
&= \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \cdot \left( \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} + \begin{pmatrix} 0 \\ x_1 x_2 \\ \beta_{12} x_1 y_2 + \beta_{21} (y_1 - \frac{1}{2} x_1^2) x_2 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 0 \\ 0 \\ \beta_{12} x_1^2 x_2 \end{pmatrix} \right) \\
&= \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ y_2 + x_1 x_2 \\ z_2 + \beta_{12} x_1 y_2 + \beta_{21} (y_1 - \frac{1}{2} x_1^2) x_2 + \frac{1}{2} \beta_{12} x_1^2 x_2 \end{pmatrix} \\
&= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + x_1 x_2 \\ z_1 + z_2 + \beta_{12} x_1 y_2 + \beta_{21} (y_1 - \frac{1}{2} x_1^2) x_2 + \frac{1}{2} \beta_{12} x_1^2 x_2 + \frac{1}{2} (x_1 (y_2 + x_1 x_2) - y_1 x_2) \end{pmatrix} \\
&= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + x_1 x_2 \\ z_1 + z_2 + (\beta_{12} + \frac{1}{2}) x_1 y_2 + (\beta_{21} - \frac{1}{2}) y_1 x_2 + \frac{1}{2} (\beta_{12} - \beta_{21} + 1) x_1^2 x_2 \end{pmatrix} \\
&= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + x_1 x_2 \\ z_1 + z_2 + \beta'_{12} x_1 y_2 + \beta'_{21} y_1 x_2 + \frac{1}{2} (\beta'_{12} - \beta'_{21}) x_1^2 x_2 \end{pmatrix},
\end{aligned}$$

where in the end we set $\beta'_{12} = \beta_{12} + \frac{1}{2}$ and $\beta'_{21} = \beta_{21} - \frac{1}{2}$. □

*Remark* 9.3.4. The reason that in Propositions 9.3.1 to 9.3.3 we restrict to prime fields is such that the information of the isomorphisms can be obtained directly from the corresponding post-Lie rings. The given operations still yield skew braces for any fields of characteristic not 2 (or 3), but there is no reason that this list should be complete in this case.

**Proposition 9.3.5.** *The statements in Propositions 9.3.1 to 9.3.3 also hold for $K = \mathbb{R}$ if we change every occurrence of skew brace by skew Lie brace and thus also demand that isomorphisms and automorphisms are diffeomorphisms.*

*Proof.* Let $(\mathfrak{a}, \triangleright)$ and $(\mathfrak{a}, \triangleright')$ be post-Lie algebras over $\mathbb{R}$. The functoriality of Theorem 8.4.14 implies that post-Lie ring isomorphisms $(\mathfrak{a}, \triangleright) \to (\mathfrak{a}, \triangleright')$ coincide with skew brace isomorphisms $\mathbf{B}(\mathfrak{a}, \triangleright) \to \mathbf{B}(\mathfrak{a}, \triangleright)$. Since the manifold structures on $(\mathfrak{a}, \triangleright)$ and $\mathbf{B}(\mathfrak{a}, \triangleright)$ are identical, this correspondence restricts to those isomorphisms that are also diffeomorphisms. We already know that any post-Lie ring isomorphism $f : (\mathfrak{a}, \triangleright) \to (\mathfrak{a}, \triangleright')$ is $\mathbb{Q}$-linear, so if moreover it is a diffeomorphism then its $\mathbb{R}$-linearity follows. Conversely, it is clear that $\mathbb{R}$-linearity implies that is a diffeomorphism. □

**Theorem 9.3.6.** *Let $p > 3$ be a prime. Up to isomorphism, Propositions 9.3.1 to 9.3.3 give a complete list of skew braces whose additive group is isomorphic to the Heisenberg group of order $p^3$.*

*Proof.* Let $p > 3$ and let $A = (K^3, \cdot, \circ)$ be a skew brace of size $p^3$ with $(K^3, \cdot)$ the Heisenberg group. If $\operatorname{Soc}(A) = \{0\}$, then up to isomorphism $A$ is given in Proposition 9.3.2. If $\operatorname{Soc}(A) \neq \{0\}$ then $\operatorname{Soc}(A) = Z(K^3, \cdot)$ and $A/\operatorname{Soc}(A)$ corresponds to one of the two post-Lie rings described in Lemma 9.1.1. If $A/\operatorname{Soc}(A)$ is trivial, then up to isomorphism $A$ is given in Proposition 9.3.1 and else in Proposition 9.3.3. □

**Corollary 9.3.7.** *Let $p > 3$ be a prime. Then there are precisely $2p^2 + p + 4$ isomorphism classes of skew braces of size $p^3$ whose additive group is isomorphic to the Heisenberg group. Among those, there are:*

- *4 isomorphism classes of skew braces whose socle is zero.*
- *$p^2 + p$ isomorphism classes of skew braces with non-zero socle whose retract is a trivial skew brace.*
- *$p^2$ isomorphism classes of skew braces with non-zero socle whose retract is a non-trivial skew brace.*

## 9.4 Skew braces on the extraspecial group of exponent $p^2$

Let $p > 2$ be a prime and let $\mathfrak{a}$ be the extraspecial Lie ring of order $p^3$. Recall from Example 1.4.37 that through the Lazard correspondence we obtain the extraspecial group of order $p^3$ and exponent $p^2$. Concretely, $(\mathbb{Z}/p \times \mathbb{Z}/p^2, \cdot) = \mathbf{Laz}(\mathfrak{a})$ with

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + \frac{1}{2}p(x_1 y_2 - y_1 x_2) \end{pmatrix}. \tag{9.3}$$

**Proposition 9.4.1.** *Let $p > 2$ be a prime and let $(\mathbb{Z}/p \times \mathbb{Z}/p^2, \cdot)$ be the extraspecial group, with the operation given by* (9.3)*.*

1. *For any $\alpha_{12} \in \mathbb{Z}/p$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + p\alpha_{12}(x_1y_2 - y_1x_2) \end{pmatrix}$$

*defines a skew brace $(\mathbb{Z}/p \times \mathbb{Z}/p^2, \cdot, \circ)$ with*

$$\mathrm{Aut}(\mathbb{Z}/p \times \mathbb{Z}/p^2, \cdot, \circ) = \left\{ \begin{pmatrix} 1 & b \\ cp & d \end{pmatrix} \mid b, c \in \mathbb{Z}/p, d \in (\mathbb{Z}/p^2)^\times \right\}.$$

*Different choices of $\alpha_{12}$ yield non-isomorphic skew braces.*

2. *For any $\alpha_{12} \in \mathbb{Z}/p$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + p(\alpha_{12}(x_1y_2 - y_1x_2) + y_1y_2) \end{pmatrix}$$

*defines a skew brace $(\mathbb{Z}/p \times \mathbb{Z}/p^2, \cdot, \circ)$ with*

$$\mathrm{Aut}(\mathbb{Z}/p \times \mathbb{Z}/p^2, \cdot, \circ) = \left\{ \begin{pmatrix} 1 & b \\ cp & 1 + dp \end{pmatrix} \mid b, c, d \in \mathbb{Z}/p \right\}.$$

*Different choices of $\alpha_{12}$ yield non-isomorphic skew braces.*

3. *For any $\alpha_{12} \neq \alpha_{21} \in \mathbb{Z}/p$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + p(\alpha_{12}x_1y_2 - \alpha_{21}y_1x_2) \end{pmatrix}$$

*defines a skew brace $(\mathbb{Z}/p \times \mathbb{Z}/p^2, \cdot, \circ)$ with*

$$\mathrm{Aut}(\mathbb{Z}/p \times \mathbb{Z}/p^2, \cdot, \circ) = \left\{ \begin{pmatrix} 1 & 0 \\ cp & 1 + pd \end{pmatrix} \mid c, d \in \mathbb{Z}/p \right\}.$$

*Different choices of $\alpha_{12}$ yield non-isomorphic skew braces.*

4. *For any $\alpha_{12}, \alpha_{22} \in \mathbb{Z}/p$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + p(x_1x_2 + \alpha_{12}x_1y_2 - \frac{1}{2}y_1x_2 + \alpha_{22}y_1y_2) \end{pmatrix}$$

*defines a skew brace $(\mathbb{Z}/p \times \mathbb{Z}/p^2, \cdot, \circ)$ with*

$$\mathrm{Aut}(\mathbb{Z}/p \times \mathbb{Z}/p^2, \cdot, \circ) = \left\{ \begin{pmatrix} 1 & 0 \\ cp & 1 + dp \end{pmatrix} \mid c, d \in \mathbb{Z}/p \right\}.$$

*Different choices of $\alpha_{12}, \alpha_{22} \in \mathbb{Z}/p$ yield non-isomorphic skew braces.*

*All of the above skew braces satisfy $A^2 \subseteq Z(A, \cdot)$. Up to isomorphism, every skew brace of the form $(\mathbb{Z}/p \times \mathbb{Z}/p^2, \cdot, \circ)$ with this property is contained in precisely one of the above families.*

*Proof.* We consider the 4 families of post-Lie rings on the extraspecial Lie ring $\mathfrak{a}$ as described in Proposition 9.2.2. Note that all of the post-Lie rings $(\mathfrak{a}, \triangleright)$ considered have the property that $(\mathfrak{a}, \triangleright)/\operatorname{Soc}(\mathfrak{a}, \triangleright)$ is a trivial brace, so it follows that $a \circ b = a \cdot \mathcal{L}_{\Omega(a)}(b) = a \cdot \mathcal{L}_a(b)$ for all $a, b \in \mathfrak{a}$.

1. Let

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 \\ p\alpha_{12}(x_1y_2 - y_1x_2) \end{pmatrix},$$

with $\alpha_{12} \in \mathbb{Z}/p$. Then $\mathbf{B}(\mathfrak{a}, \triangleright) = (\mathbb{Z}/p \times \mathbb{Z}/p^2, \cdot, \circ)$ is given by

$$\begin{aligned} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} &= \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \cdot \exp\left(\mathcal{L}_{x_1,y_1}\right) \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ y_2 + p\alpha_{12}(x_1y_2 - y_1x_2) \end{pmatrix} \\ &= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + p\alpha_{12}(x_1y_2 - y_1x_2) + \frac{1}{2}p(x_1y_2 - y_1x_2) \end{pmatrix} \\ &= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + p\alpha'_{12}(x_1y_2 - y_1x_2) \end{pmatrix}, \end{aligned}$$

where in the last step we set $\alpha'_{12} = \alpha_{12} + \frac{1}{2}$.

2. Let

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 \\ p(\alpha_{12}(x_1y_2 - y_1x_2) + y_1y_2) \end{pmatrix},$$

with $\alpha_{12} \in \mathbb{Z}/p$. Then $\mathbf{B}(\mathfrak{a}, \triangleright) = (\mathbb{Z}/p \times \mathbb{Z}/p^2, \cdot, \circ)$ is given by

$$\begin{aligned} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} &= \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \cdot \exp\left(\mathcal{L}_{x_1,y_1}\right) \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ y_2 + p(\alpha_{12}(x_1y_2 - y_1x_2) + y_1y_2) \end{pmatrix} \\ &= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + p(\alpha_{12}(x_1y_2 - y_1x_2) + y_1y_2) + \frac{1}{2}p(x_1y_2 - y_1x_2) \end{pmatrix} \\ &= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + p(\alpha'_{12}(x_1y_2 - y_1x_2) + y_1y_2) \end{pmatrix}, \end{aligned}$$

where in the last step we set $\alpha'_{12} = \alpha_{12} + \frac{1}{2}$.

3. Let

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 \\ p(\alpha_{12}x_1y_2 - \alpha_{21}y_1x_2) \end{pmatrix},$$

with $\alpha_{12} \in \mathbb{Z}/p$. Then $\mathbf{B}(\mathfrak{a}, \triangleright) = (\mathbb{Z}/p \times \mathbb{Z}/p^2, \cdot, \circ)$ is given by

$$\begin{aligned}\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} &= \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \cdot \exp\left(\mathcal{L}_{x_1,y_1}\right) \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ y_2 + p(\alpha_{12} x_1 y_2 - \alpha_{21} y_1 x_2) \end{pmatrix} \\ &= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + p(\alpha_{12} x_1 y_2 - \alpha_{21} y_1 x_2) + \frac{1}{2} p(x_1 y_2 - y_1 x_2) \end{pmatrix} \\ &= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + p(\alpha'_{12} x_1 y_2 - \alpha'_{21} y_1 x_2) \end{pmatrix},\end{aligned}$$

where in the last step we set $\alpha'_{12} = \alpha_{12} + \frac{1}{2}$ and $\alpha'_{21} = \alpha_{21} + \frac{1}{2}$.

4. Let

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 \\ p(x_1 x_2 + \alpha_{12} x_1 y_2 + \alpha_{22} y_1 y_2) \end{pmatrix},$$

with $\alpha_{12} \in \mathbb{Z}/p$. Then $\mathbf{B}(\mathfrak{a}, \triangleright) = (\mathbb{Z}/p \times \mathbb{Z}/p^2, \cdot, \circ)$ is given by

$$\begin{aligned}\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} &= \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \cdot \exp\left(\mathcal{L}_{x_1,y_1}\right) \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ y_2 + p(x_1 x_2 + \alpha_{12} x_1 y_2 + \alpha_{22} y_1 y_2) \end{pmatrix} \\ &= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + p(x_1 x_2 + \alpha_{12} x_1 y_2 + \alpha_{22} y_1 y_2) + \frac{1}{2} p(x_1 y_2 - y_1 x_2) \end{pmatrix} \\ &= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + p(x_1 x_2 + (\alpha_{12} + \frac{1}{2}) x_1 y_2 - \frac{1}{2} y_1 x_2 + \alpha_{22} y_1 y_2) \end{pmatrix} \\ &= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 + p(x_1 x_2 + \alpha'_{12} x_1 y_2 - \frac{1}{2} y_1 x_2 + \alpha_{22} y_1 y_2) \end{pmatrix},\end{aligned}$$

where in the last step we set $\alpha'_{12} = \alpha_{12} + \frac{1}{2}$. □

**Proposition 9.4.2.** *Let $p > 3$ be a prime and let $(\mathbb{Z}/p \times \mathbb{Z}/p^2, \cdot)$ be the extraspecial group, with the operation given by* (9.3)*. For any $\alpha_{22}, \beta_{12}, \beta_{21} \in \mathbb{Z}/p$ with $\alpha_{22} \neq 0$, the operation*

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 + \alpha_{22} y_1 y_2 \\ y_1 + y_2 + p(\beta_{12} x_1 y_2 - \beta_{21} y_1 x_2 - \frac{1}{2}(\beta_{12} + \beta_{21}) \alpha_{22} y_1^2 y_2) \end{pmatrix}$$

*defines a skew brace $(\mathbb{Z}/p \times \mathbb{Z}/p^2, \cdot, \circ)$ with*

$$\mathrm{Aut}(\mathbb{Z}/p \times \mathbb{Z}/p^2, \cdot, \circ) = \left\{ \begin{pmatrix} 1 & b \\ b\alpha_{22}^{-1}(\beta_{12} - \beta_{21})p & 1 + dp \end{pmatrix} \mid b, d \in \mathbb{Z}/p \right\}.$$

*Different choices of parameters $\alpha_{22}, \beta_{12}, \beta_{21}$ and $\alpha'_{22}, \beta'_{12}, \beta'_{21}$ yield isomorphic skew braces if and only if $\beta_{12} = \beta'_{12}$, $\beta_{21} = \beta'_{21}$ and $\alpha_{22}^{-1}\alpha'_{22}$ is a square in $\mathbb{Z}/p$.*

*All of the above skew braces satisfy the condition that $A^2 \not\subseteq Z(A, \cdot)$ and, up to isomorphism, every skew brace $(\mathbb{Z}/p \times \mathbb{Z}/p^2, \cdot, \circ)$ with this property is isomorphic to one of the above.*

*Proof.* We apply the Lazard correspondence to the family of post-Lie rings in Proposition 9.2.3. Let $\mathfrak{a}$ be the extraspecial Lie ring of order $p^3$ and let

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \triangleright \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} \alpha_{22} y_1 y_2 \\ p(\beta_{12} x_1 y_2 - \beta_{21} y_1 x_2) \end{pmatrix},$$

with $\alpha_{22}, \beta_{12}, \beta_{21} \in \mathbb{Z}/p$ and $\alpha_{22} \neq 0$. Since $p\mathfrak{a} \subseteq \mathrm{Soc}(\mathfrak{a}, \triangleright)$, it suffices to compute $W$ and $\Omega$ modulo $p\alpha$. We find

$$W \begin{pmatrix} x \\ y \end{pmatrix} \in \begin{pmatrix} x + \frac{1}{2}\alpha_{22} y^2 \\ y \end{pmatrix} + p\mathfrak{a},$$

and

$$\Omega \begin{pmatrix} x \\ y \end{pmatrix} \in \begin{pmatrix} x - \frac{1}{2}\alpha_{22} y^2 \\ y \end{pmatrix} + p\mathfrak{a}.$$

Therefore, $\mathbf{B}(\mathfrak{a}, \triangleright) = (\mathfrak{a}, \cdot, \circ)$ is given by

$$\begin{aligned}
&\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \cdot \exp\left(\mathcal{L}_{x_1 - \frac{1}{2}\alpha_{22} y_1^2, y_1}\right) \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \\
&= \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \cdot \left( \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} + \begin{pmatrix} \alpha_{22} y_1 y_2 \\ p(\beta_{12}(x_1 - \frac{1}{2}\alpha_{22} y_1^2) y_2 - \beta_{21} y_1 x_2) \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 0 \\ -p\beta_{21}\alpha_{22} y_1^2 y_2 \end{pmatrix} \right) \\
&= \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 + \alpha_{22} y_1 y_2 \\ y_2 + p(\beta_{12}(x_1 - \frac{1}{2}\alpha_{22} y_1^2) y_2 - \beta_{21} y_1 x_2 - \frac{1}{2}\beta_{21}\alpha_{22} y_1^2 y_2) \end{pmatrix} \\
&= \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 + \alpha_{22} y_1 y_2 \\ y_2 + p(\beta_{12} x_1 y_2 - \beta_{21} y_1 x_2 - \frac{1}{2}(\beta_{12} + \beta_{21})\alpha_{22} y_1^2 y_2) \end{pmatrix} \\
&= \begin{pmatrix} x_1 + x_2 + \alpha_{22} y_1 y_2 \\ y_1 + y_2 + p(\beta_{12} x_1 y_2 - \beta_{21} y_1 x_2 - \frac{1}{2}(\beta_{12} + \beta_{21})\alpha_{22} y_1^2 y_2 + \frac{1}{2}(x_1 y_2 - y_1(x_2 + \alpha_{22} y_1 y_2))) \end{pmatrix} \\
&= \begin{pmatrix} x_1 + x_2 + \alpha_{22} y_1 y_2 \\ y_1 + y_2 + p((\beta_{12} + \frac{1}{2}) x_1 y_2 - (\beta_{21} + \frac{1}{2}) y_1 x_2 - \frac{1}{2}(\beta_{12} + \beta_{21} + 1)\alpha_{22} y_1^2 y_2) \end{pmatrix} \\
&= \begin{pmatrix} x_1 + x_2 + \alpha_{22} y_1 y_2 \\ y_1 + y_2 + p(\beta'_{12} x_1 y_2 - \beta'_{21} y_1 x_2 - \frac{1}{2}(\beta'_{12} + \beta'_{21})\alpha_{22} y_1^2 y_2) \end{pmatrix},
\end{aligned}$$

where in the last step we set $\beta'_{12} = \beta_{12} + \frac{1}{2}$ and $\beta'_{21} = \beta_{21} + \frac{1}{2}$. □

**Theorem 9.4.3.** *Let $p > 3$ be a prime. Up to isomorphism, Propositions 9.4.1 and 9.4.2 give a complete list of skew braces on the extraspecial group of order $p^3$ and exponent $p^2$.*

**Corollary 9.4.4.** *Let $p > 3$ be a prime. Then there are precisely $4p^2 + p$ isomorphism classes of skew braces of size $p^3$ whose additive group is isomorphic to the extraspecial group of exponent $p^2$. Among those, there are:*

- *$2p^2 + p$ isomorphism classes of post-Lie rings such that $A^2 \subseteq Z(A, \cdot)$.*
- *$2p^2$ isomorphism classes of post-Lie rings such that $A^2 \not\subseteq Z(A, \cdot)$.*

# Bibliography


[1] E. Acri, R. Lutowski, and L. Vendramin. Retractability of solutions to the Yang–Baxter equation and $p$-nilpotency of skew braces. *Internat. J. Algebra Comput.*, 30(1):91–115, 2020.

[2] A. A. Agrachev and R. V. Gamkrelidze. Chronological Algebras and Nonstationary Vector Fields. *J. Sov. Math.*, 17:1650–1675, 1981.

[3] J. W. Alexander and G. B. Briggs. On types of knotted curves. *Ann. of Math. (2)*, 28(1-4):562–586, 1926/27.

[4] B. Amberg and O. Dickenschied. On the adjoint group of a radical ring. *Canad. Math. Bull.*, 38(3):262–270, 1995.

[5] B. Amberg, O. Dickenschied, and Y. P. Sysak. Subgroups of the adjoint group of a radical ring. *Canad. J. Math.*, 50(1):3–15, 1998.

[6] B. Amberg and Y. P. Sysak. Radical rings with soluble adjoint groups. *J. Algebra*, 247(2):692–702, 2002.

[7] N. Andruskiewitsch and J. Devoto. Extensions of Hopf algebras. *Algebra i Analiz*, 7(1):22–61, 1995.

[8] L. Auslander. Simply transitive groups of affine motions. *Amer. J. Math.*, 99(4):809–826, 1977.

[9] D. Bachiller. Classification of braces of order $p^3$. *J. Pure Appl. Algebra*, 219(8):3568–3603, 2015.

[10] D. Bachiller. Counterexample to a conjecture about braces. *J. Algebra*, 453:160–176, 2016.

[11] D. Bachiller. Solutions of the Yang–Baxter equation associated to skew left braces, with applications to racks. *J. Knot Theory Ramifications*, 27(8):1850055, 36, 2018.

[12] D. Bachiller, F. Cedó, and E. Jespers. Solutions of the Yang–Baxter equation associated with a left brace. *J. Algebra*, 463:80–102, 2016.

[13] D. Bachiller, F. Cedó, E. Jespers, and J. Okniński. Asymmetric product of left braces and simplicity; new solutions of the Yang–Baxter equation. *Commun. Contemp. Math.*, 21(8):1850042, 30, 2019.

[14] D. Bachiller, F. Cedó, and L. Vendramin. A characterization of finite multipermutation solutions of the Yang–Baxter equation. *Publ. Mat.*, 62(2):641–649, 2018.

[15] C. Bai, L. Guo, Y. Sheng, and R. Tang. Post-groups, (Lie-)Butcher groups and the Yang–Baxter equation. *Math. Ann.*, 388(3):3127–3167, 2024.

[16] A. Ballester-Bolinches, R. Esteban-Romero, P. Jiménez-Seral, and V. Pérez-Calabuig. Soluble skew left braces and soluble solutions of the Yang–Baxter equation. *Adv. Math.*, 455:Paper No. 109880, 27, 2024.

[17] V. Bardakov and T. Nasybullov. Embeddings of quandles into groups. *J. Algebra Appl.*, 19(7):2050136, 20, 2020.

[18] V. G. Bardakov, M. V. Neshchadim, and M. K. Yadav. On $\lambda$-homomorphic skew braces. *J. Pure Appl. Algebra*, 226(6):Paper No. 106961, 37, 2022.

[19] V. G. Bardakov, M. V. Neshchadim, and M. K. Yadav. Symmetric skew braces and brace systems. *Forum Math.*, 35(3):713–738, 2023.

[20] R. J. Baxter. Partition function of the eight-vertex lattice model. *Ann. Physics*, 70:193–228, 1972.

[21] M. Bonatto and P. Jedlička. Central nilpotency of skew braces. *J. Algebra Appl.*, 22(12):Paper No. 2350255, 16, 2023.

[22] H. Braverman. *Abelian groups of two and three dimensional simple transitive affine motions*. PhD thesis, City University of New York, 1973.

[23] D. Burde. Affine structures on nilmanifolds. *Internat. J. Math.*, 7(5):599–616, 1996.

[24] D. Burde. On a refinement of Ado's theorem. *Arch. Math. (Basel)*, 70(2):118–127, 1998.

[25] D. Burde. Crystallographic actions on Lie groups and post-Lie algebra structures. *Commun. Math.*, 29(1):67–89, 2021.

[26] D. Burde and K. Dekimpe. Post-Lie algebra structures on pairs of Lie algebras. *J. Algebra*, 464:226–245, 2016.

[27] D. Burde, K. Dekimpe, and S. Deschamps. Affine actions on nilpotent Lie groups. *Forum Math.*, 21(5):921–934, 2009.

[28] D. Burde, K. Dekimpe, and M. Monadjem. Rigidity results for Lie algebras admitting a post-Lie algebra structure. *Internat. J. Algebra Comput.*, 32(8):1495–1511, 2022.

[29] D. Burde, K. Dekimpe, and M. Monadjem. Post-Lie algebra structures for perfect Lie algebras. *Comm. Algebra*, 52(10):4255–4267, 2024.

[30] D. Burde, K. Dekimpe, and K. Vercammen. Affine actions on Lie groups and post-Lie algebra structures. *Linear Algebra Appl.*, 437(5):1250–1263, 2012.

[31] D. Burde and C. Ender. Commutative post-Lie algebra structures on nilpotent Lie algebras and Poisson algebras. *Linear Algebra Appl.*, 584:107–126, 2020.

[32] D. Burde, C. Ender, and W. A. Moens. Post-Lie algebra structures for nilpotent Lie algebras. *Internat. J. Algebra Comput.*, 28(5):915–933, 2018.

[33] D. Burde and W. A. Moens. Faithful Lie algebra modules and quotients of the universal enveloping algebra. *J. Algebra*, 325:440–460, 2011.

[34] N. P. Byott. Uniqueness of Hopf galois structure for separable field extensions. *Communications in Algebra*, 24(10):3217–3228, 1996.

[35] N. P. Byott. Integral Hopf–Galois structures on degree $p^2$ extensions of $p$-adic fields. *J. Algebra*, 248(1):334–365, 2002.

[36] N. P. Byott. Hopf–Galois structures on almost cyclic field extensions of 2-power degree. *J. Algebra*, 318(1):351–371, 2007.

[37] N. P. Byott. Solubility criteria for Hopf-Galois structures. *New York J. Math.*, 21:883–903, 2015.

[38] N. P. Byott. On insoluble transitive subgroups in the holomorph of a finite soluble group. *J. Algebra*, 638:1–31, 2024.

[39] 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*, 556:1165–1210, 2020.

[40] A. Caranti. Multiple holomorphs of finite $p$-groups of class two. *J. Algebra*, 516:352–372, 2018.

[41] A. Caranti. Bi-skew braces and regular subgroups of the holomorph. *J. Algebra*, 562(July):647–665, 2020.

[42] A. Caranti and L. Stefanello. From endomorphisms to bi-skew braces, regular subgroups, the Yang–Baxter equation, and Hopf–Galois structures. *J. Algebra*, 587:462–487, 2021.

[43] A. Caranti and L. Stefanello. Brace blocks from bilinear maps and liftings of endomorphisms. *J. Algebra*, 610:831–851, 2022.

[44] M. Castelli. A characterization of finite simple set-theoretic solutions of the Yang–Baxter equation. *Proc. Amer. Math. Soc.*, 151(12):5047–5057, 2023.

[45] M. Castelli and S. Trappeniers. Studying solutions to the Yang–Baxter equation through skew braces, with an application to indecomposable involutive solutions with abelian permutation group. *arXiv:2303.00581*, 2023.

[46] F. Catino, I. Colazzo, and P. Stefanelli. Skew left braces with non-trivial annihilator. *J. Algebra Appl.*, 18(2):1950033, 23, 2019.

[47] Cayley. On the Analytical Forms Called Trees. *Amer. J. Math.*, 4(1-4):266–268, 1881.

[48] F. Cedó, E. Jespers, and A. del Río. Involutive Yang–Baxter groups. *Trans. Amer. Math. Soc.*, 362(5):2541–2558, 2010.

[49] F. Cedó, E. Jespers, Ł. Kubat, A. Van Antwerpen, and C. Verwimp. On various types of nilpotency of the structure monoid and group of a set-theoretic solution of the Yang–Baxter equation. *J. Pure Appl. Algebra*, 227(2):Paper No. 107194, 38, 2023.

[50] F. Cedó, E. Jespers, and J. Okniński. Retractability of set theoretic solutions of the Yang–Baxter equation. *Advances in Mathematics*, 224(6):2472–2484, 8 2010.

[51] F. Cedó, E. Jespers, and J. Okniński. An abundance of simple left braces with abelian multiplicative Sylow subgroups. *Rev. Mat. Iberoam.*, 36(5):1309–1332, 2020.

[52] F. Cedó, E. Jespers, and C. Verwimp. Structure monoids of set-theoretic solutions of the Yang–Baxter equation. *Publ. Mat.*, 65(2):499–528, 2021.

[53] F. Cedó and J. Okniński. Constructing finite simple solutions of the Yang–Baxter equation. *Adv. Math.*, 391:Paper No. 107968, 40, 2021.

[54] F. Cedó and J. Okniński. Indecomposable solutions of the Yang–Baxter equation of square-free cardinality. *Adv. Math.*, 430:Paper No. 109221, 26, 2023.

[55] F. Cedó, A. Smoktunowicz, and L. Vendramin. Skew left braces of nilpotent type. *Proc. Lond. Math. Soc. (3)*, 118(6):1367–1392, 2019.

[56] S. U. Chase and M. E. Sweedler. *Hopf algebras and Galois theory*. Lecture Notes in Mathematics, Vol. 97. Springer-Verlag, Berlin-New York, 1969.

[57] L. N. Childs. On the Hopf Galois theory for separable field extensions. *Comm. Algebra*, 17(4):809–825, 1989.

[58] L. N. Childs. *Taming wild extensions: Hopf algebras and local Galois module theory*, volume 80 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2000.

[59] L. N. Childs. On the Galois correspondence for Hopf Galois structures. *New York J. Math.*, 23:1–10, 2017.

[60] L. N. Childs. Skew braces and the Galois correspondence for Hopf Galois structures. *J. Algebra*, 511:270–291, 2018.

[61] L. N. Childs. Bi-skew braces and Hopf Galois structures. *New York J. Math.*, 25:574–588, 2019.

[62] L. N. Childs. On the Galois correspondence for Hopf Galois structures arising from finite radical algebras and Zappa-Szép products. *Publ. Mat.*, 65(1):141–163, 2021.

[63] L. N. Childs, C. Greither, K. P. Keating, A. Koch, T. Kohl, P. J. Truman, and R. G. Underwood. *Hopf algebras and Galois module theory*, volume 260 of *Mathematical Surveys and Monographs*. American Mathematical Society, 2021.

[64] F. Chouraqui. Left orders in Garside groups. *Internat. J. Algebra Comput.*, 26(07):1349–1359, 2016.

[65] I. Colazzo, E. Jespers, Ł. Kubat, and A. Van Antwerpen. Simple solutions of the Yang–Baxter equation. *arXiv:2312.09687*, 2024.

[66] I. Colazzo and A. Van Antwerpen. On the cabling of non-involutive set-theoretic solutions of the Yang–Baxter equation. *arXiv:2410.23821*, 2024.

[67] T. Crespo, A. Rio, and M. Vela. On the Galois correspondence theorem in separable Hopf Galois theory. *Publ. Mat.*, 60(1):221–234, 2016.

[68] C. Curry, K. Ebrahimi-Fard, and H. Munthe-Kaas. What is a post-Lie algebra and why is it useful in geometric integration. In F. A. Radu, K. Kumar, I. Berre, J. M. Nordbotten, and I. S. Pop, editors, *Numerical Mathematics and Advanced Applications ENUMATH 2017*, pages 429–437, Cham, 2019. Springer International Publishing.

[69] K. Dekimpe. Semi-simple splittings for solvable Lie groups and polynomial structures. *Forum Math.*, 12(1):77–96, 2000.

[70] J. Deré and M. Origlia. Simply transitive NIL-affine actions of solvable Lie groups. *Forum Math.*, 33(5):1349–1367, 2021.

[71] C. Dietzel, S. Properzi, and S. Trappeniers. Indecomposable involutive set-theoretical solutions to the Yang–Baxter equation of size $p^2$. *Comm. Algebra*, 53(3):1238–1256, 2025.

[72] V. G. Drinfel'd. On some unsolved problems in quantum group theory. In *Quantum groups (Leningrad, 1990)*, volume 1510 of *Lecture Notes in Math.*, pages 1–8. Springer, Berlin, 1992.

[73] P. Etingof, T. Schedler, and A. Soloviev. Set-theoretical solutions to the quantum Yang–Baxter equation. *Duke Math. J.*, 100(2):169–209, 1999.

[74] E. Feingesicht. Dehornoy's class and Sylows for set-theoretical solutions of the Yang–Baxter equation. *Internat. J. Algebra Comput.*, 34(1):147–173, 2024.

[75] D. Fried. Distality, completeness, and affine structures. *J. Differential Geom.*, 24(3):265–273, 1986.

[76] D. Fried and W. M. Goldman. Three-dimensional affine crystallographic groups. *Adv. in Math.*, 47(1):1–49, 1983.

[77] The GAP Group. *The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.14.0*, 2024.

[78] T. Gateva-Ivanova. Set-theoretic solutions of the Yang–Baxter equation, braces and symmetric groups. *Adv. Math*, 338:649–701, 2018.

[79] T. Gateva-Ivanova and P. Cameron. Multipermutation solutions of the Yang–Baxter equation. *Comm. Math. Phys.*, 309(3):583–621, 2012.

[80] I. Gorshkov and T. Nasybullov. Finite skew braces with solvable additive group. *J. Algebra*, 574:172–183, 2021.

[81] E. Goursat. Sur les substitutions orthogonales et les divisions régulières de l'espace. *Ann. Sci. École Norm. Sup. (3)*, 6:9–102, 1889.

[82] C. Greither and B. Pareigis. Hopf Galois theory for separable field extensions. *J. Algebra*, 106(1):239–258, 3 1987.

[83] L. Guarnieri and L. Vendramin. Skew braces and the Yang–Baxter equation. *Math. Comp.*, 86(307):2519–2534, 2017.

[84] M. Hall, Jr. *The theory of groups*. The Macmillan Company, New York, 1959.

[85] J. Helmstetter. Radical d'une algèbre symétrique à gauche. *Ann. Inst. Fourier (Grenoble)*, 29(4):viii, 17–35, 1979.

[86] B. Huppert. *Endliche Gruppen. I*, volume 134 of *Die Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin-New York, 1967.

[87] N. Iyudu. Classification of contraction algebras and pre-Lie algebras associated to braces and trusses. *arXiv:2008.06033*, pages 1–19, 2020.

[88] P. Jedlička and A. Pilitowska. Indecomposable involutive solutions of the Yang–Baxter equation of multipermutation level 2 with non-abelian permutation group. *J. Combin. Theory Ser. A*, 197:Paper No. 105753, 35, 2023.

[89] P. Jedlička, A. Pilitowska, and A. Zamojska-Dzienio. The construction of multipermutation solutions of the Yang–Baxter equation of level 2. *J. Combin. Theory Ser. A*, 176:105295, 35, 2020.

[90] P. Jedlička, A. Pilitowska, and A. Zamojska-Dzienio. Indecomposable involutive solutions of the Yang–Baxter equation of multipermutational level 2 with abelian permutation group. *Forum Math.*, 33(5):1083–1096, 2021.

[91] E. Jespers, L. Kubat, A. Van Antwerpen, and L. Vendramin. Radical and weight of skew braces and their applications to structure groups of solutions of the Yang–Baxter equation. *Adv. Math.*, 385:Paper No. 107767, 20, 2021.

[92] E. Jespers, L. u. Kubat, and A. Van Antwerpen. The structure monoid and algebra of a non-degenerate set-theoretic solution of the Yang–Baxter equation. *Trans. Amer. Math. Soc.*, 372(10):7191–7223, 2019.

[93] E. Jespers, A. Van Antwerpen, and L. Vendramin. Nilpotency of skew braces and multipermutation solutions of the Yang–Baxter equation. *Commun. Contemp. Math.*, 25(9):Paper No. 2250064, 20, 2023.

[94] D. Joyce. Simple quandles. *J. Algebra*, 79(2):307–318, 1982.

[95] C. Kassel. *Quantum groups*, volume 155 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[96] E. I. Khukhro. *$p$-automorphisms of finite $p$-groups*, volume 246 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1998.

[97] E. I. Khukhro and V. D. Mazurov, editors. *The Kourovka notebook*. Sobolev Institute of Mathematics. Russian Academy of Sciences. Siberian Branch, Novosibirsk, 20th edition, 2024. Unsolved problems in group theory, September 2024 update.

[98] H. Kim. Complete left-invariant affine structures on nilpotent Lie groups. *J. Differential Geom.*, 24(3):373–394, 1986.

[99] H. Kim. Extensions of left-symmetric algebras. *Algebras Groups Geom.*, 4(1):73–117, 1987.

[100] A. Koch. Abelian maps, bi-skew braces, and opposite pairs of Hopf-Galois structures. *Proc. Amer. Math. Soc. Ser. B*, 8:189–203, 2021.

[101] A. Koch. Abelian maps, brace blocks, and solutions to the Yang–Baxter equation. *J. Pure Appl. Algebra*, 226(9):Paper No. 107047, 2022.

[102] A. Koch, T. Kohl, P. J. Truman, and R. Underwood. Normality and short exact sequences of Hopf-Galois structures. *Comm. Algebra*, 47(5):2086–2101, 2019.

[103] A. Koch and P. J. Truman. Opposite skew left braces and applications. *J. Algebra*, 546:218–235, 2020.

[104] A. Koch and P. J. Truman. Skew left braces and isomorphism problems for Hopf-Galois structures on Galois extensions. *J. Algebra Appl.*, 22(5):Paper No. 2350118, 22, 2023.

[105] T. Kohl. Classification of the Hopf Galois structures on prime power radical extensions. *J. Algebra*, 207(2):525–546, 1998.

[106] T. Kohl. Characteristic subgroup lattices and Hopf-Galois structures. *Internat. J. Algebra Comput.*, 29(2):391–405, 2019.

[107] A. Konovalov, A. Smoktunowicz, and L. Vendramin. On skew braces and their ideals. *Exp. Math.*, 30(1):95–104, 2021.

[108] J.-L. Koszul. Domaines bornés homogènes et orbites de groupes de transformations affines. *Bull. Soc. Math. France*, 89:515–533, 1961.

[109] N. H. Kuiper. Sur les surfaces localement affines. In *Géométrie différentielle. Colloques Internationaux du Centre National de la Recherche Scientifique, Strasbourg, 1953*, pages 79–87. CNRS, Paris, 1953.

[110] T. Y. Lam. *A first course in noncommutative rings*, volume 131 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2001.

[111] I. Lau. An associative left brace is a ring. *J. Algebra Appl.*, 19(9):2050179, 6, 2020.

[112] M. Lazard. Sur les groupes nilpotents et les anneaux de Lie. *Ann. Sci. École Norm. Sup. (3)*, 71:101–190, 1954.

[113] V. Lebed and A. Mortier. Abelian quandles and quandles with abelian structure group. *J. Pure Appl. Algebra*, 225(1):Paper No. 106474, 22, 2021.

[114] V. Lebed, S. Ramírez, and L. Vendramin. Involutive Yang–Baxter: cabling, decomposability, and Dehornoy class. *Revista Matemática Iberoamericana*, pages 1–13, 2023.

[115] V. Lebed and L. Vendramin. On structure groups of set-theoretic solutions to the Yang–Baxter equation. *Proc. Edinb. Math. Soc. (2)*, 62(3):683–717, 2019.

[116] T. Letourmy and L. Vendramin. Isoclinism of skew braces. *Bull. Lond. Math. Soc.*, 55(6):2891–2906, 2023.

[117] J.-H. Lu, M. Yan, and Y.-C. Zhu. On the set-theoretical Yang–Baxter equation. *Duke Math. J.*, 104(1):1–18, 2000.

[118] A. Lucchini. On imprimitive groups with small degree. *Rend. Semin. Mat. Univ. Padova*, 86:131–142, 1991.

[119] A. I. Malcev. Nilpotent torsion-free groups. *Izv. Akad. Nauk SSSR Ser. Mat.*, 13:201–212, 1949.

[120] J. Milnor. On the existence of a connection with curvature zero. *Comment. Math. Helv.*, 32:215–223, 1958.

[121] J. Milnor. On fundamental groups of complete affinely flat manifolds. *Adv. Math.*, 25(2):178–187, 1977.

[122] S. Montgomery. *Hopf algebras and their actions on rings*, volume 82 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 1993.

[123] T. Nasybullov. Connections between properties of the additive and the multiplicative groups of a two-sided skew brace. *J. Algebra*, 540:156–167, 2019.

[124] K. Nejabati Zenouz. *On Hopf-Galois Structures and Skew Braces of Order $p^3$*. PhD thesis, University of Exeter, 2018.

[125] K. Nejabati Zenouz. Skew braces and Hopf-Galois structures of Heisenberg type. *J. Algebra*, 524:187–225, 2019.

[126] D. Puljić. Right Nilpotency of Braces of Cardinality $p^4$. *arXiv:2112.15041*, pages 1–13, 2021.

[127] D. Puljić. Classification of braces of cardinality $p^4$. *J. Algebra*, 660:1–33, 2024.

[128] D. Puljić, A. Smoktunowicz, and K. Nejabati Zenouz. Some braces of cardinality $p^4$ and related Hopf-Galois extensions. *New York J. Math.*, 28:494–522, 2022.

[129] K. Reidemeister. Elementare Begründung der Knotentheorie. *Abh. Math. Sem. Univ. Hamburg*, 5(1):24–32, 1927.

[130] D. J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1996.

[131] W. Rump. A decomposition theorem for square-free unitary solutions of the quantum Yang–Baxter equation. *Adv. Math.*, 193(1):40–55, 2005.

[132] W. Rump. Braces, radical rings, and the quantum Yang–Baxter equation. *J. Algebra*, 307(1):153–170, 2007.

[133] W. Rump. Classification of cyclic braces. *J. Pure Appl. Algebra*, 209(3):671–685, 2007.

[134] W. Rump. Classification of cyclic braces, II. *Trans. Amer. Math.*, 372(1):305–328, 2019.

[135] W. Rump. Classification of indecomposable involutive set-theoretic solutions to the Yang–Baxter equation. *Forum Math.*, 32(4):891–903, 2020.

[136] W. Rump. One-generator braces and indecomposable set-theoretic solutions to the Yang–Baxter equation. *Proc. Edinb. Math. Soc. (2)*, 63(3):676–696, 2020.

[137] W. Rump. The classification of nondegenerate uniconnected cycle sets. *Pacific J. Math.*, 323(1):205–221, 2023.

[138] W. Rump. Primes in coverings of indecomposable involutive set-theoretic solutions to the Yang–Baxter equation. *Bull. Belg. Math. Soc. Simon Stevin*, 30(2):260–280, 2023.

[139] E. Sąsiada and P. M. Cohn. An example of a simple radical ring. *J. Algebra*, 5:373–377, 1967.

[140] E. Schenkman. On the norm of a group. *Illinois J. Math.*, 4:150–152, 1960.

[141] J. Scheuneman. Translations in certain groups of affine motions. *Proc. Amer. Math. Soc.*, 47:223–228, 1975.

[142] D. Segal. The structure of complete left-symmetric algebras. *Math. Ann.*, 293(3):569–578, 1992.

[143] A. Shalev and A. Smoktunowicz. From braces to pre-Lie rings. *Proc. Amer. Math. Soc.*, 152(4):1545–1559, 2024.

[144] A. Smoktunowicz. A note on set-theoretic solutions of the Yang–Baxter equation. *J. Algebra*, 500:3–18, 2018.

[145] A. Smoktunowicz. On Engel groups, nilpotent groups, rings, braces and the Yang–Baxter equation. *Trans. Amer. Math. Soc.*, 370(9):6535–6564, 2018.

[146] A. Smoktunowicz. A new formula for Lazard's correspondence for finite braces and pre-Lie algebras. *J. Algebra*, 594:202–229, 2022.

[147] A. Smoktunowicz. On the passage from finite braces to pre-Lie rings. *Adv. Math.*, 409:Paper No. 108683, 33, 2022.

[148] A. Smoktunowicz. On the passage from finite braces to pre-Lie rings. *arXiv:2202.00085v3*, 2022.

[149] A. Smoktunowicz. More on skew braces and their ideals. In *Amitsur Centennial Symposium*, volume 800 of *Contemp. Math.*, pages 301–308. Amer. Math. Soc., 2024.

[150] A. Smoktunowicz and A. Smoktunowicz. Set-theoretic solutions of the Yang–Baxter equation and new classes of R-matrices. *Linear Algebra Appl.*, 546:86–114, 2018.

[151] A. Smoktunowicz and L. Vendramin. On skew braces (with an appendix by N. Byott and L. Vendramin). *J. Comb. Algebra*, 2(1):47–86, 2018.

[152] A. Soloviev. Non-unitary set-theoretical solutions to the quantum Yang–Baxter equation. *Math. Res. Lett.*, 7(5-6):577–596, 2000.

[153] F. Spaggiari. The mutually normalizing regular subgroups of the holomorph of a cyclic group of prime power order. *Comm. Algebra*, 51(4):1623–1653, 2023.

[154] L. Stefanello and S. Trappeniers. On bi-skew braces and brace blocks. *J. Pure Appl. Algebra*, 227(5):Paper No. 107295, 22, 2023.

[155] L. Stefanello and S. Trappeniers. On the connection between Hopf-Galois structures and skew braces. *Bull. Lond. Math. Soc.*, 55(4):1726–1748, 2023.

[156] L. Stefanello and C. Tsang. Classification of the types for which every Hopf-Galois correspondence is bijective. *J. Algebra*, 664:514–526, 2025.

[157] Y. P. Sysak. The adjoint group of radical rings and related questions. In *Ischia group theory 2010*, pages 344–365. World Sci. Publ., Hackensack, NJ, 2012.

[158] S. Trappeniers. On two-sided skew braces. *J. Algebra*, 631:267–286, 2023.

[159] S. Trappeniers. A Lazard correspondence for post-lie rings and skew braces. *arXiv:2406.02475*, pages 1–20, 2024.

[160] C. Tsang. Hopf-Galois structures on cyclic extensions and skew braces with cyclic multiplicative group. *Proc. Amer. Math. Soc. Ser. B*, 9:377–392, 2022.

[161] C. Tsang. Non-abelian simple groups which occur as the type of a Hopf-Galois structure on a solvable extension. *Bull. Lond. Math. Soc.*, 55(5):2324–2340, 2023.

[162] C. Tsang and C. Qin. On the solvability of regular subgroups in the holomorph of a finite solvable group. *Internat. J. Algebra Comput.*, 30(2):253–265, 2020.

[163] B. Vallette. Homology of generalized partition posets. *J. Pure Appl. Algebra*, 208(2):699–725, 2007.

[164] L. Vendramin. Problems on skew left braces. *Adv. Group Theory Appl.*, 7:15–37, 2019.

[165] L. Vendramin and O. Konovalov. YangBaxter, combinatorial solutions for the Yang–Baxter equation, Version 0.10.6. `https://gap-packages.github.io/YangBaxter`, Jul 2024. GAP package.

[166] C. Verwimp. *Set-theoretic solutions of the Yang–Baxter equation and associated algebraic structures*. PhD thesis, Vrije Universiteit Brussel, 2022.

[167] E. B. Vinberg. The theory of homogeneous convex cones. *Trudy Moskov. Mat. Obšč.*, 12:303–358, 1963.

[168] J. F. Watters. On the adjoint group of a radical ring. *J. London Math. Soc.*, 43:725–729, 1968.

[169] C. N. Yang. Some exact results for the many-body problem in one dimension with repulsive delta-function interaction. *Phys. Rev. Lett.*, 19:1312–1315, 1967.

# List of symbols

We present here a list of symbols and notations that are used throughout this thesis, together with their description and the page number of their first appearance. We have organized these by the context in which they appear.

## General

| Symbol | Description | Page |
|---|---|---|
| $\mathbb{S}_X$ | The symmetric group on the set $X$. | 20 |
| $\mathbb{S}_n$ | The symmetric group on the set $\{1, ..., n\}$. | 20 |
| $\mathbb{Z}/n$ | The integers modulo $n$. | 24 |
| $R$ | A commutative ring. | 33 |
| $\mathbb{F}_q$ | The unique field of order $q$, for $q$ a prime power. | 38 |
| $R[X]$ | The ring of polynomials over $R$ with variables $X$. | 41 |
| $R[[X]]$ | The ring of formal power series over $R$ with variables $X$. | 41 |
| $\mathcal{P}_i$ | The set of all primes less than or equal to $i$. | 45 |
| $C_n$ | The cyclic group of order $n$. | 60 |
| $\mathrm{GL}_n(K)$ | The general linear group of degree $n$ over the field $K$. | 64 |
| $R^\times$ | The group of invertible elements of the ring $R$. | 106 |
| $F_n$ | The free non-unital ring of nilpotency class $n$ generated by $x$. | 123 |
| $F_n^*$ | The pair $(F_n, x + F_n^2)$. | 123 |

## Solutions of the Yang–Baxter equation and cycle sets

| Symbol | Description | Page |
|---|---|---|
| $(X, r)$ | A non-degenerate bijective set-theoretical solution of the Yang–Baxter equation. | 20 |
| $\sigma_x(y)$ | The first component of $r(x, y)$ for $(X, r)$ a solution. | 21 |
| $\tau_y(x)$ | The second component of $r(x, y)$ for $(X, r)$ a solution. | 21 |
| $\hat{\sigma}_x(y)$ | The first component of $r^{-1}(x, y)$ for $(X, r)$ a solution. | 21 |
| $\tau_y(x)$ | The second component of $r^{-1}(x, y)$ for $(X, r)$ a solution. | 21 |

| | | |
|---|---|---|
| $\triangleright_r$ | The operation of the derived rack of the solution $(X, r)$. | 24 |
| $(X, r')$ | The derived solution of the solution $(X, r')$. | 24 |
| $G(X, r)$ | The structure skew brace on $(X, r)$. | 25 |
| $(X, r^{(k)})$ | The $k$-cabling of the solutions $(X, r)$. | 31 |
| $\sigma_x^{(k)}(y)$ | The first component of $r^{(k)}(x, y)$ for $(X, r)$ a solution. | 31 |
| $\sigma_y^{(k)}(x)$ | The second component of $r^{(k)}(x, y)$ for $(X, r)$ a solution. | 31 |
| $\mathcal{G}(X, r)$ | The permutation skew brace on $(X, r)$. | 27 |
| $\mathrm{Ret}(X)$ | The retract of the solution $(X, r)$. | 30 |
| $\mathrm{mpl}(X, r)$ | The multipermutation level of $(X, r)$. | 31 |
| $(X, \cdot)$ | A cycle set. | 32 |
| $G(X, \cdot)$ | The structure brace of the cycle set $(X, \cdot)$. | 32 |
| $\mathcal{G}(X, \cdot)$ | The permutation brace of the cycle set $(X, \cdot)$. | 32 |
| $\mathrm{Ret}(X, \cdot)$ | The retract of the cycle set $(X, \cdot)$. | 32 |
| $\mathrm{mpl}'(X, r)$ | The variation of the multipermutation level of $(X, r)$. | 85 |
| $(X, \cdot^{(k)})$ | The $k$-cabling of the cycle set $(X, \cdot)$. | 112 |

## Groups

| Symbol | Description | Page |
|---|---|---|
| $\mathrm{Triv}(G)$ | The trivial skew brace on the group $G$. | 9 |
| $\mathrm{opTriv}(G)$ | The almost trivial skew brace on the group $G$. | 9 |
| $Z(G)$ | The center of the group $G$. | 10 |
| $\mathrm{Aut}(G)$ | The group automorphisms of the group $G$. | 12 |
| $\mathrm{Hol}(G)$ | The holomorph $G \rtimes \mathrm{Aut}(G)$ of the group $G$. | 12 |
| $\mathrm{Stab}_G(x)$ | The stabilizer of an element $x$, where $x \in X$ and the group $G$ acts on a set $X$. | 13 |
| $\mathrm{Aut}^\infty(G)$ | The Lie group automorphisms of the Lie group $G$. | 18 |
| $\mathrm{Hol}^\infty(G)$ | The smooth holomorph $G \rtimes \mathrm{Aut}^\infty(G)$ of the Lie group $G$. | 18 |
| $\mathrm{End}(M)$ | The algebra of endomorphisms of an abelian group $M$. | 36 |
| $\mathrm{End}_f(M)$ | The filtered algebra of endomorphisms of the filtered abelian group $M$. | 41 |
| $[g, h]$ | The commutator $ghg^{-1}h^{-1}$ of the elements $g, h$ in a group $G$. | 46 |
| $\mathbf{Laz}^{-1}(G)$ | The filtered Lie ring associated to the Lazard group $G$ under the Lazard correspondence. | 46 |
| $\mathcal{L}_g$ | The bijection $G \to G : h \mapsto gh$ for $G$ a group and $g \in G$. | 52 |
| $\mathcal{R}_g$ | The bijection $G \to G : h \mapsto hg$ for $G$ a group and $g \in G$. | 53 |
| $\mathrm{Ab}(G)$ | The abelianization of $G$. | 72 |
| $\mathrm{Inn}_H(G)$ | The group of inner automorphisms of the group $G$ induced by the elements of the subgroup $H$. | 65 |
| $N(G)$ | The norm of the group $G$. | 141 |
| $\mathrm{Aut}_f(G)$ | The filtered automorphisms of the filtered group $G$. | 150 |
| $\mathrm{Hol}_f(G)$ | The filtered holomorph $G \rtimes \mathrm{Aut}_f(G)$ of the filtered group $G$. | 158 |

## Lie algebras

| Symbol | Description | Page |
|---|---|---|
| $\mathfrak{der}(\mathfrak{g})$ | The Lie algebra of derivations of the Lie algebra $\mathfrak{g}$. | 33 |
| $Z(\mathfrak{g})$ | The center of the Lie algebra $\mathfrak{g}$. | 35 |
| $\mathfrak{g}_{\mathrm{op}}$ | The opposite of the Lie algebra $\mathfrak{g}$. | 35 |
| $\mathfrak{a} \oplus_\delta \mathfrak{g}$ | The semidirect sum of the Lie algebras $\mathfrak{a}$ and $\mathfrak{g}$ with respect to the action $\delta : \mathfrak{g} \to \mathfrak{der}_f(\mathfrak{a})$. | 36 |
| $\mathfrak{aff}(\mathfrak{a})$ | The affine Lie algebra $\mathfrak{a} \oplus \mathfrak{der}(\mathfrak{a})$ of the Lie algebra $\mathfrak{a}$. | 36 |
| $\mathcal{U}(\mathfrak{g})$ | The universal enveloping algebra of the Lie algebra $\mathfrak{g}$ | 36 |
| $\mathrm{ad}_x$ | The adjoint derivation $\mathfrak{g} \to \mathfrak{g} : y \mapsto [x, y]$ within a Lie algebra $\mathfrak{g}$. | 47 |
| $\mathfrak{der}_f(\mathfrak{g})$ | The filtered derivations of the filtered Lie algebra $\mathfrak{g}$. | 148 |
| $\mathrm{Aut}_f(\mathfrak{g})$ | The filtered automorphisms of the filtered Lie algebra $\mathfrak{g}$. | 152 |
| $\mathfrak{aff}_f(\mathfrak{g})$ | The filtered holomorph $\mathfrak{g} \rtimes \mathfrak{der}_f(\mathfrak{g})$ of the filtered Lie algebra $\mathfrak{g}$. | 158 |

## Skew braces

| Symbol | Description | Page |
|---|---|---|
| $(A, \cdot, \circ)$ | A skew brace. | 9 |
| $a^{\circ n}$ | The $n$-th power of $a \in A$ in the group $(A, \circ)$. | 9 |
| $a^{\cdot n}$ | The $n$-th power of $a \in A$ in the group $(A, \cdot)$ | 9 |
| $\lambda_a$ | The $\lambda$-map $A \to A : b \mapsto a^{-1} \cdot (a \circ b)$ of a skew brace $A$ and $a \in A$. | 10 |
| $\mathrm{Fix}(A)$ | The set of fixed elements of the skew brace $A$. | 10 |
| $\mathrm{Soc}(A)$ | The socle of the skew brace $A$. | 10 |
| $\mathrm{Ann}(A)$ | The annihilator of the skew brace $A$. | 11 |
| $\mathrm{Aut}(A, \cdot, \circ)$ | The automorphism group of the skew brace $A$. | 11 |
| $A \rtimes_\alpha B$ | The semidirect product of the skew braces $A$ and $B$ with respect to the action $\alpha : (B, \circ) \to \mathrm{Aut}(A, \cdot, \circ)$. | 11 |
| $A_{\mathrm{op}}$ | The opposite of the skew brace $A$. | 11 |
| $A'$ | The commutator of a skew brace $A$. | 15 |
| $X * Y$ | The subgroup of $(A, \cdot)$ generated by the set $\{x * y \mid x \in X, y \in Y\}$. | 15 |
| $\mathrm{Soc}_i(A)$ | The $i$-th term in the socle series of the skew brace $A$. | 16 |
| $\mathrm{mpl}(A)$ | The multipermutation level of the skew brace $A$. | 16 |
| $A^i$ | The $i$-th term in the left series of the skew brace $A$. | 15 |
| $A^{(i)}$ | The $i$-th term in the right series of the skew brace $A$. | 15 |
| $A^{[i]}$ | The $i$-th term in the strong series of the skew brace $A$. | 16 |
| $A_{(i)}$ | The $i$-th term in the derived series of the skew brace $A$. | 16 |
| $A_\leftrightarrow$ | The skew brace $(A, \circ, \cdot)$, where $A = (A, \cdot, \circ)$ is bi-skew brace. | 16 |
| $(A, r_A)$ | The solution on the skew brace $A$. | 25 |
| $H(A)$ | The set of all elements of the skew brace $A$ such that $\lambda_a$ is a skew brace automorphism. | 96 |
| $\mathrm{Fix}_A(S)$ | The elements $a \in A$ such that $\lambda_s(a) = a$ for all $s \in S$. | 103 |
| $L^i(A)$ | The $i$-th term in the $L$-series of the skew brace $A$. | 167 |

## Post-Lie algebras

| Symbol | Description | Page |
|---|---|---|
| $(\mathfrak{a}, \triangleright)$ | A post-Lie algebra. | 33 |
| $\mathcal{L}_x$ | The map $\mathfrak{a} \to \mathfrak{a} : y \mapsto x \triangleright y$ within a post-Lie algebra $(\mathfrak{a}, \triangleright)$. | 34 |
| $\mathfrak{a}^\circ$ | The sub-adjacent Lie algebra of the post-Lie algebra $(\mathfrak{a}, \triangleright)$. | 34 |
| $\mathrm{Fix}(\mathfrak{a}, \triangleright)$ | The set of fixed elements of the post-Lie algebra $(\mathfrak{a}, \triangleright)$. | 35 |
| $\mathrm{Soc}(\mathfrak{a}, \triangleright)$ | The socle of the post-Lie algebra $(\mathfrak{a}, \triangleright)$. | 35 |
| $\mathrm{Ann}(\mathfrak{a}, \triangleright)$ | The annihilator of the post-Lie algebra $(\mathfrak{a}, \triangleright)$. | 35 |
| $(\mathfrak{a}, \triangleright)_{\mathrm{op}}$ | The opposite of the post-Lie algebra $(\mathfrak{a}, \triangleright)$. | 35 |
| $\mathfrak{a}^i$ | The $i$-th term in the left series of the post-Lie algebra $(\mathfrak{a}, \triangleright)$. | 38 |
| $\mathfrak{a}^{(i)}$ | The $i$-th term in the right series of the post-Lie algebra $(\mathfrak{a}, \triangleright)$. | 39 |
| $L^i(\mathfrak{a}, \triangleright)$ | The $i$-th term in the $L$-series of the post-Lie algebra $(\mathfrak{a}, \triangleright)$. | 166 |

# Index