

Faculté des sciences

Some algebraic and categorical properties of skew braces

Auteure : Aude Winand

Promoteur : Marino Gran

Lecteur·rices : Tim Van der Linden, Ilaria Colazzo

Année académique 2025-2026

UNIVERSITÉ CATHOLIQUE DE LOUVAIN
FACULTÉ DES SCIENCES
ÉCOLE DE MATHÉMATIQUES

Some algebraic and categorical properties of skew braces

Aude Winand
Advisor: Marino Gran
Readers: Tim Van der Linden, Ilaria Colazzo

Master thesis
June 2026

Acknowledgments

I would like to thank Professor Gran for his availability, guidance and support throughout this thesis. His invaluable advice and insightful comments always stimulated my work. I'm grateful for the time he dedicated to share his expertise and for the enlightening discussions about algebra and category theory.

I would also like to thank Professors Van der Linden and Colazzo for accepting to be readers of this thesis.

Finally, I would like to thank my parents and my family for their support during the writing of this thesis, as for their encouragement during my whole academic course. I especially thank my father for his rereading of this work.

Introduction

The quantum Yang-Baxter equation is a statistical mechanics equation named after two physicists, Chen Ning Yang (1922-2025) and Rodney James Baxter (1940-2025). The equation first appeared in the late sixties, in Yang's research on a statistical mechanics' problem. He faced to the equation when he was trying to determine the wave function in the one-dimensional N-body problem in [44]. On the other hand, in [6], Baxter developed the solutions of vertex models, which are physics models used to study the theory of statistical mechanics and integrable systems. He noticed that these solutions have a really similar structure to the one of the equation introduced by Yang a few years earlier.

A solution of the quantum Yang-Baxter equation is a bijective linear map

$$R: V \otimes V \rightarrow V \otimes V,$$

where V is a vector space, such that

$$R_{12}R_{13}R_{23} = R_{23}R_{13}R_{12},$$

where $R_{ij}: V \otimes V \otimes V \rightarrow V \otimes V \otimes V$ acts as R on the (i, j) term and as the identity on V on the remaining term. For instance, the map $R_{12}: V \otimes V \otimes V \rightarrow V \otimes V \otimes V$ is defined by $R_{12} = R \otimes \text{id}_V$. From a physical point of view, this equation guarantees the coherence of the exchanges. If you have three particles that interact two by two following rules from the definition of R , the final outcome does not depend on the order of the interactions.

Beyond the interest of studying the Yang-Baxter equation in physics, many mathematical fields have been enriched by the search of solutions of the equation. During the last decades, many new links have been discovered between this theory and, for example, knot theory, low-dimensional topology, combinatorics, group theory and ring theory, see for instance [4], [23].

The study of solutions is a major open problem. Since the class of linear solutions is wide, it is out of the reach of mathematicians for the moment. In 1992, in [21], Drinfeld suggested to classify and study the set-theoretic solutions of the Yang-Baxter equation, i.e. solutions on a basis of the vector space V . Hence, a set-theoretic solution of the Yang-Baxter equation is a pair (X, r) , where X is a non-empty set and $r: X \times X \rightarrow X \times X$

a map such that

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

Following that idea, Weinstein and Xu, in [43], built set-theoretic solutions by using Poisson Lie groups, Lie algebras and quasitriangularity. Etingof, Schedler and Soloviev, in [22], looked at set-theoretic solutions satisfying some criteria: the involutive non-degenerate solutions. If we write the components of the map r as $r(x, y) = (\sigma_x(y), \tau_y(x))$, where σ_x and τ_y are maps from X to itself for each $x, y \in X$, we say that a solution is non-degenerate if, for each $x \in X$, the maps σ_x and τ_x are bijective. Moreover, a solution is involutive if $r^2 = \text{id}_{X \times X}$. Gateva-Ivanova and Van den Bergh, in [24], focused on involutive solutions.

In 2007, Rump, in [39], defined the new algebraic structure of left braces and he proved that involutive non-degenerate set-theoretic solutions correspond exactly to left braces. Since one is naturally interested in expanding our class of solutions, in [29], Guarnieri and Vendramin extended the concept of (left) braces to the one of skew (left) braces to study the class of (non-degenerate) not necessarily involutive set-theoretic solutions of the Yang-Baxter equation.

A skew left brace is a set A endowed with two binary operations $\circ$ and $+$ such that $(A, \circ)$ and $(A, +)$ are groups. These operations must satisfy a left distributive identity:

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

A skew brace morphism is a map between skew braces that preserve each of the operations of the skew brace. These algebraic structures and their morphisms form a category, denoted by SKB, that is actually a variety of universal algebras. Indeed, the definition of a skew brace refers to a set equipped with operations that verify some specific identities, which is exactly what makes it possible to see SKB as a variety of universal algebras. We noticed that skew braces have many common properties with the algebraic structure of groups. On the other hand, the concept of semi-abelian category captures the properties of the category Grp of groups. Indeed, semi-abelian categories were introduced by G. Janelidze, L. Márki and W. Tholen, in [32], as a non-additive counterpart of abelian categories. One of the advantages of the introduction of this notion is that it covers several important types of algebraic structures, such as the categories of groups, rings and Lie algebras, and many more. Note that in a semi-abelian category the classical isomorphism theorems and homological lemmas hold true, and can be proved by using an abstract and simple approach.

In 1990, D. Bourn introduced the notion of protomodular category [11], that is at the heart of the definition of semi-abelian category. However, the protomodular context is not sufficient to develop homological algebra, where the Short Five Lemma, the 3×3 Lemma, the Snake Lemma or the Noether Isomorphism Theorems are often needed for the development of the theory. For this, the regularity and the pointedness of the category are also necessary, naturally leading to the notion of semi-abelian category,

where the additional property of (Barr-)exactness [5] is required. This sets the definition of a semi-abelian category, i.e. a pointed, exact, protomodular category with binary coproducts. The reason why they named it a semi-abelian category comes from the fact that, in this type of categories, it is possible to define a categorical notion of semi-direct product, and also from the result asserting that a category $\mathcal{C}$ is abelian if and only if the categories $\mathcal{C}$ and $\mathcal{C}^{op}$ are semi-abelian.

The category SKB of skew braces is a remarkable example of a semi-abelian category. It is even a strongly protomodular category [10], which gives a very suitable context to develop commutator theory, as in the categories of groups and of Lie algebras.

This thesis is structured in the following way. In Chapter 1, we define the notion of skew brace and we give some of its fundamental properties. For instance, we define and examine its substructures. We also establish the link between this new algebraic structure and some related algebraic structures as radical rings and (left) braces. In Chapter 2, we look at the Yang-Baxter equation and its set-theoretic solutions. We analyze how skew braces provide a wider range of solutions than the other algebraic structures developed earlier. Moreover, we briefly introduce the concept of shelves and racks and explain the link between set-theoretic solutions and these algebraic structures. Finally, in Chapter 3, we consider skew braces from a categorical point of view. We first recall some notions of category theory and universal algebra that we carefully examine in the category of skew braces. We prove that SKB is a semi-abelian category that is also strongly protomodular. We link these general categorical properties to some more concrete aspects of the algebraic structure of skew brace.

In a few words, the aim of this thesis is to consider two different approaches to the structure of skew braces, i.e. the algebraic and categorical points of view, to compare them and to observe how each perspective contributes to improve our understanding of the richness of this structure. Moreover, we keep in mind the origin of the structure and we explore its links with the Yang-Baxter equation.

Contents

Acknowledgments	5
Introduction	7
1 Skew braces	11
1.1 Definition and properties	11
1.2 Ideals	21
1.3 Isomorphism theorems	26
1.4 Radical rings	29
1.5 Historical point on the notion of skew braces	34
1.6 Some adjunctions in the category of skew braces	38
2 Yang-Baxter equation	40
2.1 Set-theoretic solutions of the Yang-Baxter equation	41
2.2 Self-distributive operations and set-theoretic solutions	49
3 Category of Skew Braces	53
3.1 Some notions of Category Theory	53
3.2 SKB is a semi-abelian category	62
3.3 Strong protomodularity of SKB	64
3.4 Some categorical results in SKB	66
Conclusion	72

Chapter 1

Skew braces

In this chapter, we study the structure and the properties of skew braces. Since this concept is quite new in the world of mathematics, there is no universal notation and language to express this theory. We adopt the notations in the book [18].

1.1 Definition and properties

For this section, we principally refer to the Chapter 8 of the book [18] written by Ferran Cedó and Leandro Vendramin.

We first define a skew brace and give some properties and examples. Informally, a skew brace is a set equipped with two group structures such that the distributivity of one with respect to the other differs from the classical one.

Definition 1.1. *A skew left brace is a triple $(A, +, \circ)$ where $(A, +)$ and $(A, \circ)$ are (not necessarily abelian) groups such that, for all $a, b, c \in A$, we have the left distributive identity*

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

With respect to the multiplicative operation $\circ$, one writes a' for the inverse of $a \in A$ and 1 for its neutral element. Similarly, for the additive operation $+$, one writes the inverse of $a \in A$ as $-a$ and the neutral element as 0.

Since the multiplication is the higher order of operations, the identity in the definition of skew left braces can be simply written as $a \circ (b + c) = a \circ b - a + a \circ c$.

Skew (left) braces can actually be considered as a generalization of radical rings, that were developed in the 1940s. We will investigate this claim in Subsection 1.4.3.

One defines a *skew right brace* in a similar way by requiring the right distributive condition instead of the left one, i.e., for all $a, b, c \in A$,

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

Proposition 1.2. *There is a bijective correspondence between skew left braces and skew right braces.*

Proof. Let $(A, +, \circ)$ be a skew left brace. We can define the following operations

$$\tilde{+}: A \times A \rightarrow A, (a, b) \mapsto b + a$$

and

$$\tilde{\circ}: A \times A \rightarrow A, (a, b) \mapsto b \circ a.$$

The triple $(A, \tilde{+}, \tilde{\circ})$ is a skew right brace. Indeed, $(A, \tilde{+})$ and $(A, \tilde{\circ})$ are groups since $(A, +)$ and $(A, \circ)$ are groups. Moreover,

$$\begin{aligned} (a \tilde{+} b) \tilde{\circ} c &= c \circ (b + a) \\ &= c \circ b - c + c \circ a \\ &= a \tilde{\circ} c - c \tilde{+} b \tilde{\circ} c. \end{aligned}$$

On the other hand, given a skew right brace $(A, \tilde{+}, \tilde{\circ})$, we apply exactly the same reasoning as before and we find a skew left brace $(A, +, \circ)$.

These two identifications are inverses of each other such that one obtains the one-to-one correspondence between skew left braces and skew right braces. $\square$

A skew left brace is usually called a skew brace.

There is a natural notion of morphism of skew braces:

Definition 1.3. *A map $f: A \rightarrow B$ between two skew braces A and B is a skew brace morphism if $f(x \circ y) = f(x) \circ f(y)$ and $f(x + y) = f(x) + f(y)$, for all $x, y \in A$.*

The skew braces and their morphisms will form a category, denoted by SKB, which will be studied in details in Chapter 3. Considering that fact, the previous proposition provides actually an isomorphism of categories between the category of skew left braces, SKB, and the one of skew right braces, RSKB. We denote the set of skew brace morphisms between A and B by $\text{Hom}_{\text{SKB}}(A, B)$.

Remark 1.4. Since we use the symbol $\circ$ for the multiplication of a skew brace, the composition of two composable morphisms $f: A \rightarrow B$ and $g: B \rightarrow C$ will be written gf , in the first two chapters of this thesis.

Lemma 1.5. *Let $(A, +, \circ)$ be a skew brace. Then $0 = 1$, where 0 is the neutral element of the addition and 1 is the neutral element of the multiplication.*

Proof. The left distributive condition of a skew brace states that

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

for all $a, b, c \in A$. Take $c = 1$. Then $a \circ (b + 1) = a \circ b - a + a \circ 1 = a \circ b - a + a = a \circ b$. Since the neutral element for the addition 0 is unique, one obtains that $0 = 1$. $\square$

Considering this lemma, the category SKB has a zero object, $\{0\}$, implying that the category is pointed, as explained with more details in Subsection 3.1.2.

The *kernel* of a morphism $f: A \rightarrow B$ is $\ker(f) = \{a \in A \mid f(a) = 0\}$ and its *image* is $\text{Im}(f) = \{b \in B \mid \exists a \in A \text{ such that } b = f(a)\}$.

As in the case of groups, the condition $\ker(f) = \{0\}$ is equivalent to the injectivity of the morphism f .

Lemma 1.6. *A skew brace morphism $f: A \rightarrow B$ is injective if and only if*

$$\ker(f) = \{0\}.$$

Proof. " $\Rightarrow$ " Let $x \in \ker(f)$. Then $f(x) = 0 = f(0)$. Since f is injective, $x = 0$.

" $\Leftarrow$ " Let $x, y \in A$ such that $f(x) = f(y)$. Then

$$f(x) - f(y) = 0 \Leftrightarrow f(x - y) = 0,$$

which implies that

$$x - y \in \ker(f) = \{0\} \Leftrightarrow x - y = 0 \Leftrightarrow x = y.$$

Therefore, f is injective. $\square$

An *isomorphism* of skew braces is the same as a bijective skew brace morphism. An *automorphism of a skew brace* A is an isomorphism from the skew brace A to itself. We write $\text{Aut}_{\text{SKB}}(A)$ to denote the group of skew brace automorphisms of A . Two skew braces A and B are *isomorphic* if there exists an isomorphism $f: A \rightarrow B$. In this case, we write $A \cong B$.

To become more familiar with the structure of skew braces, we introduce some examples.

Example 1.7. The first simple example of a skew brace is the triple $(A, +, +)$ with $(A, +)$ a group (not necessarily abelian). We check that the left distributive condition is satisfied. Let $a, b, c \in A$. Then $a \circ (b + c) = a + (b + c)$ and $a \circ b - a + a \circ c = a + b - a + a + c = a + b + c$. Since the additive operation is associative, the condition is verified and the triple is a skew brace.

Example 1.8. Let $(A, +_A, \circ_A)$ and $(B, +_B, \circ_B)$ be skew braces. Then the product $A \times B$ endowed with the operations defined, for all $(a, b), (a_1, b_1) \in A \times B$, by

$$(a, b) + (a_1, b_1) = (a +_A a_1, b +_B b_1) \text{ and } (a, b) \circ (a_1, b_1) = (a \circ_A a_1, b \circ_B b_1)$$

is also a skew brace. Being stable under product is actually true for any variety of finitary algebras. In Section 3.1.1, we introduce this concept and prove that SKB is indeed a variety of finitary algebras.

These first two examples were still abstract. We can consider a well-known group, the symmetric group of order six, and build a skew brace from it.

Example 1.9. Let's take the symmetric group $A = (\text{Sym}(3), +)$ of order six with its natural operation of composition written additively. One defines the second operation in the following way. First, one looks at the map $\lambda: A \rightarrow \text{Aut}(A)$, $\lambda(a) = \lambda_a$ defined on elements as follows:

$$\begin{aligned} \lambda_{\text{id}} &= \lambda_{(1\ 2\ 3)} = \lambda_{(1\ 3\ 2)} = \text{id} ; \\ \lambda_{(1\ 2)} &= \lambda_{(1\ 3)} = \lambda_{(2\ 3)} = \text{conjugation by } (2\ 3). \end{aligned}$$

The multiplication on $\text{Sym}(3)$ is defined by setting $a \circ b = a + \lambda_a(b)$, for $a, b \in \text{Sym}(3)$, which forms a cyclic group of order six generated by $(1\ 2)$. It remains to prove that $(\text{Sym}(3), +, \circ)$ is a skew brace, i.e. to prove the left distributivity. Let $a, b, c \in \text{Sym}(3)$. On one hand, since λ_a is an automorphism of the group A ,

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

On the other hand,

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

Definition 1.10. Let χ be a family of groups. A skew brace A is said to be of χ -type if its additive group belongs to χ .

Example 1.11. The skew braces of abelian type are the skew braces with an abelian additive group. In Section 1.5, we will establish the link between that type of skew braces and the notion of left braces introduced by Rump. Moreover, the Theorem 2.14 will prove that the solution of the Yang-Baxter equation associated to a skew brace of abelian type is involutive.

The following example gives us a general way to build some concrete examples of skew braces.

Example 1.12. Let A be an additive group, B and C be subgroups of A such that $B \cap C = \{0\}$ and $A = B + C$, i.e. A admits an exact factorization through the subgroups B and C . Each $a \in A$ can be written uniquely as $a = b + c$ for some $b \in B$ and $c \in C$. We define the bijective application

$$f: B \times C^{op} \rightarrow A, (b, c) \mapsto b + c,$$

where $(C^{op}, +^{op})$ is the group with the elements of C and with the operation $+^{op}$ such that, for all $c_1, c_2 \in C$, $c_1 +^{op} c_2 = c_2 + c_1$. We also define the operation $\circ: A \times A \rightarrow A$ by setting $a \circ a_1 = f(f^{-1}(a) + f^{-1}(a_1))$. With that operation, $(A, \circ)$ is a group. Let $a = b + c$, $a_1 = b_1 + c_1$ for $b, b_1 \in B$ and $c, c_1 \in C$. Then we can write the operation $\circ$ as

$$a \circ a_1 = f((b, c) + (b_1, c_1)) = f(b + b_1, c_1 + c) = b + b_1 + c_1 + c = b + a_1 + c.$$

If $x, y \in A$, then

$$\begin{aligned} a \circ x - a + a \circ y &= b + x + c - (b + c) + b + y + c \\ &= b + x + y + c \\ &= a \circ (x + y). \end{aligned}$$

This allows us to conclude that $(A, +, \circ)$ is a skew brace.

For instance, we can apply that structure of examples to the group $\text{GL}_n(\mathbb{C})$, for some positive integer n .

The next lemma gives some useful results for the computations with skew braces and its left distributive identity.

Lemma 1.13. *Let A be a skew brace. Then the following properties hold:*

1. $a \circ (-b + c) = a - (a \circ b) + (a \circ c) \quad \forall a, b, c \in A;$
2. $a \circ (b - c) = (a \circ b) - (a \circ c) + a \quad \forall a, b, c \in A.$

Proof. The left distributive condition implies that $a \circ (b + c) = a \circ b - a + a \circ c$, for all $a, b, c \in A$.

1. One sets $d = b + c$. Then $a \circ d = a \circ b - a + a \circ (-b + d)$, which is equivalent to $a \circ (-b + d) = a - (a \circ b) + (a \circ d)$.
2. One sets $d = b + c$. Then $a \circ d = a \circ (d - c) - a + a \circ c$, which is equivalent to $a \circ (d - c) = (a \circ d) - (a \circ c) + a$.

□

From the point 1 of the previous proposition, we obtain that, for all a, b in a skew brace $(A, +, \circ)$,

$$a \circ (-b) = a - (a \circ b) + a \circ 0 = a - a \circ b + a.$$

Proposition 1.14. *Let A be a skew brace. For each $a \in A$, the map*

$$\lambda_a: A \rightarrow A, b \mapsto -a + (a \circ b)$$

is an automorphism of $(A, +)$. Moreover, the map $\lambda: (A, \circ) \rightarrow \text{Aut}(A, +)$ defined by $\lambda(a) = \lambda_a$ is a group homomorphism.

Proof. First, one proves that, for all $a \in A$, $\lambda_a \in \text{Aut}(A, +)$, i.e. λ_a is bijective and preserves the additive structure. Let $a \in A$. One defines the inverse of λ_a , denoted by λ_a^{-1} , by setting $\lambda_a^{-1}(b) = a' \circ (a + b)$. This map is the inverse of λ_a since, for all $b \in A$, by associativity of the operations $\circ$ and $+$,

$$\begin{aligned} \lambda_a \lambda_a^{-1}(b) &= \lambda_a(a' \circ (a + b)) \\ &= -a + (a \circ (a' \circ (a + b))) \\ &= -a + ((a \circ a') \circ (a + b)) \\ &= -a + (a + b) \\ &= b, \end{aligned}$$

and

$$\begin{aligned} \lambda_a^{-1} \lambda_a(b) &= \lambda_a^{-1}(-a + (a \circ b)) \\ &= a' \circ (a + (-a + (a \circ b))) \\ &= a' \circ ((a + (-a)) + (a \circ b)) \\ &= a' \circ (a \circ b) \\ &= b. \end{aligned}$$

It remains to prove that λ_a preserves the structure of the addition, i.e.

$$\lambda_a(b + c) = \lambda_a(b) + \lambda_a(c),$$

for all $b, c \in A$. Indeed, by the left distributive condition of a skew brace,

$$\begin{aligned} \lambda_a(b + c) &= -a + a \circ (b + c) \\ &= -a + a \circ b - a + a \circ c \\ &= \lambda_a(b) + \lambda_a(c). \end{aligned}$$

Next, one shows that the map $\lambda: (A, \circ) \rightarrow \text{Aut}(A, +)$ is a group homomorphism. For

all $a, b \in A$, one can rewrite the definition of $\lambda_a(b)$ by $\lambda_a(b) = a \circ (a' + b)$. Indeed,

$$a \circ (a' + b) = a \circ a' - a + a \circ b = -a + a \circ b = \lambda_a(b).$$

Then, for all $a, b, c \in A$,

$$\begin{aligned} \lambda_a(\lambda_b(c)) &= \lambda_a(b \circ (b' + c)) \\ &= -a + a \circ b \circ (b' + c) \\ &= -a + a \circ b \circ b' - a \circ b + a \circ b \circ c \\ &= -a \circ b + a \circ b \circ c \\ &= \lambda_{a \circ b}(c). \end{aligned}$$

It follows that λ is a group homomorphism. $\square$

Remark 1.15. With the definition of the map λ , the operation $\circ$ can be written in terms of the operation $+$ and conversely. Indeed, for all $a, b \in A$, $a \circ b = a + \lambda_a(b)$, $a + b = a \circ \lambda_a^{-1}(b) = a \circ \lambda_{a'}(b)$ and $\lambda_a(a') = -a$.

Remark 1.16. Let $a \in A$. If one writes id_A for the identity map on A , then

$$\begin{aligned} \lambda_a = \text{id}_A &\Leftrightarrow \forall x \in A, \lambda_a(x) = x \\ &\Leftrightarrow \forall x \in A, -a + (a \circ x) = x \\ &\Leftrightarrow \forall x \in A, a \circ x = a + x. \end{aligned}$$

So, $\ker(\lambda) = \{a \in A \mid \lambda_a = \text{id}_A\} = \{a \in A \mid \forall x \in A, a \circ x = a + x\}$ is a normal subgroup of $(A, \circ)$.

Considering the Proposition 1.14, for a skew brace A , the map λ yields a left action from $(A, \circ)$ on $(A, +)$ by automorphisms.

We can also define a right action of $(A, \circ)$ on the set A .

Proposition 1.17. *Let A be a skew brace. For all $a \in A$, the map*

$$\mu_a: A \rightarrow A, b \mapsto \lambda_b(a)' \circ b \circ a$$

is bijective. Moreover, the map

$$\mu: (A, \circ) \rightarrow \text{Sym}(A), a \mapsto \mu_a$$

satisfies, for all $a, b \in A$, the identity $\mu_b \mu_a = \mu_{a \circ b}$.

In the previous statement, the notation $\text{Sym}(A)$ denotes the symmetric group of A , i.e. the group of bijective maps from A to A . We now prove this proposition.

Proof. By definition of λ , we get another way to define $\mu_a(b)$ for $a, b \in A$:

$$\mu_a(b) = \lambda_b(a)' \circ b \circ a = (b \circ (b' + a))' \circ b \circ a = (b' + a)' \circ a.$$

From this definition of μ_a , we can deduce its inverse map:

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

We can easily check that μ_a and μ_a^{-1} are inverses of each other.

Finally, for all $a, b, c \in A$,

$$\begin{aligned} \mu_b(\mu_a(c)) &= \mu_b((c' + a)' \circ a) \\ &= (a' \circ (c' + a) + b)' \circ b \\ &= (a' \circ c' - a' + b)' \circ b \\ &= (a' \circ (c' + a \circ b))' \circ b \\ &= (c' + a \circ b)' \circ a \circ b \\ &= \mu_{a \circ b}(c). \end{aligned}$$

□

The previous proposition also implies that μ is a right action of $(A, \circ)$ on A . Those two group actions (λ and μ) will be meaningful in the framework of solutions of the Yang-Baxter Equation associated to skew braces.

The map λ gives a characterization of the maps that are skew brace morphisms. We describe it in the following lemma.

Lemma 1.18. *Let A and B be skew braces. A map $f: A \rightarrow B$ is a skew brace morphism if and only if $f(a \circ b) = f(a) \circ f(b)$ and $f(\lambda_a(b)) = \lambda_{f(a)}(f(b))$ for all $a, b \in A$.*

Proof. " $\Rightarrow$ " Let $a, b \in A$. The equality $f(a \circ b) = f(a) \circ f(b)$ follows by definition of skew brace morphism. For the second one,

$$f(\lambda_a(b)) = f(-a + (a \circ b)) = -f(a) + (f(a) \circ f(b)) = \lambda_{f(a)}(f(b)),$$

by definition of skew brace morphism and of the map $\lambda: (A, \circ) \rightarrow \text{Aut}(A, +)$.

" $\Leftarrow$ " Let $a, b \in A$. We just have to prove that, for all $a, b \in A$, $f(a + b) = f(a) + f(b)$. The addition operation can be expressed in terms of the operation $\circ$ and the map λ (by

Remark 1.15), hence we get

$$\begin{aligned}
f(a + b) &= f(a \circ \lambda_{a'}(b)) \\
&= f(a) \circ f(\lambda_{a'}(b)) \\
&= f(a) \circ \lambda_{f(a')}(f(b)) \\
&= f(a) \circ \lambda_{f(a)'}(f(b)) \\
&= f(a) + f(b).
\end{aligned}$$

□

The same lemma with the condition $f(a + b) = f(a) + f(b)$ instead of the condition $f(a \circ b) = f(a) \circ f(b)$ also holds.

Now, we introduce another type of skew braces that will be useful for the study of solutions of the Yang-Baxter Equation.

Definition 1.19. A skew brace A is said to be a two-sided skew brace if

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

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

Hence, a two-sided skew brace is a skew (left) brace that is also a skew right brace. Let us see some examples of this special type of skew braces.

Example 1.20. The Example 1.7 of skew brace $(A, +, +)$ is in fact a two-sided skew brace. Indeed, for all $a, b, c \in A$,

$$(a + c) - c + (b + c) = a + (b + c) = (a + b) + c,$$

by associativity of the addition.

Example 1.21. Any skew brace with abelian multiplicative group is two-sided. Let $(A, +, \circ)$ be a skew brace such that $(A, \circ)$ is abelian. Then, for all $a, b, c \in A$, by commutativity of the multiplication and by the left distributive condition of the skew brace,

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

The next example was inspired by Mara Pompili's thesis, see [37, Examples 1.5].

Example 1.22. Let $\mathbb{Z}/n\mathbb{Z}$ be the cyclic group of n elements endowed with the natural addition $+$ of $\mathbb{Z}/n\mathbb{Z}$. One defines the second operation as follows: for all $a, b \in \mathbb{N}$,

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

Then $(\mathbb{Z}/n\mathbb{Z}, +, \circ)$ is a two-sided skew brace if and only if $n \in \{1, 2, 4\}$.

Indeed, $(\mathbb{Z}/n\mathbb{Z}, \circ)$ is a group. Let us check that the operation $\circ$ is associative. Let $a, b, c \in \mathbb{N}$: on one hand,

$$\begin{aligned}(a \circ b) \circ c &= (-1)^c(a \circ b) + c \\ &= (-1)^c((-1)^b a + b) + c \\ &= (-1)^{c+b} a + (-1)^c b + c.\end{aligned}$$

On the other hand,

$$a \circ (b \circ c) = (-1)^{b \circ c} a + (b \circ c) \quad (1.1)$$

$$= (-1)^{(-1)^{c+b+c}} a + (-1)^c b + c. \quad (1.2)$$

In order to have the equality between the two terms, we need to check the sign of the terms $(-1)^{(-1)^{c+b+c}}$ and $(-1)^{c+b}$. If c is even, the sign of $(-1)^{(-1)^{c+b+c}}$ is the same as the sign of $(-1)^{c+b}$, because $(-1)^{c+b+c} = c+b$. If c is odd, one gets that $(-1)^{c+b+c} = -b+c$. So, the sign of $(-1)^{c+b}$ is equal to the sign of $(-1)^{(-1)^{c+b+c}} = (-1)^{-b+c}$ if and only if $b \equiv -b \pmod{2}$, which is always satisfied. Therefore, the operation $\circ$ is associative. Moreover, the operation $\circ$ has a neutral element: 0. Indeed, $0 \circ b = (-1)^b 0 + b = b$ and $a \circ 0 = (-1)^0 a + 0 = a$, for every $a, b \in \mathbb{N}$. Finally, every element has an inverse. Let $a \in \mathbb{N}$. If a is even, its inverse is $-a$. Indeed,

$$a \circ (-a) = (-1)^{(-a)} a + (-a) = a + (-a) = 0,$$

and

$$(-a) \circ a = (-1)^a (-a) + a = -a + a = 0.$$

If a is odd, its inverse is a :

$$a \circ a = (-1)^a a + a = -a + a = 0.$$

Moreover, we check the distributive conditions of the definition of a two-sided skew brace. Let $a, b, c \in \mathbb{N}$.

For the left distributive condition, we have

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

and, on the other hand,

$$\begin{aligned}a \circ b - a + a \circ c &= (-1)^b a + b - a + (-1)^c a + c \\ &= ((-1)^b - 1 + (-1)^c) a + b + c.\end{aligned}$$

We get the left distributive condition if and only if

$$\begin{aligned} (-1)^{b+c}a + b + c &\equiv ((-1)^b - 1 + (-1)^c)a + b + c \pmod{n} \\ \Leftrightarrow (-1)^{b+c} &\equiv (-1)^b - 1 + (-1)^c \pmod{n}. \end{aligned}$$

If b and c are both even and if one is even and the other one is odd, the condition is verified for all $n \in \mathbb{N}$. But when b and c are both odds,

$$(-1)^{b+c} \equiv (-1)^b - 1 + (-1)^c \pmod{n} \Leftrightarrow 1 \equiv -3 \pmod{n} \Leftrightarrow n \text{ divides } 4.$$

This last statement implies that the triple is a skew left brace if and only if $n \in \{1, 2, 4\}$.

Now, we check the right distributive condition. First, we have

$$(a + b) \circ c = (-1)^c(a + b) + c,$$

and, on the other hand,

$$\begin{aligned} a \circ c - c + b \circ c &= (-1)^c a + c - c + (-1)^c b + c \\ &= (-1)^c(a + b) + c. \end{aligned}$$

Hence, the triple always satisfies the right distributive condition. Therefore, we can conclude that $(\mathbb{Z}/n\mathbb{Z}, +, \circ)$ is a two-sided skew brace if and only if $n \in \{1, 2, 4\}$.

The lemma 1.5 has a dual statement for the skew right braces, stated in Lemma 1.23. Therefore, the two-sided skew braces satisfy these two lemmas.

Lemma 1.23. *Let A be a skew right brace. Then the following properties hold:*

1. $0 = 1$;
2. $(-a + b) \circ c = c - (a \circ c) + (b \circ c)$, for all $a, b, c \in A$;
3. $(a - b) \circ c = a \circ c - b \circ c + c$, for all $a, b, c \in A$.

The proof is similar to the one of the left case.

Therefore, if A is a skew right brace, for all $a, b \in A$,

$$(-a) \circ b = b - a \circ b + 0 \circ b = b - a \circ b + b.$$

1.2 Ideals

Another important part of the study of an algebraic structure is the definition and properties of its subobjects and ideals. These two concepts will allow us to state and prove the

Noether isomorphism theorems for skew braces. The given definitions are the one mentioned by Ferran Cedó and Leandro Vendramin in their book [18].

Definition 1.24. Let $(A, +, \circ)$ be a skew brace. Let I be a subset of A .

1. One says that I is a subbrace of A if $(I, +)$ is a subgroup of $(A, +)$ and $(I, \circ)$ is a subgroup of $(A, \circ)$.
2. One says that I is a left ideal of A if $(I, +)$ is a subgroup of $(A, +)$ such that $\lambda_a(I) \subseteq I$ for all $a \in A$.
3. One says that I is an ideal of A if $(I, +)$ is a normal subgroup of $(A, +)$ and $(I, \circ)$ is a normal subgroup of $(A, \circ)$ such that $\lambda_a(I) \subseteq I$ for all $a \in A$.

The following proposition gives an equivalence with another definition of an *ideal* of a skew brace.

Proposition 1.25. Let $(A, +, \circ)$ be a skew brace. Let I be a subset of A such that $(I, +)$ is a normal subgroup of $(A, +)$ and $(I, \circ)$ is a normal subgroup of $(A, \circ)$. Then I is an ideal of A if and only if $a + I = a \circ I$ for all $a \in A$.

Proof. " $\Rightarrow$ " First, we suppose that I is an ideal of A . Let $a \in A$, $i \in I$. Then, by definition of ideal, $\lambda_a(i) = -a + a \circ i \in I$, which means that there exists $\tilde{i} \in I$ such that

$$\begin{aligned}\lambda_a(i) = \tilde{i} &\Leftrightarrow -a + a \circ i = \tilde{i} \\ &\Leftrightarrow a \circ i = a + \tilde{i}.\end{aligned}$$

From this, we conclude that, for all $a \in A$, $a + I = a \circ I$.

" $\Leftarrow$ " Conversely, let $a \in A$, $i \in I$. Then

$$\lambda_a(i) = -a + (a \circ i) = -a + (a + i_0) = -a + i_1 + a,$$

for some $i_0, i_1 \in I$ since $a + I = a \circ I$ and $(I, +)$ is a normal subgroup of $(A, +)$. Again by the normality of $(I, +)$, $-a + i_1 + a \in I$, so $\lambda_a(i) \in I$. $\square$

Proposition 1.26. A left ideal I of a skew brace A is a subbrace.

Proof. We just need to prove that $(I, \circ)$ is a subgroup of $(A, \circ)$. First, I is non empty since it is an additive subgroup of A .

Let $x, y \in I$. Then $x \circ y = x + \lambda_x(y) \in I + I \subseteq I$, since $\lambda_x(I) \subseteq I$ for all $x \in A$, moreover, $x' = -\lambda_{x'}(x) \in I$. From this, we can conclude that I is a subbrace of A . $\square$

Proposition 1.27. Let S be a set.

1. Let $\{B_\alpha\}_{\alpha \in S}$ be a family of subbraces of a skew brace A . Then $\bigcap_{\alpha \in S} B_\alpha$ is a subbrace of A .
2. Let $\{I_\alpha\}_{\alpha \in S}$ be a family of ideals of a skew brace A . Then $\bigcap_{\alpha \in S} I_\alpha$ is an ideal of A .

Proof. 1. For all $\alpha \in S$, B_α is a subgroup of $(A, +)$ and $(A, \circ)$. Therefore, $\bigcap_{\alpha \in S} B_\alpha$ is a subgroup of $(A, +)$ and $(A, \circ)$ and hence a subbrace of A .

2. For all $\alpha \in S$, I_α is a normal subgroup of $(A, +)$ and $(A, \circ)$. Therefore, $\bigcap_{\alpha \in S} I_\alpha$ is a normal subgroup of $(A, +)$ and $(A, \circ)$. The last thing to show is that, for all $a \in A$,

$$\lambda_a \left(\bigcap_{\alpha \in S} I_\alpha \right) \subseteq \bigcap_{\alpha \in S} I_\alpha.$$

Let $a \in A, x \in \bigcap_{\alpha \in S} I_\alpha$. Then, for all $\alpha \in S$, $x \in I_\alpha$ which implies, since each I_α is an ideal, that $\lambda_a(x) \in I_\alpha$. Hence, $\lambda_a(x) \in \bigcap_{\alpha \in S} I_\alpha$ and $\bigcap_{\alpha \in S} I_\alpha$ is an ideal of A . □

Definition 1.28. Let I and J be subsets of A . We define

$$I + J = \{i + j \mid i \in I, j \in J\} \text{ and } I \circ J = \{i \circ j \mid i \in I, j \in J\}.$$

Lemma 1.29. Let A be a skew brace, B a subbrace of A and I an ideal of A . The following properties hold:

1. $B + I = B \circ I$;
2. $B + I = B \circ I$ is a subbrace of A ;
3. if $B = J$ is an ideal of A , then $J + I = J \circ I$ is an ideal of A .

Proof. 1. We clearly have that $B + I = \bigcup_{b \in B} b + I$ and $B \circ I = \bigcup_{b \in B} b \circ I$. But, for all $b \in B$, $b + I = b \circ I$ since I is an ideal. Therefore,

$$B + I = \bigcup_{b \in B} b + I = \bigcup_{b \in B} b \circ I = B \circ I.$$

2. Since $(B + I, +)$ is a subgroup of $(A, +)$ and $(B \circ I, \circ)$ is a subgroup of $(A, \circ)$, $(B + I, +, \circ)$ is a subbrace of A .
3. Let $a \in A$. We prove that $J + I$ is a normal subgroup of A such that $a \circ (J + I) = a + (J + I)$ for all $a \in A$. First, by 2, one knows that $J + I$ is a subbrace of A . Moreover, let $a \in A, i \in I, j \in J$. Since J and I are ideals of A , it follows that

$$a + (j + i) - a = a + j - a + a + i - a \in J + I.$$

Hence, $J + I$ is a normal subgroup of A . Now, let $a \in A$, by the first point of this proposition, by the Remark 1.15 and since I and J are ideals of A ,

$$\begin{aligned}
a \circ (J + I) &= a \circ (J \circ I) \\
&= a \circ \left(\bigcup_{j \in J} j \circ I \right) \\
&= \bigcup_{j \in J} (a \circ j) \circ I \\
&\stackrel{1.15}{=} \bigcup_{j \in J} (a + \lambda_a(j)) \circ I \\
&= \bigcup_{j \in J} (a + \lambda_a(j) + I) \\
&\subseteq a + (J + I).
\end{aligned}$$

In a similar way, we obtain that $a + (J + I) \subseteq a \circ (J + I)$.

□

For a skew brace A and an ideal I of A , one considers the canonical quotient map

$$\pi_I: A \rightarrow A/I$$

defined by $\pi_I(a) = a + I = a \circ I$, for $a \in A$.

Lemma 1.30. *Let A be a skew brace and let $I \subseteq A$ be an ideal. Then I and A/I are skew braces.*

Proof. By definition of an ideal, I is a normal subgroup of $(A, +)$ and $(A, \circ)$. Since I is a subset of A and the left distributive condition is satisfied for every element of A , it is also satisfied for every element of I . Then I is a skew brace.

On the other hand, since $a + I = a \circ I$ for all $a \in A$, the quotient groups A/I for both operations $+$ and $\circ$ are the same, and then A/I is a skew brace with the naturally induced operations:

$$\begin{aligned}
\circ_q: A/I \times A/I &\rightarrow A/I, (a \circ I, b \circ I) \mapsto (a \circ b) \circ I, \\
+_q: A/I \times A/I &\rightarrow A/I, (a + I, b + I) \mapsto (a + b) + I.
\end{aligned}$$

□

The next proposition gives an insight of a categorical property of skew braces, which is that ideals are exactly the normal monomorphisms (i.e. kernels). The precise statement and proof of this correspondence are given in Lemma 3.15.

Proposition 1.31. *Let $f: A \rightarrow B$ be a skew brace morphism.*

1. *The image of f , $\text{Im}(f)$, is a subbrace of B .*
2. *The kernel of f , $\ker(f)$, is an ideal of A .*
3. *Every ideal is the kernel of a skew brace morphism.*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow & \nearrow \\ & \text{Im}(f) & \end{array}$$

Proof. 1. Let $b_1, b_2 \in \text{Im}(f)$. Then there exist $a_1, a_2 \in A$ such that $f(a_1) = b_1$ and $f(a_2) = b_2$. One first shows that $(\text{Im}(f), +)$ is a subgroup of $(A, +)$. Indeed, $b_1 + b_2 = f(a_1) + f(a_2) = f(a_1 + a_2)$, $-b_1 = -f(a_1) = f(-a_1)$ and $0 = f(0)$. Similarly, $(\text{Im}(f), \circ)$ is a subgroup of $(A, \circ)$.

2. The kernel of f is a normal subgroup of $(A, +)$ and $(A, \circ)$. Indeed, let $x, y \in \ker(f)$ and $a \in A$, then $f(x \circ y') = f(x) \circ f(y)' = 0$ and

$$f(a' \circ x \circ a) = f(a)' \circ f(x) \circ f(a) = f(a)' \circ f(a) = 0.$$

Hence, $\ker(f)$ is a normal subgroup of $(A, \circ)$. On the other hand, $f(x - y) = f(x) - f(y) = 0$ and $f(a + x - a) = f(a) + f(x) - f(a) = f(a) - f(a) = 0$, so $\ker(f)$ is a normal subgroup of $(A, +)$.

Moreover, let $a \in A$, $x \in \ker(f)$, by Lemma 1.18,

$$f(\lambda_a(x)) = \lambda_{f(a)}(f(x)) = \lambda_{f(a)}(0) = 0.$$

So $\lambda_a(x) \in \ker(f)$. It means that $\lambda_a(\ker(f)) \subseteq \ker(f)$. One concludes that $\ker(f)$ is an ideal of A .

3. Let I be an ideal of a skew brace A . One considers the canonical projection

$$\pi_I: A \rightarrow A/I, a \mapsto a \circ I.$$

By construction, $I = \ker(\pi_I)$. Moreover, π_I is a skew brace morphism: let $a, b \in A$,

$$\pi_I(a \circ b) = (a \circ b) \circ I = (a \circ I) \circ (b \circ I) = \pi_I(a) \circ \pi_I(b),$$

$$\pi_I(a + b) = (a + b) + I = (a + I) + (b + I) = \pi_I(a) + \pi_I(b).$$

Hence, the ideal I is the kernel of the skew brace morphism π_I .

□

1.3 Isomorphism theorems

We now prove the Noether isomorphism theorems for skew braces. The proofs are based on [37].

Theorem 1.32. *Let $f: A \rightarrow B$ be a skew brace morphism. Then*

$$A/\ker(f) \cong \text{Im}(f).$$

Proof. The objective is to build an isomorphism

$$\phi: A/\ker(f) \rightarrow \text{Im}(f).$$

We define $\phi(a + \ker(f)) = f(a)$. We have to prove that ϕ is well defined, a skew brace morphism, injective and surjective.

1. " ϕ is well defined": Let $a, b \in A$ such that $a + \ker(f) = b + \ker(f)$. Then $a - b \in \ker(f)$ and we get

$$f(a - b) = 0 \Leftrightarrow f(a) - f(b) = 0 \Leftrightarrow f(a) = f(b) \Leftrightarrow \phi(a + \ker(f)) = \phi(b + \ker(f)).$$

2. " ϕ is a skew brace morphism": Let $a, b \in A$. Then, by definition of ϕ and since f is a skew brace morphism,

$$\begin{aligned} \phi((a + \ker(f)) + (b + \ker(f))) &= \phi((a + b) + \ker(f)) \\ &= f(a + b) \\ &= f(a) + f(b) \\ &= \phi(a + \ker(f)) + \phi(b + \ker(f)) \end{aligned}$$

and

$$\begin{aligned} \phi((a + \ker(f)) \circ (b + \ker(f))) &= \phi((a \circ b) + \ker(f)) \\ &= f(a \circ b) \\ &= f(a) \circ f(b) \\ &= \phi(a + \ker(f)) \circ \phi(b + \ker(f)). \end{aligned}$$

3. " ϕ is injective": Let $a \in A$ be such that $\phi(a + \ker(f)) = 0$. It implies that

$$f(a) = 0 \Leftrightarrow a \in \ker(f) \Leftrightarrow a + \ker(f) = \ker(f),$$

and hence ϕ is injective.

4. " ϕ is surjective": Let $b \in \text{Im}(f)$. Then there exists $a \in A$ such that $f(a) = b$, i.e. $b = \phi(a + \ker(f))$ and ϕ is surjective. $\square$

To illustrate the proof of the second isomorphism theorem, we will draw a diagram containing short exact sequences. We first recall the notions related to a short exact sequence in the context of skew braces.

The kernel morphism $\ker(f)$ of a morphism $f: A \rightarrow B$ is a morphism

$$\ker(f): K \rightarrow A$$

such that $f \ker(f) = 0$ and, for any morphism $u: Z \rightarrow A$ with $fu = 0$, there exists a unique morphism $\phi: Z \rightarrow K$ such that $\ker(f)\phi = u$, as in the following diagram.

$$\begin{array}{ccccc} K & \xrightarrow{\ker(f)} & A & \xrightarrow{f} & B \\ \uparrow \phi & & \nearrow u & & \\ Z & & & & \end{array}$$

The cokernel morphism $\operatorname{coker}(f)$ of a morphism $f: A \rightarrow B$ is a morphism

$$\operatorname{coker}(f): B \rightarrow Q$$

such that $\operatorname{coker}(f)f = 0$ and, for any morphism $v: B \rightarrow X$ with $vf = 0$, there exists a unique morphism $\psi: Q \rightarrow X$ such that $\psi \operatorname{coker}(f) = v$, as in the following diagram.

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \xrightarrow{\operatorname{coker}(f)} & Q \\ & & \searrow v & & \downarrow \psi \\ & & & & X \end{array}$$

If $p: A \rightarrow B$ is a surjective morphism, then $p = \operatorname{coker}(\ker(p))$. A short exact sequence is a diagram

$$0 \longrightarrow K \xrightarrow{k} A \xrightarrow{p} B \longrightarrow 0$$

such that $k = \ker(p)$ and $p = \operatorname{coker}(k)$. In this thesis, the notation $\xrightarrow{\sim}$ illustrates a monomorphism and the notation $\twoheadrightarrow$ a regular epimorphism.

We now state the second isomorphism theorem.

Theorem 1.33. *Let A be a skew brace. For every subbrace B of A and every ideal I of A , there is the following isomorphism*

$$(B + I)/I \cong B/(B \cap I).$$

Proof. The proof of this theorem is an easy application of the first isomorphism theorem 1.32. One defines a morphism

$$f: B \rightarrow (B + I)/I, b \mapsto b + I.$$

1. " f is a skew brace morphism": Indeed, let $b, b' \in B$,

$$f(b + b') = (b + b') + I = (b + I) + (b' + I) = f(b) + f(b'),$$

and

$$f(b \circ b') = (b \circ b') \circ I = (b \circ I) \circ (b' \circ I) = f(b) \circ f(b').$$

2. " f is surjective": Let $b \in B, i \in I$, then $(b + i) + I \in (B + I)/I$ and $(b + i) + I = b + I = f(b)$.
3. " $\ker(f)$ ": $\ker(f) = \{b \in B \mid f(b) = I\} = \{b \in B \mid b + I = I\} = B \cap I$.

By applying the first isomorphism theorem, one gets that

$$B/\ker(f) \cong \text{Im}(f) \Leftrightarrow B/(B \cap I) \cong (B + I)/I.$$

The following diagram illustrates the proof, where the rows are short exact sequences:

$$\begin{array}{ccccccc} 0 & \longrightarrow & B \cap I & \longrightarrow & B & \longrightarrow & \frac{B}{B \cap I} \longrightarrow 0 \\ & & \downarrow & & \downarrow & \searrow f & \downarrow \\ 0 & \longrightarrow & I & \longrightarrow & B + I & \longrightarrow & \frac{B + I}{I} \longrightarrow 0. \end{array}$$

□

We finally prove the third isomorphism theorem.

Theorem 1.34. *Let I, J be ideals of a skew brace A such that $I \subseteq J$. Then*

$$\frac{A/I}{J/I} \cong A/J.$$

Proof. It is also an application of the first isomorphism theorem [1.32](#). One defines a morphism

$$f: A/I \rightarrow A/J, a + I \mapsto a + J.$$

1. " f is well defined": Let $a, b \in A$ such that $a + I = b + I$. Then $a - b \in I \subseteq J$ which implies $a + J = b + J$.
2. " f is a skew brace morphism": Let $a, b \in A$. Then

$$f((a + I) + (b + I)) = f((a + b) + I) = (a + b) + J = (a + J) + (b + J) = f(a + I) + f(b + I).$$

Similarly, one checks that $f((a + I) \circ (b + I)) = f(a + I) \circ f(b + I)$.

3. " f is surjective": Let $a \in A$. Then $a + J = f(a + I)$.

4. " $\ker(f)$ ": We compute the kernel of f as follows:

$$\begin{aligned}\ker(f) &= \{a + I \in A/I \mid f(a + I) = J\} = \{a + I \in A/I \mid a + J = J\} \\ &= \{a + I \in A/I \mid a \in J\} = J/I.\end{aligned}$$

By applying the first isomorphism theorem, it follows that

$$\frac{A/I}{\ker(f)} \cong \text{Im}(f) \Leftrightarrow \frac{A/I}{J/I} \cong A/J.$$

The following diagram illustrates the proof.

$$\begin{array}{ccccc} I & \longrightarrow & J & \twoheadrightarrow & J/I \\ & \searrow & \downarrow & & \downarrow \\ & & A & \twoheadrightarrow & A/I \\ & & \downarrow & \nearrow f & \downarrow \\ & & A/J & \cong & \frac{A/I}{J/I} \end{array}$$

□

1.4 Radical rings

As briefly said, skew braces are a generalization of radical rings. It is interesting to recall the definition of that notion and to make clear and rigorous the link between these two algebraic structures.

This section is grounded on [18, Chapter 3].

1.4.1 Jacobson radical of a ring

To get the definition of a radical ring, one first needs to define the Jacobson radical of a ring. This notion was introduced by Nathan Jacobson in 1945, see [31].

Definition 1.35. *Let R be a ring. Let M be an R -module and S a subset of M . The annihilator of S is*

$$\text{Ann}_R(S) = \{a \in R \mid as = 0 \ \forall s \in S\}.$$

Definition 1.36. *A module M is simple if $M \neq \{0\}$ and if $\{0\}$ and M are the only submodules of M .*

Definition 1.37. Let R be a ring. The Jacobson radical of R is defined by

$$J(R) = \bigcap_{V \text{ simple } R\text{-module}} \text{Ann}_R(V).$$

Remark 1.38. Since each $\text{Ann}_R(V)$ is an ideal of R , $J(R)$ is also an ideal of R .

The following theorem and its proof can be found in [18, Theorem 3.2.2].

Theorem 1.39. Let R be a ring and $a \in R$. Then the following are equivalent:

1. $a \in J(R)$;
2. $a \in M$, for every maximal left ideal M of R ;
3. $R(1 - xa) = R$, for all $x \in R$;
4. $1 - xay$ is invertible, for all $x, y \in R$;
5. the dual left-right conditions of the fourth previous conditions.

From the previous theorem, one can deduce an equivalent definition of Jacobson radical.

Proposition 1.40. Let R be a ring. Let $\text{Max}_l(R)$ denote the set of maximal left ideals of R . Then the Definition 1.37 of Jacobson radical of R is equivalent to

$$J(R) = \bigcap_{L \in \text{Max}_l(R)} L.$$

1.4.2 Definition and characterization of radical rings

All the tools presented in the previous subsection enable us to define a radical ring.

Definition 1.41. Let S be a ring without unit. We say that S is a radical ring if it is isomorphic to the Jacobson radical of a ring (with unit).

The following proposition allows us to characterize radical rings in a more convenient way. We will see later that this proposition is similar to a proposition Rump proved in the first steps of the theory of braces.

Proposition 1.42. Let S be a ring without unit (or with unit). Define on S the operation $\circ : S \times S \rightarrow S, (a, b) \mapsto a \circ b = a + b + ab$. Then S is a radical ring if and only if $(S, \circ)$ is a group.

Proof. " $\Rightarrow$ ": If we first assume that S is a radical ring, we want to prove that $(S, \circ)$ is a group, i.e. the $\circ$ operation applied to two elements of S belongs to S , the associativity of $\circ$, the existence of a neutral element for the $\circ$ operation and of the inverse of each element of S with respect to the $\circ$ operation.

1. Let $a, b \in S$. Then $a \circ b = a + b + ab \in S$ since $(S, +, \cdot)$ is a ring.
2. Let $a, b, c \in S$. Then

$$\begin{aligned}(a \circ b) \circ c &= (a + b + ab) \circ c \\ &= a + b + ab + c + (a + b + ab)c \\ &= a + b + ab + c + ac + bc + abc.\end{aligned}$$

On the other hand,

$$\begin{aligned}a \circ (b \circ c) &= a \circ (b + c + bc) \\ &= a + b + c + bc + a(b + c + bc) \\ &= a + b + c + bc + ab + ac + abc.\end{aligned}$$

Since $(S, +, \cdot)$ is a ring, $(S, +)$ is an abelian group. Hence $(a \circ b) \circ c = a \circ (b \circ c)$.

3. The neutral element of the $\circ$ operation is the same as the neutral element for the addition of the ring, i.e. $e_\circ = 0$. Indeed, let $a \in S$, $0 \circ a = 0 + a + 0a = a$ and $a \circ 0 = a + 0 + a0 = a$.
4. Since S is a radical ring, there exists a ring with unit R such that $S \cong J(R)$. Let $\psi: S \rightarrow R$ be an injective homomorphism of rings without unit such that $\text{Im}(\psi) = J(R)$ (which exists since $S \cong J(R)$). Then, for $a \in S$, by the Theorem 1.39, since $\psi(a) \in J(R)$ and $-1 \in R$, $1 + \psi(a) \in R$ is invertible. So, there exists $c \in R$ such that $(1 + \psi(a))(1 + c) = (1 + c)(1 + \psi(a)) = 1$. This equality is equivalent to

$$1 + c + \psi(a) + \psi(a)c = 1 \Leftrightarrow c = -\psi(a) - \psi(a)c.$$

Therefore, $c = -\psi(a) - \psi(a)c \in J(R)$ since $\psi(a) \in J(R)$ and $J(R)$ is an ideal of R . But $J(R) = \text{Im}(\psi)$, so there exists $b \in S$ such that $\psi(b) = c$. This implies that

$$\begin{aligned}\psi(b) &= -\psi(a) - \psi(a)\psi(b) \Leftrightarrow \psi(a) + \psi(b) + \psi(a)\psi(b) = 0 \\ &\Leftrightarrow \psi(a + b + ab) = 0 \\ &\Leftrightarrow a + b + ab = 0,\end{aligned}$$

where the last equality is a consequence of the fact that ψ is injective. Similarly, we obtain $a + b + ba = 0$. The two results together imply that $a \circ b = 0 = b \circ a$, so b is an inverse for a for the $\circ$ operation. The uniqueness of b is clear. Indeed, if

there exists $\tilde{b} \in S$ such that $a \circ \tilde{b} = 0 = \tilde{b} \circ a$, then

$$a \circ \tilde{b} = a \circ b \Leftrightarrow a + \tilde{b} + a\tilde{b} = a + b + ab \Leftrightarrow \tilde{b}(1 + a) = b(1 + a) \Leftrightarrow \tilde{b} = b,$$

since $1 + a$ is invertible by the condition 4 of Theorem 1.39.

We conclude that $(S, \circ)$ is a group.

" $\Leftarrow$ ": Conversely, we first set $S^1 = \mathbb{Z} \times S$ endowed with the componentwise addition and the multiplication defined as follows: for all $z_1, z_2 \in \mathbb{Z}$ and $a, b \in S$,

$$(z_1, a)(z_2, b) = (z_1 z_2, z_1 b + z_2 a + ab).$$

We can easily check that S^1 is a ring with unit element $(1, 0)$. Moreover, $\{0\} \times S$ is an ideal of S^1 which is naturally isomorphic to S as rings without unit.

To prove that S is a radical ring, we will show that $S \cong J(S^1)$. For that, we will look at the maximal left ideals of S^1 . Let M be a maximal left ideal of S^1 . Since $(S, \circ)$ is a group, for all $a \in S$, there exists $b \in S$ such that $a + b + ab = a + b + ba = 0$, then $(1, a)(1, b) = (1, a + b + ab) = (1, 0) = (1, b)(1, a)$, which means that every element of the form $(1, a)$, with $a \in S$, is invertible. Suppose that, for $a \in S$, $(0, a) \notin M$, then there exist $(z_1, c) \in S^1$ and $(z_2, d) \in M$ such that

$$(z_1, c)(0, a) + (z_2, d) = (1, 0) \Leftrightarrow (0, z_1 a + ca) + (z_2, d) = (1, 0) \Leftrightarrow (z_2, z_1 a + ca + d) = (1, 0).$$

Hence, $z_2 = 1$ and $(1, d) \in M$ which is a contradiction since $(1, d)$ is invertible. Therefore, we know that $\{0\} \times S \subseteq M$ and $M = I \times S$ where I is a maximal ideal of $\mathbb{Z}$. We conclude that $J(S^1) = \{0\} \times S \cong S$ and S is a radical ring. $\square$

1.4.3 Link between radical rings and skew braces

Now that we clearly defined the notion of radical rings, we are going to establish the link between this algebraic structure and skew braces.

Consider a skew brace $(A, +, \circ)$. One defines a new operation on A

$$\begin{aligned} \star: A \times A &\rightarrow A, \\ (a, b) &\mapsto a \star b = \lambda_a(b) - b = -a + a \circ b - b. \end{aligned}$$

Then we have the following identity

$$a \star (b + c) = a \star b + b + a \star c - b. \quad (1.3)$$

The equality is obtained by a simple calculation:

$$\begin{aligned}
a \star (b + c) &= -a + a \circ (b + c) - (b + c) \\
&= -a + a \circ b - a + a \circ c - c - b \\
&= -a + a \circ b - b + b + a \star c - b \\
&= a \star b + b + a \star c - b.
\end{aligned}$$

In [34], Thomas Letourmy and Leandro Vendramin stated a link between radical rings and skew braces.

Theorem 1.43. *A skew brace of abelian type $(A, +, \circ)$ is two-sided if and only if $(A, +, \star)$ is a radical ring.*

Proof. " $\Rightarrow$ ": We want to show that $(A, +, \star)$ is a radical ring. To apply the Proposition 1.42, we need to prove that $(A, +, \star)$ is a non-unitary ring and that $(A, \tilde{\circ})$ is a group with $a \tilde{\circ} b = a + b + a \star b$ for all $a, b \in A$.

By assumption, $(A, +, \circ)$ is a two-sided skew brace of abelian type, hence, $(A, +)$ is an abelian group and $(A, \circ)$ is a group.

For all $a, b \in A$, $a \star b = -b - a + a \tilde{\circ} b = -a + a \circ b - b$, then, by commutativity of the addition, $a \tilde{\circ} b = a \circ b$. Therefore, $(A, \tilde{\circ}) = (A, \circ)$ is a group.

It remains to show that the $\star$ operation is associative and that the left and right distributive conditions hold. Let $a, b, c \in A$. On one hand, we have, by definition of $\star$, by properties of $\star$ and $\circ$ and by commutativity of the addition,

$$\begin{aligned}
a \star (b \star c) &= a \star (-b + b \circ c - c) \\
&= -a + a \circ (-b + b \circ c - c) - (-b + b \circ c - c) \\
&= -a + a \circ (-b) - a + a \circ (b \circ c - c) + c - b \circ c + b \\
&= -a + a \circ (-b) - a + a \circ (b \circ c) - a + a \circ (-c) + c - b \circ c + b \\
&= -a + a - a \circ b + a - a + a \circ (b \circ c) - a + a - a \circ c + a + c - b \circ c + b \\
&= a \circ (b \circ c) - a \circ b - a \circ c - b \circ c + a + b + c.
\end{aligned}$$

On the other hand,

$$\begin{aligned}
(a \star b) \star c &= (-a + a \circ b - b) \star c \\
&= -(-a + a \circ b - b) + (-a + a \circ b - b) \circ c - c \\
&= b - a \circ b + a + (-a) \circ c - c + (a \circ b - b) \circ c - c \\
&= b - a \circ b + a + (-a) \circ c - c + (a \circ b) \circ c - c + (-b) \circ c - c \\
&= b - a \circ b + a + c - a \circ c + c - c + (a \circ b) \circ c - c + c - b \circ c + c - c \\
&= (a \circ b) \circ c - a \circ b - a \circ c - b \circ c + a + b + c.
\end{aligned}$$

By associativity of the $\circ$ operation, we get the associativity of the $\star$ operation.

Moreover, by the equation 1.3, since the addition is commutative, the left distributive condition is satisfied: let $a, b, c \in A$,

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

Finally, we check the right distributive condition: let $a, b, c \in A$, by the commutativity of the addition,

$$\begin{aligned} (a + b) \star c &= -(a + b) + (a + b) \circ c - c \\ &= -b - a + a \circ c - c + b \circ c - c \\ &= -a + a \circ c - c - b + b \circ c - c \\ &= a \star c + b \star c. \end{aligned}$$

From this, we know that $(A, +, \star)$ is a (non-unitary) ring such that $(A, \circ)$ is a group and we get, by applying the Proposition 1.42, that $(A, +, \star)$ is a radical ring.

" $\Leftarrow$ ": If A is a radical ring with ring multiplication $(a, b) \mapsto ab$ for all $a, b \in A$, then the operation on A defined for all $a, b \in A$ by $a \circ b = a + b + ab$ turns A into a two-sided skew brace of abelian type $(A, +, \circ)$. Indeed, $(A, +)$ is an abelian group and $(A, \circ)$ is a group. Moreover, for all $a, b, c \in A$, by commutativity of the addition,

$$\begin{aligned} a \circ b - a + a \circ c &= a + b + ab - a + a + c + ac \\ &= a + b + ab + c + ac \\ &= a + b + c + a(b + c) \\ &= a \circ (b + c). \end{aligned}$$

Finally, for all $a, b, c \in A$, by commutativity of the addition,

$$\begin{aligned} a \circ c - c + b \circ c &= a + c + ac - c + b + c + bc \\ &= a + b + c + ac + bc \\ &= a + b + c + (a + b)c \\ &= (a + b) \circ c. \end{aligned}$$

Therefore, $(A, +, \circ)$ is a two-sided skew brace of abelian type. □

1.5 Historical point on the notion of skew braces

The structure of skew braces, that was introduced in 2017 by Guarnieri and Vendramin, is initiated by other mathematical tools developed earlier.

In [39], Rump was the first to introduce the notion of left braces to study involutive solutions of the Yang-Baxter Equation.

Definition 1.44. *Let $(A, +)$ be an abelian group with a multiplication $A \times A \rightarrow A$. We call A a left brace if the following conditions are satisfied for all $a, b, c \in A$,*

1. $a(b + c) = ab + ac$ (left distributivity);
2. $(ab + a + b)c = a(bc) + ac + bc$;
3. the map $\phi_a: A \rightarrow A, x \mapsto ax + x$ is bijective.

If A is an abelian group with a multiplication $A \times A \rightarrow A$ that satisfies the conditions 1 and 2 from the definition of left brace and the right distributivity, i.e., for all $a, b, c \in A$, $(a + b)c = ac + bc$, then A is an associative ring (without unit). Indeed, we can show that A is associative with respect to the multiplication. Let $a, b, c \in A$. On one hand, by the right distributivity,

$$(ab + a + b)c = (ab)c + ac + bc.$$

On the other hand, by the condition 2,

$$(ab + a + b)c = a(bc) + ac + bc.$$

Since both expressions are equal, we get that $(ab)c = a(bc)$.

The characterization of radical rings in terms of a group as in Proposition 1.42 is inspired by the characterization Rump gave for the left braces.

Indeed, for an abelian group $(A, +)$ with a multiplication, we define the circle operation $a \circ b = ab + a + b$ for $a, b, c \in A$, as for the rings.

Proposition 1.45. *Let $(A, +)$ be an abelian group with a left distributive multiplication. Then A is a left brace if and only if $(A, \circ)$ is a group.*

Proof. " $\Rightarrow$ ": We need to prove that $\circ$ is associative, has a neutral element and that each element of A has an inverse with respect to $\circ$.

1. Associativity: Let $a, b, c \in A$. Then, by the condition 2 of left brace,

$$\begin{aligned} (a \circ b) \circ c &= (ab + a + b) \circ c \\ &= (ab + a + b)c + ab + a + b + c \\ &= a(bc) + ac + bc + ab + a + b + c. \end{aligned}$$

On the other hand, by the left distributivity,

$$\begin{aligned} a \circ (b \circ c) &= a \circ (bc + b + c) \\ &= a(bc + b + c) + a + bc + b + c \\ &= a(bc) + ab + ac + a + bc + b + c. \end{aligned}$$

Since the addition is commutative, $(a \circ b) \circ c = a \circ (b \circ c)$.

2. Neutral element: The neutral element of $\circ$ is 0. Indeed, if $b, c \in A$, then $c \circ 0 = c0 + c$ and $cb = c(b + 0) = cb + c0$, so $c0 = 0$, and this implies that $c \circ 0 = c$. On the other hand, $0 \circ c = 0c + c$. Moreover, the condition 2 of left brace with $a = b = 0$ gives $0c = 0(0c) + 0c + 0c \Leftrightarrow 0 = 0(0c) + 0c$. Since the map $\phi_a: x \mapsto ax + x$ is bijective and $0c$ is in its kernel, $0c = 0$. Hence, $0 \circ c = c$.
3. Inverse of a, for $a \in A$: We want to find $b \in A$ such that $a \circ b = 0 = b \circ a$, i.e. such that $ab + a + b = 0$ and $ba + b + a = 0$. The first condition on b is equivalent to $\phi_a(b) = -a$. Since ϕ_a is bijective, there exists a unique $b \in A$ such that $\phi_a(b) = -a$. So b is a right inverse of a with respect to $\circ$. It is also a left inverse because $a \circ b \circ a = 0 \circ a = a = a \circ 0$ implies $b \circ a = 0$.

" $\Leftarrow$ ": We need to check the three conditions of the definition of left brace.

1. By assumption, the left distributive condition is satisfied.
2. Since $\circ$ is associative, for $a, b, c \in A$,

$$(a \circ b) \circ c = (ab + a + b) \circ c = (ab + a + b)c + ab + a + b + c,$$

and

$$a \circ (b \circ c) = a \circ (bc + b + c) = a(bc + b + c) + a + bc + b + c = a(bc) + ab + ac + a + bc + b + c.$$

By the equality $(a \circ b) \circ c = a \circ (b \circ c)$, we get

$$(ab + a + b)c = a(bc) + ac + bc.$$

3. Let $a \in A$ and $\phi_a: A \rightarrow A, x \mapsto ax + x$. For $x \in A$, $\phi_a(x) = a \circ x - a$. We define the map $\phi_a^{-1}: A \rightarrow A, y \mapsto a' \circ (y + a)$, with a' the inverse of a with respect to $\circ$. We verify that ϕ_a^{-1} is an inverse of ϕ_a : let $x, y \in A$,

$$(\phi_a \phi_a^{-1})(y) = \phi_a(a' \circ (y + a)) = a \circ (a' \circ (y + a)) - a = y,$$

and

$$(\phi_a^{-1} \phi_a)(x) = \phi_a^{-1}(a \circ x - a) = a' \circ ((a \circ x - a) + a) = x.$$

□

Corollary 1.46. *A left brace A is right distributive if and only if it is a radical ring.*

Proof. " $\Rightarrow$ ": Since A is a left brace, A is an abelian group with a left distributive multiplication. So we can apply the Proposition 1.45 and we get that $(A, \circ)$ is a group. Since A is a left brace with right distributivity, A is a ring. Hence, by the equivalence between radical rings and groups in Proposition 1.42, we get that A is a radical ring.

" $\Leftarrow$ ": Since A is a ring, A has a right distributive multiplication. Moreover, since A is a radical ring, $(A, \circ)$ is a group and so, by Proposition 1.45, A is then a left brace. Therefore, A is a left brace with right distributivity. $\square$

Now, we are able to make the link between the theory developed by Rump and the theory of skew braces.

Proposition 1.47. *Let A be an abelian group. Then A is a left brace if and only if A is a skew brace of abelian type.*

Proof. " $\Rightarrow$ ": By assumption, $(A, +)$ is an abelian group. Since A is a left brace, $(A, \circ)$ is a group. Moreover, for $a, b, c \in A$,

$$\begin{aligned} a \circ b - a + a \circ c &= ab + a + b - a + ac + a + c \\ &= ab + ac + a + b + c \\ &= a(b + c) + a + b + c \\ &= a \circ (b + c). \end{aligned}$$

Therefore, $(A, +, \circ)$ is a skew brace of abelian type.

" $\Leftarrow$ ": Let $(A, +, \circ)$ be a skew brace of abelian type. Then $(A, +)$ is an abelian group and $(A, \circ)$ is a group. We define a multiplication on A by setting $ab = a \circ b - a - b$. The left distributivity of the multiplication is satisfied:

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

So, we can apply the Proposition 1.45 and we get that A is a left brace. $\square$

A skew left brace generalizes the notion of left braces to the non-commutative case. Indeed, this notion is less restrictive than the left braces, and also allows us to study the non-involutive solutions of the Yang-Baxter Equation.

1.6 Some adjunctions in the category of skew braces

In this Chapter, we defined different notions that can be linked and compared in a categorical way. We already introduced the category SKB of skew braces. By the one-to-one correspondence between radical rings and two-sided skew braces of abelian type in Theorem 1.43, we can consider the radical rings as a subcategory of SKB denoted by RadRng. Moreover, since left braces are exactly the skew braces of abelian type by Proposition 1.47, left braces can be seen as a subcategory of SKB denoted by BR. We can illustrate the link between these categories with the following diagram of functors.

$$\begin{array}{ccccc}
 & & H & & \\
 & \swarrow & & \searrow & \\
 \text{RadRng} & \xleftarrow{G} & \text{BR} & \xleftarrow{F} & \text{SKB} \\
 & \searrow & & \swarrow & \\
 & & U_R & & U_B
 \end{array}$$

The functors U_R , U_B and its composition $U_B U_R$ are inclusion functors.

The functor $H: \text{SKB} \rightarrow \text{RadRng}$ associates to a skew brace A its universal radical ring $\frac{A}{\text{Rad}(A)}$, where $\text{Rad}(A)$ is the subgroup of $(A, +)$ generated by the elements

$$(a + b) \circ c - b \circ c + c - a \circ c, \quad a + b - a - b,$$

for all $a, b, c \in A$. This subgroup $\text{Rad}(A)$ is an ideal of A , which is called the radicalator of A and is developed and explained in [27]. We can show that H is a left adjoint functor to the functor $U_B U_R$.

The functor $F: \text{SKB} \rightarrow \text{BR}$ maps a skew brace A to $\frac{A}{[A, A]_{\text{SKB}}}$, where $[A, A]_{\text{SKB}}$ is the subgroup of $(A, +)$ generated by the elements $a + b - a - b$, for all $a, b \in A$. We can check that $\frac{A}{[A, A]_{\text{SKB}}}$ is a left brace. We can show that F is a left adjoint functor to U_B .

The functor $G: \text{BR} \rightarrow \text{RadRng}$ maps a left brace A to $\frac{A}{[A, A]_{\text{BR}}}$, where $[A, A]_{\text{BR}}$ is the subgroup of $(A, +)$ generated by the elements $(a + b)c - bc - ac$, for all $a, b, c \in A$. We can check that $\frac{A}{[A, A]_{\text{BR}}}$ is a radical ring. We can show that G is a left adjoint functor to U_R .

As mentioned in Example 1.7, a group defines a skew brace with twice the operation of the group while an abelian group defines a skew brace of abelian type with twice the operation of the group. With a slight abuse of notations, we write Grp to denote the subcategory of SKB formed by skew braces with twice the same operation, which is isomorphic to the usual category of groups. Similarly, we denote by Ab the subcategory of SKB formed by skew braces of abelian type with twice the same operation. We can

also link these three categories with functors and adjunctions.

$$\begin{array}{ccccc}
 & & L & & \\
 & \swarrow & & \searrow & \\
 \text{Ab} & \xrightleftharpoons[U_A]{K} & \text{Grp} & \xrightleftharpoons[U_G]{J} & \text{SKB} \\
 & \nwarrow & & \nearrow & \\
 & & & &
 \end{array}$$

The left part of the diagram is the well-known adjunction between the forgetful functor U_A and the abelianisation functor that sends a group $(G, \cdot)$ to $\frac{G}{[G, G]}$, where $[G, G]$ is a subgroup of G generated by the elements $g \cdot h \cdot g^{-1} \cdot h^{-1}$, for all $g, h \in G$.

The functor U_G is the inclusion functor that maps a group $(G, \cdot)$ to the skew brace $(G, \cdot, \cdot)$. In Section 3.1.1, we introduce the notion of variety of algebras. In this framework, the variety of groups can be identified to the subvariety Grp of SKB determined by the additional identity $a \circ b = a + b$, for all a, b in a skew brace $(A, +, \circ)$. The functor J associates to a skew brace $(A, +, \circ)$ the quotient group $\frac{A}{A \star A}$, where $A \star A$ is the subgroup of $(A, +)$ generated by the elements $-a + a \circ b - b$, for all $a, b \in A$. We can prove that J is a left adjoint to U_G .

Finally, the functor L maps a skew brace $(A, +, \circ)$ to the quotient group $\frac{A}{A'}$, where A' is the subgroup of $(A, +)$ generated by the elements

$$-a + a \circ b - b, \quad a + b - a - b,$$

for all $a, b \in A$. We can check that $\frac{A}{A'}$ is an abelian group.

We can add to the previous diagram an adjunction between the category RadRng of radical rings and Ab of abelian groups. The functor P maps an abelian group $(A, +)$ to the two-sided skew brace of abelian type $(A, +, +)$, which is in bijection with a radical ring. On the other hand, the functor M sends a radical ring A , that corresponds to a two-sided skew brace of abelian type $(A, +, \circ)$, to the quotient $A/\tilde{A}$ where $\tilde{A}$ is the ideal of $(A, +)$ generated by the elements $-a + a \circ b - b$, for all $a, b \in A$.

$$\begin{array}{ccccc}
 & & \text{SKB} & & \\
 & \swarrow H & & \searrow U_G & \\
 \text{RadRng} & \xrightleftharpoons[U_B U_R]{P} & & \xrightleftharpoons[U_A]{K} & \text{Grp} \\
 & \nwarrow M & & \nearrow & \\
 & & \text{Ab} & &
 \end{array}$$

The definitions of functors and the adjunctions are explained with more details in [27].

Chapter 2

Yang-Baxter equation

We are now interested in showing the link between the skew brace structure and the Yang-Baxter equation. First, we consider some results concerning this equation. We refer to [18, Chapter 4].

A solution of the quantum Yang-Baxter equation is a bijective linear map

$$R: V \otimes V \rightarrow V \otimes V,$$

where V is a vector space, such that $R_{12}R_{13}R_{23} = R_{23}R_{13}R_{12}$, where

$$R_{ij}: V \otimes V \otimes V \rightarrow V \otimes V \otimes V$$

acts as R on the (i, j) term and as the identity on V on the remaining term. For instance, the map $R_{12}: V \otimes V \otimes V \rightarrow V \otimes V \otimes V$ is defined by $R_{12} = R \otimes \text{id}_V$.

A very useful map to get another way of defining a solution of the quantum Yang-Baxter equation is the *flip map* which is defined as the map $\phi: V \otimes V \rightarrow V \otimes V$ such that $\phi(u, v) = (v, u)$ for all $u, v \in V$.

Proposition 2.1. *Let $R: V \otimes V \rightarrow V \otimes V$ be a bijective linear map on a vector space V . Then R is a solution of the quantum Yang-Baxter equation if and only if $\bar{R} = \phi R$ is a solution of*

$$\bar{R}_{12}\bar{R}_{23}\bar{R}_{12} = \bar{R}_{23}\bar{R}_{12}\bar{R}_{23},$$

where the maps $\bar{R}_{ij}$ are defined in a similar way to the previous maps R_{ij} . In this case, we say that $\bar{R}$ is a solution of the Yang-Baxter equation.

Proof. We set, for all $u, v \in V$, $R(u \otimes v) = \sigma(u \otimes v) \otimes \tau(u \otimes v)$, where $\sigma, \tau: V \otimes V \rightarrow V$ are maps. Then, for all $u, v, w \in V$, on one hand, we have

$$\begin{aligned} & R_{12}R_{13}R_{23}(u \otimes v \otimes w) \\ &= R_{12}R_{13}(u \otimes \sigma(v \otimes w) \otimes \tau(v \otimes w)) \\ &= R_{12}(\sigma(u \otimes \tau(v \otimes w)) \otimes \sigma(v \otimes w) \otimes \tau(u \otimes \tau(v \otimes w))) \\ &= \sigma(\sigma(u \otimes \tau(v \otimes w)) \otimes \sigma(v \otimes w)) \otimes \tau(\sigma(u \otimes \tau(v \otimes w)) \otimes \sigma(v \otimes w)) \otimes \tau(u \otimes \tau(v \otimes w)) \end{aligned}$$

and

$$\begin{aligned}
& R_{23}R_{13}R_{12}(u \otimes v \otimes w) \\
&= R_{23}R_{13}(\sigma(u \otimes v) \otimes \tau(u \otimes v) \otimes w) \\
&= R_{23}(\sigma(\sigma(u \otimes v) \otimes w) \otimes \tau(u \otimes v) \otimes \tau(\sigma(u \otimes v) \otimes w)) \\
&= \sigma(\sigma(u \otimes v) \otimes w) \otimes \sigma(\tau(u \otimes v) \otimes \tau(\sigma(u \otimes v) \otimes w)) \otimes \tau(\tau(u \otimes v) \otimes \tau(\sigma(u \otimes v) \otimes w)).
\end{aligned}$$

On the other hand, we have

$$\begin{aligned}
& \bar{R}_{12}\bar{R}_{23}\bar{R}_{12}(u \otimes v \otimes w) \\
&= \bar{R}_{12}\bar{R}_{23}(\tau(u \otimes v) \otimes \sigma(u \otimes v) \otimes w) \\
&= \bar{R}_{12}(\tau(u \otimes v) \otimes \tau(\sigma(u \otimes v) \otimes w) \otimes \sigma(\sigma(u \otimes v) \otimes w)) \\
&= \tau(\tau(u \otimes v) \otimes \tau(\sigma(u \otimes v) \otimes w)) \otimes \sigma(\tau(u \otimes v) \otimes \tau(\sigma(u \otimes v) \otimes w)) \otimes \sigma(\sigma(u \otimes v) \otimes w)
\end{aligned}$$

and

$$\begin{aligned}
& \bar{R}_{23}\bar{R}_{12}\bar{R}_{23}(u \otimes v \otimes w) \\
&= \bar{R}_{23}\bar{R}_{12}(u \otimes \tau(v \otimes w) \otimes \sigma(v \otimes w)) \\
&= \bar{R}_{23}(\tau(u \otimes \tau(v \otimes w)) \otimes \sigma(u \otimes \tau(v \otimes w)) \otimes \sigma(v \otimes w)) \\
&= \tau(u \otimes \tau(v \otimes w)) \otimes \tau(\sigma(u \otimes \tau(v \otimes w)) \otimes \sigma(v \otimes w)) \otimes \sigma(\sigma(u \otimes \tau(v \otimes w)) \otimes \sigma(v \otimes w)).
\end{aligned}$$

With these computations, we get the desired equivalence:

$$R_{12}R_{13}R_{23} = R_{23}R_{13}R_{12} \Leftrightarrow \bar{R}_{12}\bar{R}_{23}\bar{R}_{12} = \bar{R}_{23}\bar{R}_{12}\bar{R}_{23}.$$

□

2.1 Set-theoretic solutions of the Yang-Baxter equation

Drinfeld, in [21], suggested to study the set-theoretic solutions of the Yang-Baxter equation. This comes from the idea of studying the solutions on the basis X of the vector space V .

Definition 2.2. A set-theoretic solution of the Yang-Baxter equation is a pair (X, r) , where X is a non-empty set and $r: X \times X \rightarrow X \times X$ is a map that satisfies the braid equation

$$(r \times id_X)(id_X \times r)(r \times id_X) = (id_X \times r)(r \times id_X)(id_X \times r).$$

We write, for all $x, y \in X$, $r(x, y) = (\sigma_x(y), \tau_y(x))$, where $\sigma_x, \tau_y: X \rightarrow X$ are maps.

The Figure 2.1 illustrates a set-theoretic solution of the Yang-Baxter equation, where

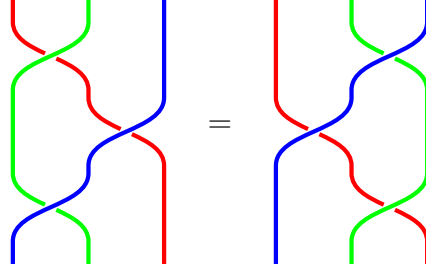


Figure 2.1: Braid representation of the Yang-Baxter equation.

a straight line represents the identity map and the crossing of two lines represents the map r , as in Figure 2.2.

We can also define some special types of set-theoretic solutions.

Definition 2.3. *A set-theoretic solution (X, r) is said to be*

- finite if X is a finite set;
- bijective if r is bijective;
- non-degenerate if, for all $x \in X$, the maps σ_x and τ_x are permutations of X ($\sigma_x, \tau_x \in \text{Sym}(X)$), i.e. bijections on X ;
- involutive if $r^2 = \text{id}_{X \times X}$.

Let (X, r) be a bijective set-theoretic solution with $r(x, y) = (\sigma_x(y), \tau_y(x))$ for $x, y \in X$. By convention, we denote the inverse of r as follows:

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

with $\hat{\sigma}_x, \hat{\tau}_y: X \rightarrow X$ maps.

Since

$$(x, y) = r^{-1}r(x, y) = r^{-1}(\sigma_x(y), \tau_y(x)) = (\hat{\sigma}_{\sigma_x(y)}\tau_y(x), \hat{\tau}_{\tau_y(x)}\sigma_x(y)),$$

we have a way to express x and y in terms of the maps $\sigma, \tau, \hat{\sigma}, \hat{\tau}$: $x = \hat{\sigma}_{\sigma_x(y)}\tau_y(x)$ and $y = \hat{\tau}_{\tau_y(x)}\sigma_x(y)$.

We give some simple examples of set-theoretic solutions.

Example 2.4. 1. Let X be a non-empty set. Then $(X, \text{id}_{X \times X})$ is a set-theoretic solution of the Yang-Baxter equation which is not non-degenerate but bijective.

2. Let X be a non-empty set. Then (X, r) , with r defined as the flip map

$$r(x, y) = (y, x)$$

is a set-theoretic solution that we call the *trivial solution* over the set X . This solution is involutive, bijective and non-degenerate.

3. Let X be a non empty set, $\sigma: X \rightarrow X$ a bijection and $r(x, y) = (\sigma(y), \sigma^{-1}(x))$. Then (X, r) is a bijective, involutive and non-degenerate solution.

The following lemma gives us a computational way to characterize a set-theoretic solution of the Yang-Baxter equation.

Lemma 2.5. *Let X be a non-empty set and $r: X \times X \rightarrow X \times X$ a map where $r(x, y) = (\sigma_x(y), \tau_y(x))$ for all $x, y \in X$. Then (X, r) is a set-theoretic solution of the Yang-Baxter equation if and only if the following identities are satisfied for all $x, y, z \in X$:*

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

Proof. The equivalence follows from the computations of each side of the Yang-Baxter equation. Indeed, on one hand, for all $x, y, z \in X$, we have

$$\begin{aligned} (r \times \text{id}_X)(\text{id}_X \times r)(r \times \text{id}_X)(x, y, z) &= (r \times \text{id}_X)(\text{id}_X \times r)(\sigma_x(y), \tau_y(x), z) \\ &= (r \times \text{id}_X)(\sigma_x(y), \sigma_{\tau_y(x)}(z), \tau_z \tau_y(x)) \\ &= (\sigma_{\sigma_x(y)} \sigma_{\tau_y(x)}(z), \tau_{\sigma_{\tau_y(x)}(z)} \sigma_x(y), \tau_z \tau_y(x)). \end{aligned}$$

On the other hand, we get

$$\begin{aligned} (\text{id}_X \times r)(r \times \text{id}_X)(\text{id}_X \times r)(x, y, z) &= (\text{id}_X \times r)(r \times \text{id}_X)(x, \sigma_y(z), \tau_z(y)) \\ &= (\text{id}_X \times r)(\sigma_x \sigma_y(z), \tau_{\sigma_y(z)}(x), \tau_z(y)) \\ &= (\sigma_x \sigma_y(z), \sigma_{\tau_{\sigma_y(z)}(x)} \tau_z(y), \tau_{\tau_z(y)} \tau_{\sigma_y(z)}(x)). \end{aligned}$$

In order to have a solution of the Yang-Baxter equation, the three components of the ternary product have to be equal, yielding the identities of the lemma. $\square$

In [20], Colazzo, Jespers, Van Antwerpen and Verwimp showed the following important result.

Proposition 2.6. *Let (X, r) be a set-theoretic solution with X finite and σ_x bijective for all $x \in X$. Then*

$$(X, r) \text{ is bijective} \Leftrightarrow (X, r) \text{ is non-degenerate.}$$

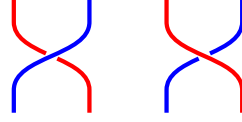


Figure 2.2: Braid diagrams: the left one represents the map r of a set-theoretic solution (X, r) and the right one represents the map r^{-1} when the solution is bijective.

Moreover, Jedlicka and Pilitowska proved that any non-degenerate set-theoretic solution is bijective, in [33, Corollary 3.4].

In a classical way, we define a homomorphism of set-theoretic solutions.

Definition 2.7. A homomorphism between the set-theoretic solutions (X, r) and (Y, s) is a map $f: X \rightarrow Y$ such that the diagram

$$\begin{array}{ccc} X \times X & \xrightarrow{r} & X \times X \\ f \times f \downarrow & & \downarrow f \times f \\ Y \times Y & \xrightarrow{s} & Y \times Y \end{array}$$

commutes, i.e. $(f \times f)r = s(f \times f)$.

An isomorphism of set-theoretic solutions is a bijective homomorphism of set-theoretic solutions.

Lemma 2.8. Let (X, r) be a non-degenerate (hence bijective) set-theoretic solution of the Yang-Baxter equation.

1. Given $x, u \in X$, there exist unique $y, v \in X$ such that $r(x, y) = (u, v)$.
2. Given $y, v \in X$, there exist unique $x, u \in X$ such that $r(x, y) = (u, v)$.

Proof. 1. We take $y = \sigma_x^{-1}(u)$ and $v = \tau_y(x)$ and get the result.

2. We take $x = \tau_y^{-1}(v)$ and $u = \sigma_x(y)$ and get the result.

□

We can interpret this lemma in the following way. Let's consider the Figure 2.2 where the left braid diagram represents the map r and the right one represents the map r^{-1} when r is bijective. On the left braid diagram, the bijectivity of the solution means that, from each row, we can determine the whole square, whereas the non-degeneracy of the solution means that, from each column, we can determine the whole square.

The following examples come from the Category Theory Seminar about set-theoretic solutions of the Yang-Baxter equation through skew braces, presented by Ilaria Colazzo at UCLouvain in November 2025.

Example 2.9. Let X be a non empty set and $\sigma, \tau: X \rightarrow X$ maps such that $\sigma\tau = \tau\sigma$. Then, (X, r) with $r(x, y) = (\sigma(y), \tau(x))$ is a set-theoretic solution of the Yang-Baxter equation. Indeed, for $x, y, z \in X$,

$$\begin{aligned} (r \times \text{id}_X)(\text{id}_X \times r)(r \times \text{id}_X)(x, y, z) &= (r \times \text{id}_X)(\text{id}_X \times r)(\sigma(y), \tau(x), z) \\ &= (r \times \text{id}_X)(\sigma(y), \sigma(z), \tau\tau(x)) \\ &= (\sigma\sigma(z), \tau\sigma(y), \tau\tau(x)), \end{aligned}$$

and

$$\begin{aligned} (\text{id}_X \times r)(r \times \text{id}_X)(\text{id}_X \times r)(x, y, z) &= (\text{id}_X \times r)(r \times \text{id}_X)(x, \sigma(z), \tau(y)) \\ &= (\text{id}_X \times r)(\sigma\sigma(z), \tau(x), \tau(y)) \\ &= (\sigma\sigma(z), \sigma\tau(y), \tau\tau(x)). \end{aligned}$$

Moreover,

$$\sigma, \tau \in \text{Sym}(X) \Leftrightarrow (X, r) \text{ is a non-degenerate (bijective) solution.}$$

This is the permutation solution associated with permutations σ and τ , called the *Lyubashenko solution*.

Finally, r is involutive if and only if $\sigma\tau = \text{id}_X$.

Example 2.10. Let G be a group.

- Then (G, r_1) with $r_1(x, y) = (xyx^{-1}, x)$, for $x, y \in G$, is a non-degenerate set-theoretic solution. Indeed, it satisfies the condition of a set-theoretic solution for all $x, y, z \in G$:

$$\begin{aligned} (r_1 \times \text{id}_G)(\text{id}_G \times r_1)(r_1 \times \text{id}_G)(x, y, z) &= (r_1 \times \text{id}_G)(\text{id}_G \times r_1)(xyx^{-1}, x, z) \\ &= (r_1 \times \text{id}_G)(xyx^{-1}, xzx^{-1}, x) \\ &= (xyzzy^{-1}x^{-1}, xyx^{-1}, x) \end{aligned}$$

and

$$\begin{aligned} (\text{id}_G \times r_1)(r_1 \times \text{id}_G)(\text{id}_G \times r_1)(x, y, z) &= (\text{id}_G \times r_1)(r_1 \times \text{id}_G)(x, yzy^{-1}, y) \\ &= (\text{id}_G \times r_1)(xyzzy^{-1}x^{-1}, x, y) \\ &= (xyzzy^{-1}x^{-1}, xyx^{-1}, x). \end{aligned}$$

Moreover, the maps $y \mapsto xyx^{-1}$ and $x \mapsto x$ are bijective.

- One can check that (G, r_2) with $r_2(x, y) = (x^2y, y^{-1}x^{-1}y)$, for $x, y \in G$, is also a non-degenerate set-theoretic solution.

Lu, Yan and Zhu, in [35], showed the following theorem that makes a connection between group actions and non-degenerate solutions. The proof given in this thesis comes from [18].

Theorem 2.11. *Let G be a group, $\xi: G \times G \rightarrow G$, $\xi(x, y) = x \triangleright y$, a left action of the group G on itself, regarded as a set, and $\eta: G \times G \rightarrow G$, $\eta(x, y) = x \triangleleft y$, a right action of the group G on itself, regarded as a set. If the compatibility condition $uv = (u \triangleright v)(u \triangleleft v)$ holds for all $u, v \in G$, then (G, r) with $r: G \times G \rightarrow G \times G$, defined for $u, v \in G$ by $r(u, v) = (u \triangleright v, u \triangleleft v)$, is a bijective non-degenerate set-theoretic solution of the Yang-Baxter equation.*

Proof. On one hand of the braid equation, we have this equality

$$\begin{aligned} & (r \times \text{id}_G)(\text{id}_G \times r)(r \times \text{id}_G)(u, v, w) \\ &= ((u \triangleright v) \triangleright ((u \triangleleft v) \triangleright w), (u \triangleright v) \triangleleft ((u \triangleleft v) \triangleright w), (u \triangleleft v) \triangleleft w) \\ &=: (u_1, v_1, w_1). \end{aligned}$$

On the other hand, we have

$$\begin{aligned} & (\text{id}_G \times r)(r \times \text{id}_G)(\text{id}_G \times r)(u, v, w) \\ &= (u \triangleright (v \triangleright w), (u \triangleleft (v \triangleright w)) \triangleright (v \triangleleft w), (u \triangleleft (v \triangleright w)) \triangleleft (v \triangleleft w)) \\ &=: (u_2, v_2, w_2). \end{aligned}$$

By the compatibility condition, we get that $u_1 v_1 w_1 = uvw = u_2 v_2 w_2$. Hence, to prove that (G, r) is a set-theoretic solution, it suffices to show that $u_1 = u_2$ and $w_1 = w_2$. And, once again by the compatibility condition and the fact that ξ is a left action, we obtain

$$u_1 = (u \triangleright v) \triangleright ((u \triangleleft v) \triangleright w) = ((u \triangleright v)(u \triangleleft v)) \triangleright w = (uv) \triangleright w = u \triangleright (v \triangleright w) = u_2.$$

Similarly, by the compatibility condition and the fact that η is a right action, we have

$$w_2 = (u \triangleleft (v \triangleright w)) \triangleleft (v \triangleleft w) = u \triangleleft ((v \triangleright w)(v \triangleleft w)) = u \triangleleft (vw) = (u \triangleleft v) \triangleleft w = w_1.$$

Since ξ and η are a left and a right action respectively, it is clear that the maps $u \triangleright -$ and $- \triangleleft u$ are bijective for all $u \in G$. This fact implies that r is a non-degenerate solution.

Finally, we also need to prove that r is invertible. If we note $r(u, v) = (x, y)$, for $u, v \in G$, then $u \triangleright v = x$, $u \triangleleft v = y$ and $uv = xy$. Moreover,

$$(y \triangleright v^{-1})u = (y \triangleright v^{-1})(y \triangleleft v^{-1}) = yv^{-1} = x^{-1}u$$

implies that $y \triangleright v^{-1} = x^{-1}$ and so $v^{-1} = y^{-1} \triangleright x^{-1}$. Similarly,

$$v(u^{-1} \triangleleft x) = (u^{-1} \triangleright x)(u^{-1} \triangleleft x) = u^{-1}x = vy^{-1}$$

implies $u^{-1} \triangleleft x = y^{-1}$ and thus $u^{-1} = y^{-1} \triangleleft x^{-1}$. Therefore, we have an inverse for r defined as $r^{-1} = \zeta(i \times i)r(i \times i)\zeta$, where $\zeta(x, y) = (y, x)$ and $i(x) = x^{-1}$ for all $x, y \in G$. Indeed, if we look at this function applied to an element of $X \times X$, we get

$$\begin{aligned} r^{-1}(x, y) &= \zeta(i \times i)r(i \times i)\zeta(x, y) \\ &= \zeta(i \times i)r(y^{-1}, x^{-1}) \\ &= \zeta(i \times i)(y^{-1} \triangleright x^{-1}, y^{-1} \triangleleft x^{-1}) \\ &= ((y^{-1} \triangleleft x^{-1})^{-1}, (y^{-1} \triangleright x^{-1})^{-1}). \end{aligned}$$

□

Proposition 2.12. *Under the assumptions of the Theorem 2.11, if $r(x, y) = (u, v)$, then*

$$r(v^{-1}, u^{-1}) = (y^{-1}, x^{-1}), \quad r(x^{-1}, u) = (y, v^{-1}), \quad r(v, y^{-1}) = (u^{-1}, x).$$

Proof. • Since $r^{-1}(y^{-1}, x^{-1}) = \zeta(i \times i)r(i \times i)\zeta(y^{-1}, x^{-1}) = \zeta(i \times i)(u, v) = (v^{-1}, u^{-1})$, then $r(v^{-1}, u^{-1}) = (y^{-1}, x^{-1})$.

- Since $r(x, y) = (u, v)$, then $x \triangleright y = u$ which implies that $x^{-1} \triangleright u = y$. So, for some $z \in G$, $r(x^{-1}, u) = (y, z)$. By the compatibility condition, $xy = uv$ and $x^{-1}u = yz$, thus

$$yv^{-1} = x^{-1}xyv^{-1} = x^{-1}uvv^{-1} = x^{-1}u = yz,$$

and therefore $z = v^{-1}$.

- In a similar way, we have that $x \triangleleft y = v$ which implies that $v \triangleleft y^{-1} = x$. So $r(v, y^{-1}) = (z, x)$ for some $z \in G$. By the compatibility condition, $xy = uv$ and $vy^{-1} = zx$, thus

$$u^{-1}x = u^{-1}xyy^{-1} = u^{-1}uvy^{-1} = vy^{-1} = zx,$$

so $z = u^{-1}$.

□

Rump, in [39], introduced a family of solutions which makes a link between set-theoretic solutions and radical rings. This is actually a special case of the Theorem 2.14. So, we will just prove the more general theorem.

Proposition 2.13. *Let R be a radical ring. Then (R, r) , where*

$$r(x, y) = (-x + x \circ y, (-x + x \circ y)' \circ x \circ y),$$

is an involutive and non-degenerate set-theoretic solution.

If $r(x, y) = (\sigma_x(y), \tau_y(x))$ is an involutive and non-degenerate solution, then

$$(x, y) = r^2(x, y) = r(\sigma_x(y), \tau_y(x)) = (\sigma_{\sigma_x(y)}\tau_y(x), \tau_{\tau_y(x)}\sigma_x(y)).$$

Hence, $\sigma_x(y) = \tau_{\tau_y(x)}^{-1}(y)$ and $\tau_y(x) = \sigma_{\sigma_x(y)}^{-1}(x)$. It means that, for an involutive non-degenerate solution, it is sufficient to know the set $\{\sigma_x | x \in X\}$ to determine the whole set $\{\tau_x | x \in X\}$ and conversely.

The Proposition 2.13 can be generalized to the structure of skew braces allowing to consider non-involutive solutions of the Yang-Baxter equation.

Theorem 2.14. *Let $(A, +, \circ)$ be a skew brace. Then (A, r_A) , where $r_A: A \times A \rightarrow A \times A$ is defined by*

$$r_A(a, b) = (\lambda_a(b), \mu_b(a)),$$

is a set-theoretic solution of the Yang-Baxter equation. Moreover, r_A is involutive if and only if $(A, +)$ is an abelian group.

Proof. By using the Theorem 2.11 and the fact that λ and μ are, respectively, a left and a right action of $(A, \circ)$ on the set A , we only need to prove that the compatibility condition is satisfied. It means that we have to check the following identity

$$a \circ b = \lambda_a(b) \circ \mu_b(a).$$

Since $\mu_b(a) = \lambda_a(b)' \circ a \circ b$, the result is clear.

It remains to prove the equivalence between the involution of r_A and the commutativity of the addition. For $a, b \in A$, we have that

$$\begin{aligned} r_A^2(a, b) &= r_A(-a + a \circ b, (-a + a \circ b)' \circ a \circ b) \\ &= (-(-a + a \circ b) + a \circ b, (-(-a + a \circ b) + a \circ b)' \circ a \circ b) \\ &= (-(a \circ b) + a + a \circ b, (-(a \circ b) + a + a \circ b)' \circ a \circ b). \end{aligned}$$

Therefore, if $(A, +)$ is abelian, it is clear that $r_A^2 = \text{id}_{A \times A}$. On the other hand, by involution of r_A , we have $-(a \circ b) + a + a \circ b = a$ which implies $a + a \circ b = (a \circ b) + a$. Since $(A, \circ)$ is a group, for all $c \in A$, there exists a unique $b \in A$ such that $c = a \circ b$. It suffices to take $b = a' \circ c$ to get that $(A, +)$ is abelian. $\square$

By the equivalence between left braces and skew braces of abelian type, we observe that left braces determine involutive solutions. Hence, skew braces allow us to find non-involutive solutions.

2.2 Self-distributive operations and set-theoretic solutions

The theory of self-distributive operations also provides a class of set-theoretic solutions. We introduce the algebraic structure of shelves and racks to give a look at this theory. We still refer to [18].

Definition 2.15. Let X be a non empty set and $\triangleleft: X \times X \rightarrow X$ a binary operation on X . We say that the pair $(X, \triangleleft)$ is a shelf if the following identity is satisfied for all $x, y, z \in X$:

$$(x \triangleleft y) \triangleleft z = (x \triangleleft z) \triangleleft (y \triangleleft z).$$

If, in addition, for all $y \in X$, the map $\rho_y: X \rightarrow X, x \mapsto x \triangleleft y$ is a bijection, then $(X, \triangleleft)$ is called a rack.

We give some examples of this new concept.

Example 2.16. • Let X be a set and $f: X \rightarrow X$ a map. We define, for $x, y \in X$, $x \triangleleft y := f(x)$, which is a shelf. Indeed, $(x \triangleleft y) \triangleleft z = f(x \triangleleft y) = f^2(x)$ and $(x \triangleleft z) \triangleleft (y \triangleleft z) = f(x) \triangleleft f(y) = f^2(x)$. Moreover, if f is bijective, $x \triangleleft y$ is a rack.

- Let $X = \mathbb{Z}/n\mathbb{Z}$. We define, for $x, y \in X$, $x \triangleleft y := 2y - x$, which is a rack. Indeed, $(x \triangleleft y) \triangleleft z = 2z - (x \triangleleft y) = 2z + x - 2y$ and

$$(x \triangleleft z) \triangleleft (y \triangleleft z) = (2z - x) \triangleleft (2z - y) = 2(2z - y) - (2z - x) = 2z - 2y + x.$$

This rack is called the *dihedral quandle*.

- Let A be an abelian group and $f \in \text{Aut}(A)$. Then, for $x, y \in A$,

$$x \triangleleft y = (\text{id} - f)(y) + f(x)$$

turns A into a rack.

As mentioned, these notions allow us to find another family of set-theoretic solutions of the Yang-Baxter equation.

Proposition 2.17. Let $(X, \triangleleft)$ be a set with $\triangleleft: X \times X \rightarrow X$ a binary operation and define a map $r: X \times X \rightarrow X \times X$ by $r(x, y) = (y, x \triangleleft y)$. Then (X, r) is a set-theoretic solution of the Yang-Baxter equation if and only if $(X, \triangleleft)$ is a shelf.

Moreover, (X, r) is a non-degenerate set-theoretic solution if and only if $(X, \triangleleft)$ is a rack.

Proof. We compute each side of the braid equation for $x, y, z \in X$. On one hand, we have

$$\begin{aligned} (r \times \text{id}_X)(\text{id}_X \times r)(r \times \text{id}_X)(x, y, z) &= (r \times \text{id}_X)(\text{id}_X \times r)(y, x \triangleleft y, z) \\ &= (r \times \text{id}_X)(y, z, (x \triangleleft y) \triangleleft z) \\ &= (z, y \triangleleft z, (x \triangleleft y) \triangleleft z). \end{aligned}$$

On the other hand,

$$\begin{aligned} (\text{id}_X \times r)(r \times \text{id}_X)(\text{id}_X \times r)(x, y, z) &= (\text{id}_X \times r)(r \times \text{id}_X)(x, z, y \triangleleft z) \\ &= (\text{id}_X \times r)(z, x \triangleleft z, y \triangleleft z) \\ &= (z, y \triangleleft z, (x \triangleleft z) \triangleleft (y \triangleleft z)). \end{aligned}$$

We clearly get that

$$(X, r) \text{ is a set-theoretic solution} \Leftrightarrow (x \triangleleft y) \triangleleft z = (x \triangleleft z) \triangleleft (y \triangleleft z) \Leftrightarrow (X, \triangleleft) \text{ is a shelf.}$$

Finally, (X, r) is non-degenerate if and only if, for all $x \in X$, $\sigma_x: X \rightarrow X, y \mapsto y$ and, for all $y \in X$, $\tau_y: X \rightarrow X, x \mapsto x \triangleleft y$ are bijections, which is equivalent to say that $(X, \triangleleft)$ is a rack. $\square$

Definition 2.18. Let X and Z be racks. A rack homomorphism from the rack X to the rack Z is a map $f: X \rightarrow Z$ such that $f(x \triangleleft y) = f(x) \triangleleft f(y)$ for all $x, y \in X$.

An isomorphism of racks is a bijective rack homomorphism.

The following proposition defines a binary operation on a set-theoretic solution to obtain a rack. The proof comes from [18, Proposition 4.3.7].

Proposition 2.19. Let (X, r) be a bijective non-degenerate set-theoretic solution of the Yang-Baxter equation. Then

$$x \triangleleft y = \sigma_y \tau_{\sigma_x^{-1}(y)}(x) = \sigma_y \hat{\sigma}_y^{-1}(x) \quad (2.1)$$

turns X into a rack and each σ_x is a rack homomorphism. Moreover, (X, r) is involutive if and only if $(X, \triangleleft)$ is the trivial rack (i.e. $x \triangleleft y = x$ for all $x, y \in X$).

Proof. First, we prove the equality $\sigma_y \tau_{\sigma_x^{-1}(y)}(x) = \sigma_y \hat{\sigma}_y^{-1}(x)$, for all $x, y \in X$. By convention, we write $r(x, y) = (\sigma_x(y), \tau_y(x))$ and $r^{-1}(x, y) = (\hat{\sigma}_x(y), \hat{\tau}_y(x))$. Since $r(x, \sigma_x^{-1}(y)) = (y, \tau_{\sigma_x^{-1}(y)}(x))$, we get

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

This equality implies that $x = \hat{\sigma}_y(\tau_{\sigma_x^{-1}(y)}(x))$, which is equivalent to $\hat{\sigma}_y^{-1}(x) = \tau_{\sigma_x^{-1}(y)}(x)$.

By means of the Proposition 2.17, it suffices to show that (X, s) , with the map

$$s: X \times X \rightarrow X \times X$$

defined by $s(x, y) = (y, x \triangleleft y)$, is a bijective non-degenerate solution of the Yang-Baxter equation. For that purpose, the proof of the identity

$$\sigma_x(y) \triangleleft \sigma_x \sigma_y(z) = \sigma_x(y \triangleleft \sigma_y(z)),$$

for all $x, y, z \in X$, will be useful and will show that σ_x is a rack homomorphism. On one hand, by using the identities of Lemma 2.5, we get

$$\begin{aligned} \sigma_x(y) \triangleleft \sigma_x \sigma_y(z) &\stackrel{2.1}{=} \sigma_{\sigma_x \sigma_y(z)} \tau_{\sigma_x^{-1}(y)}(\sigma_x \sigma_y(z))(\sigma_x(y)) \\ &\stackrel{2.5}{=} \sigma_{\sigma_x \sigma_y(z)} \tau_{\sigma_{\tau_y(x)}(z)}(\sigma_x(y)) \\ &\stackrel{2.5}{=} \sigma_{\sigma_x \sigma_y(z)} \sigma_{\tau_{\sigma_y(z)}(x)} \tau_z(y). \end{aligned}$$

On the other hand, we get, with Lemma 2.5,

$$\begin{aligned} \sigma_x(y \triangleleft \sigma_y(z)) &\stackrel{2.1}{=} \sigma_x \sigma_{\sigma_y(z)} \tau_z(y) \\ &\stackrel{2.5}{=} \sigma_{\sigma_x \sigma_y(z)} \sigma_{\tau_{\sigma_y(z)}(x)} \tau_z(y). \end{aligned}$$

Now, we define a map $J: X \times X \times X \rightarrow X \times X \times X$ by setting

$$J(x, y, z) = (x, \sigma_x(y), \sigma_x \sigma_y(z)).$$

Showing that J is bijective and satisfies the identities $(s \times \text{id}_X)J = J(r \times \text{id}_X)$ and $(\text{id}_X \times s)J = J(\text{id}_X \times r)$ will allow us to prove that (X, s) is a set-theoretic solution to the Yang-Baxter equation. Indeed, since (X, r) is a set-theoretic solution, one has, with the properties of J ,

$$\begin{aligned} (s \times \text{id}_X)(\text{id}_X \times s)(s \times \text{id}_X) &= J(r \times \text{id}_X)J^{-1}J(\text{id}_X \times r)J^{-1}J(r \times \text{id}_X)J^{-1} \\ &= J(\text{id}_X \times r)(r \times \text{id}_X)(\text{id}_X \times r)J^{-1} \\ &= (\text{id}_X \times s)JJ^{-1}(s \times \text{id}_X)JJ^{-1}(\text{id}_X \times s) \\ &= (\text{id}_X \times s)(s \times \text{id}_X)(\text{id}_X \times s). \end{aligned}$$

The inverse of J is given by $J^{-1}(x, y, z) = (x, \sigma_x^{-1}(y), \sigma_{\sigma_x^{-1}(y)}^{-1} \sigma_x^{-1}(z))$. This statement can be proved by a simple computation. It remains to prove the two identities involving r , s and J . By using the fact that $\sigma_x(y) \triangleleft \sigma_x \sigma_y(z) = \sigma_x(y \triangleleft \sigma_y(z)) = \sigma_x \sigma_{\sigma_y(z)} \tau_z(y)$, we

obtain, for all $x, y, z \in X$,

$$\begin{aligned}
(\text{id}_X \times s)J(x, y, z) &= (\text{id}_X \times s)(x, \sigma_x(y), \sigma_x \sigma_y(z)) \\
&= (x, \sigma_x \sigma_y(z), \sigma_x(y) \triangleleft \sigma_x \sigma_y(z)) \\
&= (x, \sigma_x \sigma_y(z), \sigma_x \sigma_{\sigma_y(z)} \tau_z(y)) \\
&= J(x, \sigma_y(z), \tau_z(y)) \\
&= J(\text{id}_X \times r)(x, y, z)
\end{aligned}$$

and, by the identities of Lemma 2.5,

$$\begin{aligned}
J(r \times \text{id}_X)(x, y, z) &= J(\sigma_x(y), \tau_y(x), z) \\
&= (\sigma_x(y), \sigma_{\sigma_x(y)} \tau_y(x), \sigma_{\sigma_x(y)} \sigma_{\tau_y(x)}(z)) \\
&= (\sigma_x(y), x \triangleleft \sigma_x(y), \sigma_x \sigma_y(z)) \\
&= (s \times \text{id}_X)(x, \sigma_x(y), \sigma_x \sigma_y(z)) \\
&= (s \times \text{id}_X)J(x, y, z).
\end{aligned}$$

Therefore, (X, s) is a set-theoretic solution. Moreover, it is non-degenerate since σ_x and τ_x are bijective for all $x \in X$, hence it is also a bijective solution. By applying Proposition 2.17, $(X, \triangleleft)$ is a rack.

Finally, we prove the equivalence between the involution of the solution and the trivial rack. If (X, r) is involutive, then, for all $x, y \in X$,

$$r^2(x, y) = (\sigma_{\sigma_x(y)} \tau_y(x), \tau_{\tau_y(x)} \sigma_x(y)) = (x, y).$$

Hence, $x \triangleleft \sigma_x(y) = \sigma_{\sigma_x(y)} \tau_y(x) = x$. Because of the bijectivity of σ_x , we obtain that $(X, \triangleleft)$ is trivial. Conversely, we suppose that $x \triangleleft y = \sigma_y \tau_{\sigma_x^{-1}(y)}(x) = x$ for all $x, y \in X$. We get

$$r^2(x, \sigma_x^{-1}(y)) = r(y, \tau_{\sigma_x^{-1}(y)}(x)) = r(y, \sigma_y^{-1}(x)) = (x, \tau_{\sigma_y^{-1}(x)}(y)) = (x, \sigma_x^{-1}(y)),$$

implying that the solution is involutive. $\square$

Chapter 3

Category of Skew Braces

In Chapter 1, we studied the algebraic structure of skew braces and its main properties. We can also consider that notion from a categorical perspective. Indeed, skew braces and their morphisms form a category, denoted SKB. The objective of this chapter is to highlight the properties of this category, which actually provide another explanation of some of the results of Chapter 1.

3.1 Some notions of Category Theory

We first recall some categorical notions and concepts of universal algebra in a general way and we illustrate them with a well-known example, the category Grp of groups. Then, we will explain how these concepts interact with the category of skew braces.

3.1.1 Introduction to varieties of algebras

To begin, we introduce some notions of universal algebra, especially the one of *variety of algebras*. We rely on [16] and [1] to define an equational category.

Definition 3.1. *Let A be a non-empty set and n a non-negative integer. We set*

$$A^0 = \{*\} \text{ and } A^n = A \times A \times \dots \times A,$$

the n -th cartesian product of A .

1. *An n -ary operation on A is a map $\sigma: A^n \rightarrow A$. We say that n is the arity of σ .*
2. *A finitary operation is an n -ary operation for some $n \in \mathbb{N}$.*
3. *A nullary operation is an n -ary operation with $n = 0$. Hence the arity of the operation is zero.*
4. *For $n = 1, 2, 3$, we say, respectively, a unary, binary, ternary operation.*

Definition 3.2. Let Σ be a set endowed with a map $ar: \Sigma \rightarrow \mathbb{N}$ such that, for every $\sigma \in \Sigma$, $ar(\sigma)$ is the arity of the operation σ . A Σ -algebra is a set A such that, for each $\sigma \in \Sigma$, there exists a map $\sigma_A: A^{ar(\sigma)} \rightarrow A$.

Using that definition, many algebraic structures can be defined as Σ -algebras. Here are some examples.

Examples 3.3. 1. A monoid is a set M endowed with two operations

$$\cdot_M: M \times M \rightarrow M \text{ and } e_M \in M$$

satisfying the equations: $x \cdot_M (y \cdot_M z) = (x \cdot_M y) \cdot_M z$ and $x \cdot_M e_M = x = e_M \cdot_M x$. Hence, $\Sigma = \{\cdot_M, e_M\}$, $ar(\cdot_M) = 2$ and $ar(e_M) = 0$.

2. A group is a monoid $(M, \cdot_M, e_M)$ with a unary operation $()^{-1}: M \rightarrow M$ such that $x \cdot_M x^{-1} = e_M = x^{-1} \cdot_M x$. In that case, $\Sigma = \{\cdot_M, e_M, ()^{-1}\}$ and $ar(()^{-1}) = 1$.

3. An abelian group is a group $(M, \cdot_M, e_M, ()^{-1})$ such that $x \cdot_M y = y \cdot_M x$.

In the examples, we notice that an abelian group and a group have the same set Σ . It means that one can't entirely characterize a structure by giving the set Σ of its operations, but one can also add the equations that are satisfied by the operations, as in Definition 3.7. Before considering that fact, we explain how the Σ -algebras form a category, for a given set Σ .

Definition 3.4. Let Σ be a set of operations. Let $(A, \{\sigma_A\})$ and $(B, \{\sigma_B\})$ be two Σ -algebras. A morphism of Σ -algebras is a map $f: A \rightarrow B$ such that, for each $\sigma \in \Sigma$, if $ar(\sigma) = n$, then

$$f(\sigma_A(a_1, \dots, a_n)) = \sigma_B(f(a_1), \dots, f(a_n)),$$

for every $a_1, \dots, a_n \in A$. That condition is equivalent to require the commutativity of the diagram:

$$\begin{array}{ccc} A^n & \xrightarrow{f^n} & B^n \\ \sigma_A \downarrow & & \downarrow \sigma_B \\ A & \xrightarrow{f} & B. \end{array}$$

In this chapter, we use the $\circ$ symbol to denote both the composition of morphisms and the multiplicative operation of some algebraic structures (for instance skew braces or radical rings). Normally, the role of the notation is quite clear depending on the context. Besides, when there could be a confusion, we write the composition of morphisms $f: A \rightarrow B$ and $g: B \rightarrow C$ by gf .

Lemma 3.5. Let Σ be a set of operations. The Σ -algebras and the morphisms of Σ -algebras form a category, denoted $\Sigma\text{-Alg}$.

Proof. Let $f: A \rightarrow B$ and $g: B \rightarrow C$ be two composable morphisms of Σ -algebras. Then $g \circ f$ is a morphism of Σ -algebras. Indeed, since each square of the following diagram commutes, the entire diagram commutes.

$$\begin{array}{ccccc} A^n & \xrightarrow{f^n} & B^n & \xrightarrow{g^n} & C^n \\ \sigma_A \downarrow & & \downarrow \sigma_B & & \downarrow \sigma_C \\ A & \xrightarrow{f} & B & \xrightarrow{g} & C \end{array}$$

Moreover, the composition of morphisms is associative. For a Σ -algebra A , the identity morphism on A is the identity map on the underlying set of A . $\square$

Definition 3.6. Let Σ be a set of operations. Let A and B be two Σ -algebras. We say that B is a subalgebra of A if $B \subseteq A$ and every operation in B is the restriction of the corresponding operation in A , for all $\sigma \in \Sigma$, $\sigma_B = \sigma_A|_B$.

Previously, we noticed that the set of operations does not allow one to characterize entirely some algebraic structures. It is essential to provide also the equations that the operations have to satisfy. This leads us to the definition of a variety of algebras.

Definition 3.7. Let Σ be a set of operations and let E be a set of equations. An equational category of Σ -algebras, or a variety of algebras, denoted $(\Sigma, E)\text{-Alg}$, is a full subcategory of $\Sigma\text{-Alg}$ formed by all algebras satisfying the equations of E .

We consider the Examples 3.3 with the notion of equational category.

Examples 3.8. 1. A monoid M is a (Σ, E) -algebra with $\Sigma = \{\cdot_M, e_M\}$ and

$$E = \{x \cdot_M (y \cdot_M z) = (x \cdot_M y) \cdot_M z, x \cdot_M e_M = x = e_M \cdot_M x\}.$$

Hence, monoids form a category of $(\Sigma, E)\text{-Alg}$, for this choice of Σ and E .

2. A group M is a (Σ, E) -algebra with $\Sigma = \{\cdot_M, e_M, ()^{-1}\}$ and

$$E = \{x \cdot_M (y \cdot_M z) = (x \cdot_M y) \cdot_M z, x \cdot_M e_M = x = e_M \cdot_M x, x \cdot_M x^{-1} = e_M = x^{-1} \cdot_M x\}.$$

Hence, groups form a category of $(\Sigma, E)\text{-Alg}$, for this choice of Σ and E .

3. An abelian group M is a (Σ, E) -algebra with $\Sigma = \{\cdot_M, e_M, ()^{-1}\}$ and

$$E = \left\{ \begin{array}{l} x \cdot_M (y \cdot_M z) = (x \cdot_M y) \cdot_M z, \quad x \cdot_M e_M = x = e_M \cdot_M x, \\ x \cdot_M x^{-1} = e_M = x^{-1} \cdot_M x, \quad x \cdot_M y = y \cdot_M x \end{array} \right\}.$$

Hence, abelian groups form a category of $(\Sigma, E)\text{-Alg}$, for this choice of Σ and E .

4. A skew brace $(A, +, \circ)$ is a (Σ, E) -algebra with $\Sigma = \{0, +, \circ, -(), ()'\}$ and

$$E = \left\{ \begin{array}{l} x \circ (y \circ z) = (x \circ y) \circ z, \quad x \circ 0 = x = 0 \circ x, \\ x \circ x' = 0 = x' \circ x, \quad x - x = 0 = -x + x, \\ x + (y + z) = (x + y) + z, \quad x + 0 = x = 0 + x, \\ x \circ (y + z) = x \circ y - x + x \circ z \end{array} \right\}.$$

Hence, skew braces form a category of (Σ, E) -Alg, for this choice of Σ and E .

5. We can also look at radical rings as an equational class. The Theorem 1.43 states an isomorphism between radical rings and two-sided skew braces of abelian type. By adding two equations to the previous examples, the right distributivity

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

and the commutativity of the addition $a + b = b + a$, we get an equational class that is equivalent to the one of radical rings.

We could also have considered the Proposition 1.42 that characterizes the radical rings among all rings.

6. In the previous chapter, we introduced the notion of racks with the Definition 2.15. Actually, a rack can also be defined by two operations satisfying equations and can then be considered as an equational class (see [38] for this definition of racks). Indeed, let X be a set equipped with two binary operations $\triangleleft$ and $\triangleleft^{-1}$ on X . If these operations satisfy, for all $x, y, z \in X$, the equations

- a) $(x \triangleleft y) \triangleleft^{-1} y = x = (x \triangleleft^{-1} y) \triangleleft y$;
- b) $(x \triangleleft y) \triangleleft z = (x \triangleleft z) \triangleleft (y \triangleleft z)$,

then X is called a rack. The equivalence between the two definitions of a rack is quite straightforward. Therefore, racks form a variety of algebras, denoted by Rck.

One can characterize the varieties of algebras by considering the Birkhoff Theorem, which allows one to determine if a class of Σ -algebra is a variety. Here we give the statement of this classical theorem whose proof can be found, for instance, in [1].

Theorem 3.9. *Let Σ be a set of operations. A full subcategory $\mathcal{A}$ of Σ -Alg is equational if and only if it is closed in Σ -Alg under products, subalgebras and regular quotients.*

Let $e: A \rightarrow Q$ be a regular epimorphism (i.e. the coequalizer of two morphisms) in a category $\mathcal{A}$. In this case, we will say that Q is a regular quotient of A .

We will now state some fundamental results of universal algebra, whose proofs can be found in [1]. We consider the example of the category Grp of groups to provide an intuition behind those results.

To recall, one says that a category is complete and cocomplete when it has all limits and colimits.

Proposition 3.10. *Let Σ be a set of operations and E a set of equations. Then the category $(\Sigma, E)\text{-Alg}$ is complete and cocomplete.*

Instead of giving a proof in general, we'll illustrate this property on an important example, namely the category Grp of groups.

In Grp , the set $\{e\}$ is the zero object. The binary product of two groups G, H is the cartesian product of the groups with the projections on the first and second component, written p_1, p_2 respectively. For any group K and morphisms $f: K \rightarrow G$ and $g: K \rightarrow H$, there exists a unique morphism $\phi: K \rightarrow G \times H$, defined by $\phi(k) = (f(k), g(k))$, such that $p_1 \circ \phi = f$ and $p_2 \circ \phi = g$.

$$\begin{array}{ccccc} G & \xleftarrow{p_1} & G \times H & \xrightarrow{p_2} & H \\ & \searrow f & \uparrow \phi & \nearrow g & \\ & & K & & \end{array}$$

The description of arbitrary products in this category is similar.

The binary coproduct of two groups G, H is the free product $G * H$ of the groups with the canonical injections i_G, i_H . An element of the free product is a "reduced" word, namely a sequence $s_1 \dots s_n$, where each s_i belongs either to G or to H and where one uses the properties of G and of H to reduce it. This means that one "removes" the neutral element if this latter occurs in a word, and one replaces two consecutive elements of the sequence lying in the same group by the result of their multiplication in that group. For any group K and morphisms $f: G \rightarrow K$ and $g: H \rightarrow K$, there exists a unique morphism $\psi: G * H \rightarrow K$, defined by $\psi(k) = f(k)$ if $k \in G$ or $\psi(k) = g(k)$ if $k \in H$, such that $\psi \circ i_G = f$ and $\psi \circ i_H = g$.

$$\begin{array}{ccccc} G & \xrightarrow{i_G} & G * H & \xleftarrow{i_H} & H \\ & \searrow f & \downarrow \psi & \nearrow g & \\ & & K & & \end{array}$$

The pullback of two group morphisms $u: G \rightarrow K, v: H \rightarrow K$ is the group

$$G \times_K H = \{(g, h) \in G \times H \mid u(g) = v(h)\}$$

with the projections defined by $p_1(g, h) = g$ and $p_2(g, h) = h$, for $g \in G, h \in H$. It is

illustrated by the following commutative diagram.

$$\begin{array}{ccc} G \times H & \xrightarrow{p_1} & G \\ \downarrow p_2 & & \downarrow u \\ H & \xrightarrow{v} & K \end{array}$$

The pushout of two group morphisms $\phi: F \rightarrow G$, $\psi: F \rightarrow H$ is the amalgamated free product $Q = (G * H)/N$ where N is the smallest normal subgroup of $G * H$ containing the set

$$\{\phi(f)\psi(f)^{-1} \mid f \in F\}.$$

The morphisms p_1, p_2 are $\pi \circ i_G, \pi \circ i_H$ respectively, where $\pi: G * H \rightarrow (G * H)/N$ is the canonical quotient map and i_G, i_H are the inclusions of G and H , respectively, in $G * H$. We represent the pushout with the following commutative diagram.

$$\begin{array}{ccc} F & \xrightarrow{\phi} & G \\ \downarrow \psi & & \downarrow p_1 \\ H & \xrightarrow{p_2} & Q \end{array}$$

The equalizer of two group morphisms $u, v: A \rightarrow B$ is the group

$$C = \{a \in A \mid u(a) = v(a)\}$$

with the inclusion map $i: C \rightarrow A$. The first condition of equalizer is clearly satisfied, $u \circ i = v \circ i$. Moreover, for any group D and morphism $g: D \rightarrow A$ such that $u \circ g = v \circ g$, there exists a unique morphism $\phi: D \rightarrow C$ such that $i \circ \phi = g$. This morphism is defined by $\phi(d) = g(d)$, for $d \in D$.

$$\begin{array}{ccccc} C & \xrightarrow{i} & A & \xrightarrow[u]{v} & B \\ \uparrow \phi & & \nearrow g & & \\ D & & & & \end{array}$$

The coequalizer of two group morphisms $u, v: A \rightarrow B$ is the group B/N , where N is the normal closure of the subset $\{u(a)v(a)^{-1} \mid a \in A\}$ of B , with the canonical quotient map $q: B \rightarrow B/N$. First, $q \circ u = q \circ v$. Moreover, for any group C and morphism $f: B \rightarrow C$ such that $f \circ u = f \circ v$, there exists a unique morphism $\psi: B/N \rightarrow C$ such that $\psi \circ q = f$. This morphism is defined by $\psi(\bar{b}) = f(b)$, for $b \in B$.

$$\begin{array}{ccccc} A & \xrightarrow[u]{v} & B & \xrightarrow{q} & B/N \\ & & \searrow f & & \downarrow \psi \\ & & & & C \end{array}$$

Another relevant property of a variety of algebras is the following one. A proof of this proposition is in [1, Corollary 3.18].

Proposition 3.11. *Let Σ be a set of operations and E a set of equations. Then the category $(\Sigma, E)\text{-Alg}$ is regular and exact.*

We first recall the definitions of a regular and of an exact category.

Definition 3.12. *Let $\mathcal{C}$ be a finitely complete category. Then $\mathcal{C}$ is regular if*

1. *every regular epimorphism is pullback stable ;*
2. *every morphism has a (regular epi, mono) factorization.*

The pullback stability of regular epimorphisms means that, in a pullback such as the following one, if g is a regular epimorphism, then p_1 is a regular epimorphism.

$$\begin{array}{ccc} A \times B & \xrightarrow{p_1} & A \\ \downarrow p_2 & & \downarrow f \\ B & \xrightarrow{g} & C \end{array}$$

A morphism $f: A \rightarrow B$ admits a (regular epi, mono) factorization if there exist an object I , a regular epimorphism $e: A \rightarrow I$ and a monomorphism $m: I \rightarrow B$ such that $f = m \circ e$.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow e & \nearrow m \\ & I & \end{array}$$

Definition 3.13. *Let $\mathcal{C}$ be a finitely complete category. Then $\mathcal{C}$ is exact (in the sense of Barr) if*

1. *$\mathcal{C}$ is regular ;*
2. *any equivalence relation in $\mathcal{C}$ is effective (i.e. it is the kernel pair of some arrow).*

The kernel pair of the morphism $f: A \rightarrow B$, denoted by $\text{Eq}(f)$, is the pullback of f along itself.

$$\begin{array}{ccc} \text{Eq}(f) & \xrightarrow{\pi_1} & A \\ \downarrow \pi_2 & & \downarrow f \\ A & \xrightarrow{f} & B \end{array}$$

These definitions allow one to explain the Proposition 3.11 in the case of the category Grp of groups.

First, let $f: A \rightarrow C$ and $g: B \rightarrow C$ be two group morphisms with g a regular epimorphism and consider the following pullback.

$$\begin{array}{ccc} A \times_C B & \xrightarrow{p_1} & A \\ p_2 \downarrow & & \downarrow f \\ B & \xrightarrow{g} & C \end{array}$$

In Grp, as in any variety of algebras, the regular epimorphisms are exactly the surjective morphisms. We have observed that

$$A \times_C B = \{(a, b) \in A \times B \mid f(a) = g(b)\}.$$

We are going to show that the first projection p_1 is surjective. If $a \in A$, then $f(a) \in C$. Since g is surjective, there exists $b \in B$ such that $g(b) = f(a)$. By definition of the pullback in Grp, $(a, b) \in A \times_C B$ and $p_1(a, b) = a$. This shows that p_1 is surjective and that regular epimorphisms are pullback stable in Grp.

Let $f: A \rightarrow B$ be a group morphism. By the definitions of kernel pair and pullback in Grp, we get $\text{Eq}(f) = \{(a_1, a_2) \in A \times A \mid f(a_1) = f(a_2)\}$. Then the (regular epi, mono) factorization of f is given by $I = A/\text{Eq}(f)$, $e: A \rightarrow A/\text{Eq}(f)$ the canonical quotient map (hence surjective) and $m: A/\text{Eq}(f) \rightarrow B$ defined by $m(\bar{a}) = f(a)$, for $a \in A$, which is an injective map because of the definition of $\text{Eq}(f)$.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow e & \nearrow m \\ & A/\text{Eq}(f) & \end{array}$$

We have just proved that Grp is a regular category. It remains to show that any equivalence relation in Grp is effective to prove the exactness.

Let R be an equivalence relation on a group A in Grp. We define the canonical quotient map $\pi: A \rightarrow A/R$. The kernel pair of π is isomorphic to R . Indeed,

$$(x, y) \in R \iff \bar{x}^R = \bar{y}^R \iff \pi(x) = \pi(y) \iff (x, y) \in \text{Eq}(\pi),$$

for any $x, y \in A$. Then Grp is an exact category.

3.1.2 Semi-abelian category

Another notion in Category Theory, that will be relevant for the category of skew braces, is the concept of a semi-abelian category. The definition was introduced in [32] by Janelidze, Márki and Tholen.

Definition 3.14. A category $\mathcal{C}$ is semi-abelian if

1. it is pointed;
2. it has binary coproducts;
3. it is exact;
4. it is protomodular.

A category $\mathcal{C}$ is said to be *pointed* if there exists a zero object 0 , meaning that there exists an object 0 of $\mathcal{C}$ such that, for every object A of $\mathcal{C}$, there exists a unique morphism $0 \rightarrow A$ and a unique morphism $A \rightarrow 0$.

In [11], Bourn defined a protomodular category with the notions of category of "points" and change of base functor. Since we do not use these concepts in this thesis, we will consider an equivalent definition of a protomodular category. A category $\mathcal{C}$ is *protomodular* if the Split Short Five Lemma holds in $\mathcal{C}$. The Split Short Five Lemma holds in $\mathcal{C}$ if, for any commutative diagram in $\mathcal{C}$

$$\begin{array}{ccccccc} 0 & \longrightarrow & K & \xrightarrow{k} & A & \begin{smallmatrix} \xrightarrow{p} \\ \xleftarrow{s} \end{smallmatrix} & B \longrightarrow 0 \\ & & \downarrow u & & \downarrow v & & \downarrow w \\ 0 & \longrightarrow & K' & \xrightarrow{k'} & A' & \begin{smallmatrix} \xrightarrow{p'} \\ \xleftarrow{s'} \end{smallmatrix} & B' \longrightarrow 0 \end{array}$$

where each row is a split short exact sequence (i.e. it is a short exact sequence such that there exists a section of p , i.e. a morphism $s: B \rightarrow A$ such that $p \circ s = \text{id}_B$), u and w are isomorphisms, then v is an isomorphism.

The category of groups is a semi-abelian category. Indeed, we have just proved in Subsection 3.1.1 that it has binary coproducts and it is exact. Moreover, the zero object is the trivial group, $\{0\}$. Finally, one can prove the Split Short Five Lemma holds in Grp by showing that v is injective and surjective in the above diagram. The first relevant fact to notice is that there is no restriction in assuming that k and k' are subgroup inclusions as subgroups.

Let $a \in A$ such that $v(a) = 0$. Then $p'(v(a)) = 0$, so $w(p(a)) = 0$. Since w is injective, $p(a) = 0$ and $a \in K$. Hence, $k'(u(a)) = v(k(a)) = v(a) = 0$ and, by injectivity of k' and u , $a = 0$. This implies that v is injective.

Let us then prove that v is surjective. Given $a' \in A'$, we want to prove that there exists $a \in A$ such that $v(a) = a'$. By surjectivity of w and p , there exists $b \in B$ such that $w(b) = p'(a')$ and there exists $\tilde{a} \in A$ such that $p(\tilde{a}) = b$. Hence,

$$p'(a') = w(b) = w(p(\tilde{a})) = p'(v(\tilde{a})),$$

which implies that $p'(v(\tilde{a})^{-1}a') = 0$ and $v(\tilde{a})^{-1}a' \in K'$. By surjectivity of u , there exists $k \in K$ such that $u(k) = v(\tilde{a})^{-1}a'$. Moreover, $v(k) = k'(u(k)) = v(\tilde{a})^{-1}a'$ and this implies that $v(\tilde{a}k) = a'$. Hence, we have proved the surjectivity of v by taking $a = \tilde{a}k$. Actually, this proof also works to prove the Short Five Lemma in Grp (where p and p' are only required to be surjective homomorphisms) since only the surjectivity of p and p' have been used in the proof, not the existence of their sections s and s' .

This ends to prove that the category of groups is semi-abelian. This categorical property allows one to state some fundamental results. For instance, in Section 1.3, we have proved the Noether isomorphism theorems for the category of skew braces. Actually, these theorems can be proved for any semi-abelian category, which is a property of the category SKB as explained in the next section.

3.2 SKB is a semi-abelian category

As mentioned in the introduction of this Chapter, the objects of the category SKB are skew braces and the morphisms are the skew brace morphisms (as in Definition 1.3). It is a well-defined category since the composition of two composable skew brace morphisms is a skew brace morphism, the composition is associative and the identity morphism is a skew brace morphism.

In this section, we'll show that SKB is a semi-abelian category. Before this, we state a lemma about the specific structure of a normal monomorphism in the category of skew braces. To recall, a monomorphism is normal if it is the kernel of some morphism.

Lemma 3.15. *In SKB, the normal monomorphisms are exactly the ideals, as defined in Definition 1.24.*

Proof. Let $u: K \rightarrow A$ be a normal monomorphism in SKB. Hence, there exists $f: A \rightarrow B$ such that $u = \ker(f)$. By Proposition 1.31, K is an ideal of A .

Conversely, by Proposition 1.31, every ideal is the kernel of some morphism. Let I be an ideal of a skew brace A and let $\iota: I \rightarrow A$ be the inclusion morphism of I in A . Then $\iota = \ker(\pi)$, where $\pi: A \rightarrow A/I$ is the canonical projection. One concludes that ι is a normal monomorphism. The following diagram is then a short exact sequence:

$$0 \longrightarrow I \xrightarrow{\iota} A \xrightarrow{\pi} A/I \longrightarrow 0.$$

This concludes the proof of the equivalence between the normal monomorphisms and the ideals in SKB. $\square$

Proposition 3.16. *The category SKB of skew braces is semi-abelian.*

Proof. As observed in the Examples 3.8, the category SKB of skew braces is a variety of algebras. Therefore, SKB is complete, cocomplete and also exact. Its limits are built in the same way as in the category of groups.

From Lemma 1.5, we can deduce that SKB is a pointed category, i.e. it admits a zero object. Since the multiplication and the addition of a skew brace have the same neutral element, denoted by 0, the initial and the terminal object of the category is the trivial skew brace $\{0\}$, which is then called a zero object.

It remains to prove the protomodularity. Since any skew brace is equipped in particular with a group structure, the Split Short Five Lemma is proved as in Grp (see Section 3.1.2). Hence, the category is protomodular.

We can conclude that SKB is semi-abelian. $\square$

To complete the proof, we explain why the category SKB is regular. The pullback of two morphisms in SKB is formed as in Set and regular epimorphisms are surjective morphisms. This implies the pullback stability of regular epimorphisms. Moreover, the (regular epi, mono) factorization of a morphism was already introduced in Proposition 1.31 when we defined the image of a skew brace morphism. The following commutative diagram illustrates it, where the map e is the corestriction of f to its image and the map m is the inclusion of the image of f in B .

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow e & \nearrow m \\ & \text{Im}(f) & \end{array}$$

In order to prove that SKB is a semi-abelian variety, one could also have used the characterization of semi-abelian varieties, first established in [15]. Indeed, a variety of algebras $\mathcal{V}$ is semi-abelian if and only if there exist n binary operations $\{\alpha_i\}_{i \in \{1, \dots, n\}}$, a unique 0-ary operation, called the constant 0, and an $(n+1)$ -ary operation β such that, for all elements x, y of the variety, $\alpha_i(x, x) = 0$, for every $i \in \{1, \dots, n\}$, and $\beta(\alpha_1(x, y), \dots, \alpha_n(x, y), y) = x$.

In SKB, with the constant term 0 and $n = 1$, one can define the operations $\alpha_1(x, y) = x - y$ and $\beta(x, y) = x + y$ that satisfy the identities $\alpha_1(x, x) = 0$ and

$$\beta(\alpha_1(x, y), y) = (x - y) + y = x.$$

3.3 Strong protomodularity of SKB

Strong protomodularity is another interesting property of a category. This notion was introduced in 2000 by D. Bourn in [10]. It is related to the concept of normal subobjects. Although the definition was first expressed in terms of functors between the category of points of a category $\mathcal{C}$ and the category $\mathcal{C}$ itself, we will use the following equivalent definition in the context of exact categories.

Definition 3.17. *An exact pointed category $\mathcal{C}$ is called strongly protomodular when it is protomodular and the following property is satisfied: for any commutative diagram such as the following one, where $k = \ker(p)$ and $k' = \ker(p')$ and p, p' are split epimorphisms with sections s, s' respectively,*

$$\begin{array}{ccccccc} 0 & \longrightarrow & K & \xrightarrow{k} & A & \xleftarrow[p]{s} & B \\ & & \downarrow u & & \downarrow v & & \parallel \\ 0 & \longrightarrow & K' & \xrightarrow{k'} & A' & \xleftarrow[p']{s'} & B \end{array}$$

if u is a normal monomorphism, then $k' \circ u$ is a normal monomorphism in $\mathcal{C}$.

The category $\mathbf{Grp}$ of groups and the category $\mathbf{Rng}$ of rings are well-known examples of strongly protomodular categories. We will prove that the category $\mathbf{SKB}$ is also strongly protomodular. We first introduce the following definition and lemma.

Definition 3.18. *In a finitely complete category, a pair of arrows $A \xrightarrow{a} C \xleftarrow{b} B$ is jointly strongly epimorphic if for any monomorphism $m: M \rightarrow C$ and for any morphisms $A \xrightarrow{\alpha} M \xleftarrow{\beta} B$ such that $m \circ \alpha = a$ and $m \circ \beta = b$, then m is an isomorphism.*

$$\begin{array}{ccccc} & & M & & \\ & \nearrow \alpha & \downarrow m & \nwarrow \beta & \\ A & \xrightarrow{a} & C & \xleftarrow{b} & B \end{array}$$

Lemma 3.19. *In a pointed protomodular category, let $p: A \rightarrow B$ be a split epimorphism with section s and let $k = \ker(p): K \rightarrow A$, then the pair (k, s) is jointly strongly epimorphic.*

Proof. In order to prove that (k, s) is jointly strongly epimorphic, we need to show the following property. Let $m: M \rightarrow A$ be a monomorphism, let $\alpha: K \rightarrow M$ and $\beta: B \rightarrow M$ be morphisms such that $m \circ \alpha = k$ and $m \circ \beta = s$, then m is an isomorphism. This

property is illustrated by the following diagram, where the square is the pullback of the morphisms $p: A \rightarrow B$ and $0 \rightarrow B$, hence the kernel of p .

$$\begin{array}{ccccc}
 & & \alpha & \xrightarrow{\quad} & M \\
 & & \nearrow & & \nearrow m \\
 K & \xrightarrow{k} & A & & \\
 \downarrow & & \downarrow p & \uparrow s & \downarrow \beta \\
 0 & \longrightarrow & B & &
 \end{array}$$

Since the category is protomodular, the Split Short Five Lemma holds in it. We consider the following diagram

$$\begin{array}{ccccccc}
 0 & \longrightarrow & K & \xrightarrow{\alpha} & M & \xleftarrow{\beta} & B \\
 & & \parallel & & \downarrow m & \xrightarrow{p \circ m} & \parallel \\
 0 & \longrightarrow & K & \xrightarrow{k} & A & \xleftarrow[p]{s} & B.
 \end{array}$$

To apply the Split Short Five Lemma, we first need to check that β is a section of $p \circ m$ and that $\alpha = \ker(p \circ m)$. On one hand, $p \circ m \circ \beta = p \circ s = 1_B$, which implies that β is a section of $p \circ m$. On the other hand, it is clear that $p \circ m \circ \alpha = p \circ k = 0$. Moreover, if $\gamma: C \rightarrow M$ is a morphism such that $p \circ m \circ \gamma = 0$, by the universal property of the kernel k of p , there exists a unique morphism $\phi: C \rightarrow K$ such that $k \circ \phi = m \circ \gamma$. Moreover, by the condition $m \circ \alpha = k$, $m \circ \gamma = k \circ \phi = m \circ \alpha \circ \phi$, and by the fact that m is a monomorphism, it follows that $\gamma = \alpha \circ \phi$. We have just proved that $\alpha = \ker(p \circ m)$.

We conclude, by the Split Short Five Lemma, that m is an isomorphism, and that (k, s) is jointly strongly epimorphic. $\square$

Now, we can show that the category of skew braces is strongly protomodular. The proof of this can be found in [12].

Proposition 3.20. *The category SKB is strongly protomodular.*

Proof. We have already proved that SKB is pointed and protomodular. Let's consider the diagram of the Definition 3.17 in the category of skew braces.

$$\begin{array}{ccccccc}
 0 & \longrightarrow & K & \xrightarrow{k} & A & \xleftarrow[p]{s} & B \\
 & & \downarrow u & & \downarrow v & & \parallel \\
 0 & \longrightarrow & K' & \xrightarrow{k'} & A' & \xleftarrow[p']{s'} & B
 \end{array}$$

One needs to prove that $k'u$ is a normal monomorphism, which is equivalent to prove that K is an ideal of A' in SKB. Hence, one needs to show the three following conditions:

$(K, \circ)$ is a normal subgroup of $(A', \circ)$, $(K, +)$ is a normal subgroup of $(A', +)$ and $\lambda_{a'}(K) \subseteq K$ for every $a' \in A'$. Since the category of groups is known to be strongly protomodular (Bourn showed it in [10]), the first two points are straightforward. Indeed, $u: (K, \circ) \rightarrow (K', \circ)$ and $u: (K, +) \rightarrow (K', +)$ are normal subgroups in Grp, hence $k'u: (K, \circ) \rightarrow (A', \circ)$ and $k'u: (K, +) \rightarrow (A', +)$ are normal subgroups in Grp.

It remains to show that $\lambda_{a'}(K) \subseteq K$ for every $a' \in A'$. By using the section s' of p' , one gets the equality $a' = s'(p'(a')) \circ s'(p'(a'))^{-1} \circ a'$. Since $p's' = 1_B$,

$$p'(s'(p'(a'))^{-1} \circ a') = p'(s'(p'(a')))^{-1} \circ p'(a') = 0,$$

which implies that $s'(p'(a'))^{-1} \circ a' \in K'$. Hence $a' = s'(b') \circ \hat{k}$ with $\hat{k} = s'(p'(a'))^{-1} \circ a' \in K'$ and $b' = p'(a') \in B$. This is also a consequence of the fact that (k', s') is jointly strongly epimorphic.

Let $\tilde{k} \in K$. Then

$$\lambda_{a'}(\tilde{k}) = \lambda_{s'(b') \circ \hat{k}}(\tilde{k}) = \lambda_{s'(b')} \lambda_{\hat{k}}(\tilde{k}),$$

with $\bar{k} := \lambda_{\hat{k}}(\tilde{k}) \in K$ since K is an ideal of K' and $\hat{k} \in K'$, $\tilde{k} \in K$. By commutativity of the diagram, $s'(b') = v s(b')$. Since the right vertical arrow in the previous diagram is an identity, in particular a monomorphism, the left-hand square is a pullback, and this implies that it reflects monomorphisms. This property is proved by Bourn in [11]. Hence, v is an injective map that we can consider as an inclusion map, implying that $s'(b') = s(b') \in A$. So,

$$\lambda_{a'}(\tilde{k}) = \lambda_{s'(b')}(\bar{k}) = \lambda_{s(b')}(\bar{k}) \in K$$

since K is an ideal of A . This allows one to conclude that $k'u$ is a normal monomorphism in SKB. $\square$

3.4 Some categorical results in SKB

The properties of the category SKB of skew braces we have introduced in this thesis are relevant in the study of this algebraic structure. Indeed, it helps us to understand that this category has many common properties with the one of groups. It means that this structure with two group operations can sometimes be considered as a group and that we can apply some properties of the category of groups to SKB, making some results easier to understand.

For instance, in Chapter 1, we proved the Noether isomorphism theorems for skew braces. As a matter of fact, these results can actually be proved in any semi-abelian category.

The first isomorphism theorem is a direct consequence of a result proved by Bourn in [8, Proposition 2].

Theorem 3.21. *Let $\mathcal{C}$ be a semi-abelian category and let $f: X \rightarrow Y$ be a regular epimorphism in $\mathcal{C}$. Then $X/\ker(f) \cong Y$, where $\ker(f)$ denotes the kernel of f .*

Proof. Since a semi-abelian category is a pointed protomodular category, f is the cokernel of its kernel, by [8, Proposition 2].

$$\begin{array}{ccc} \ker(f) & \xrightarrow{\ker(f)} & X \xrightarrow{f} Y \\ & & \searrow q \\ & & X/\ker(f) \end{array}$$

The fact that q is the cokernel of $\ker(f)$ implies that q and f are isomorphic and $X/\ker(f) \cong Y$. $\square$

To state the second isomorphism theorem, we need to define the intersection and the supremum of two normal subobjects in a semi-abelian category. Let $\mathcal{C}$ be a semi-abelian category and let $n: N \rightarrow A$ and $m: M \rightarrow A$ be two normal subobjects of an object A . The intersection of N and M , denoted by $N \cap M$, is defined as the pullback of the monomorphisms n and m :

$$\begin{array}{ccc} N \cap M & \longrightarrow & N \\ \downarrow & & \downarrow n \\ M & \xrightarrow{m} & A. \end{array}$$

Let's consider the pushout of the morphisms $\text{coker}(n)$ and $\text{coker}(m)$:

$$\begin{array}{ccc} A & \xrightarrow{\text{coker}(n)} & A/N \\ \text{coker}(m) \downarrow & \searrow p & \downarrow \\ A/M & \longrightarrow & P. \end{array}$$

We set $p: A \rightarrow P$ as the diagonal morphism of this pushout. The supremum of N and M , denoted by $N \vee M$, is the kernel of p , i.e. $N \vee M = \ker(p)$. In other words, this is the smallest normal subobject of A that contains N and M .

To prove the second isomorphism theorem, we use the 3×3 Lemma asserting that, in a commutative diagram with 3 rows and 3 columns, if the three columns and two out of three rows are short exact sequences, the third row is a short exact sequence. This lemma is valid in any semi-abelian category, as Bourn proved in [8].

Theorem 3.22. *Let $\mathcal{C}$ be a semi-abelian category and let $n: N \rightarrow A$ and $m: M \rightarrow A$ be two normal subobjects of an object A . Then, $\frac{N}{N \cap M} \cong \frac{N \vee M}{M}$.*

Proof. Consider the following commutative diagram.

$$\begin{array}{ccccccc}
& & 0 & & 0 & & 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & N \cap M & \xrightarrow{j_N} & N & \xrightarrow{\pi_N} & \frac{N}{N \cap M} \longrightarrow 0 \\
& & \downarrow j_M & & \downarrow i_N & & \downarrow \phi \\
0 & \longrightarrow & M & \xrightarrow{i_M} & N \vee M & \xrightarrow{q_M} & \frac{N \vee M}{M} \longrightarrow 0 \\
& & \downarrow \pi_M & & \downarrow q_N & & \downarrow \pi \\
& & \frac{M}{N \cap M} & \xrightarrow{\psi} & \frac{N \vee M}{N} & \xrightarrow{q} & \frac{N \vee M / M}{N / N \cap M} \\
& & \downarrow & & \downarrow & & \downarrow \\
& & 0 & & 0 & & 0
\end{array}$$

By the universal property of the arrow π_N which is the cokernel of j_N , there exists a unique morphism $\phi: \frac{N}{N \cap M} \rightarrow \frac{N \vee M}{M}$ such that $\phi \circ \pi_N = q_M \circ i_N$. Let's denote by π its cokernel.

By the universal property of π_M which is the cokernel of j_M , there exists a unique morphism $\psi: \frac{M}{N \cap M} \rightarrow \frac{N \vee M}{N}$ such that $\psi \circ \pi_M = q_N \circ i_M$. By the universal property q_N , there exists a unique morphism $q: \frac{N \vee M}{N} \rightarrow \frac{N \vee M / M}{N / N \cap M}$.

Since the left-hand square $i_M \circ j_M = i_N \circ j_N$ is a pullback and the first two lines are short exact sequences, ϕ is a monomorphism. It is even a normal monomorphism because i_N is a normal monomorphism, q_M and π_N are normal epimorphisms and the category is semi-abelian. Hence, the right-hand column is a short exact sequence. By a similar reasoning, ψ is a normal monomorphism.

Since the three columns and the first two lines are short exact sequences, we can apply the 3×3 Lemma and we obtain that the last line (ψ, q) is also a short exact sequence.

Since π_M is a normal epimorphism and the last two lines are short exact sequences, the right-hand square $q \circ q_N = \pi \circ q_M$ is a pushout. But the pushout of q_N, q_M is equal to 0. Therefore, $\frac{N \vee M / M}{N / N \cap M} = 0$ which implies that ϕ and ψ are isomorphisms. $\square$

The third isomorphism theorem is proved, for instance, in [25, Lemma 1.3], in the more general context of normal categories.

Theorem 3.23. *Let $\mathcal{C}$ be a semi-abelian category. Let $h: H \rightarrow X$ and $k: K \rightarrow X$ be normal subobjects of X , with $K \subseteq H$. Then $X/H \cong \frac{X/K}{H/K}$.*

Proof. Consider the following commutative diagram.

$$\begin{array}{ccccccc}
& & & 0 & & & \\
& & & \downarrow & & & \\
0 & \longrightarrow & K & \xrightarrow{j} & H & \xrightarrow{\text{coker}(j)} & H/K \longrightarrow 0 \\
& & \parallel & & \downarrow h & & \downarrow \theta \\
0 & \longrightarrow & K & \xrightarrow{k} & X & \xrightarrow{\text{coker}(k)} & X/K \longrightarrow 0 \\
& & & & \downarrow \text{coker}(h) & & \downarrow \pi \\
& & & & X/H & = & X/H \\
& & & & \downarrow & & \\
& & & & 0 & &
\end{array}$$

By the universal property of $\text{coker}(j)$, there exists a unique arrow $\theta: H/K \rightarrow X/K$ such that $\theta \circ \text{coker}(j) = \text{coker}(k) \circ h$. The morphism θ is a monomorphism since the arrow $\text{coker}(k) \circ h$ factorizes as a normal epimorphism followed by a monomorphism and $\text{coker}(j)$ is a normal epimorphism.

By the universal property of $\text{coker}(k)$, there exists a unique arrow $\pi: X/K \rightarrow X/H$ such that $\pi \circ \text{coker}(k) = \text{coker}(h)$. Moreover, π is a normal epimorphism.

By the universal property of $\ker(\pi)$, there exists a unique arrow $\phi: H \rightarrow \ker(\pi)$ such that $\ker(\pi) \circ \phi = \text{coker}(k) \circ h$.

$$\begin{array}{ccc}
\ker(\pi) & \xrightarrow{\ker(\pi)} & X/K \xrightarrow{\pi} X/H \\
\uparrow \phi & \nearrow \text{coker}(k) \circ h & \\
H & &
\end{array}$$

Since normal epimorphisms are pullback stable, ϕ is a normal epimorphism. Then, $\ker(\pi) \circ \phi = \theta \circ \text{coker}(j)$ are two (regular epi, mono) factorizations of the same morphism. This implies that θ is isomorphic to the kernel of π .

$$\begin{array}{ccc}
H & \xrightarrow{\text{coker}(j)} & H/K \\
\downarrow \phi & & \downarrow \theta \\
\ker(\pi) & \xrightarrow{\ker(\pi)} & X/K
\end{array}$$

Since π is the cokernel of its kernel, $\pi = \text{coker}(\theta)$ and (θ, π) is a short exact sequence. It allows us to conclude that $X/H \cong \frac{X/K}{H/K}$. $\square$

We also noticed the strong protomodularity of SKB. This categorical property is rel-

evant in commutator theory. Indeed, being strongly protomodular enables to assert a correspondence between two notions of centrality, the first one of normal subobjects (due to Huq [30]) and the second one of equivalence relations (due to Smith [40]). In this thesis, we refer to the definitions and terminology used by Bourn and Gran in [14].

The Huq cooperator can be expressed in the following way. Let $\mathcal{C}$ be a finitely complete category. Let $m: X \rightarrow Z$ and $n: Y \rightarrow Z$ be two normal subobjects of Z . Let

$$i_1 = (1, 0): X \rightarrow X \times Y \text{ and } i_2 = (0, 1): Y \rightarrow X \times Y$$

be the induced arrows of the cartesian product $X \times Y$. We say that X and Y *cooperate* if there exists a unique morphism $c: X \times Y \rightarrow Z$ such that

$$c \circ i_1 = m \text{ and } c \circ i_2 = n.$$

We illustrate this definition by the following diagram:

$$\begin{array}{ccccc} & & X \times Y & & \\ & i_1 \nearrow & \downarrow c & \nwarrow i_2 & \\ X & \xrightarrow{m} & Z & \xleftarrow{n} & Y. \end{array}$$

If there exists such a morphism c , one calls it the *cooperator* of X and Y and writes

$$[X, Y]_H = 0.$$

For instance, in the category Grp of groups, the cooperator of two normal subobjects is defined by $c(x, y) = x \cdot y$ for any $x \in X$ and $y \in Y$. When there is such a cooperator, it allows one to get the equality $x \cdot y = y \cdot x$.

We now look at the notion of connector. Let $\mathcal{C}$ be a finitely complete protomodular category and let R and S be equivalence relations on an object X . Let's consider the pullback

$$\begin{array}{ccc} R \times_S X & \xrightarrow{p_2} & S \\ p_1 \downarrow & & \downarrow s_1 \\ R & \xrightarrow{r_2} & X \end{array}$$

where r_2 and s_1 are the second and first projections of R and S , respectively.

We say that R and S centralize each other if there exists a unique morphism

$$p: R \times_S X \rightarrow X$$

such that $p \circ i_R = r_1$ and $p \circ i_S = s_2$, where $i_R: R \rightarrow R \times_X S$ is defined by $i_R(x, y) = (x, y, y)$ and, similarly, $i_S: S \rightarrow R \times_X S$ is defined by $i_S(x, y) = (x, x, y)$. These morphisms are well-defined since the relations R and S are reflexive. The conditions on the morphism p are equivalent to the identities $p(x, y, y) = x$ and $p(x, x, y) = y$ and are illustrated by the following diagram:

$$\begin{array}{ccccc} R & \xrightarrow{i_R} & R \times_X S & \xleftarrow{i_S} & S \\ & \searrow r_1 & \downarrow p & \swarrow s_2 & \\ & & X & & \end{array}$$

where r_1 and s_2 are the first and second projections of R and S , respectively.

If such a morphism p exists, one calls it the *connector* of R and S and writes

$$[R, S]_S = \Delta_X,$$

where Δ_X is the discrete relation on X .

For instance, in Grp , when it exists, the connector on two equivalence relations R and S is given by $p(x, y, z) = x \cdot y^{-1} \cdot z$.

Let $\mathcal{C}$ be a pointed, exact and protomodular category. Let $r_1, r_2: R \rightarrow X$ be an equivalence relation on an object X . Let's consider the following diagram with the kernel morphism of r_1 , $k: \ker(r_1) \rightarrow R$,

$$\ker(r_1) \xrightarrow{k} R \xrightleftharpoons[r_2]{r_1} X.$$

The normal subobject associated to the equivalence relation R is $r_2 \circ k: \ker(r_1) \rightarrow X$, we denote it by N_R .

In a pointed, exact and protomodular category, if R and S are two equivalence relations such that $[R, S]_S = \Delta_X$, then $[N_R, N_S]_H = 0$.

The converse statement holds in strongly protomodular categories, as shown in [14]. This means that, in a strongly protomodular category, the existence of a cooperator between two normal subobjects is equivalent to the existence of a connector between their associated equivalence relations. This is not true, in general, for any semi-abelian category. For example, the category DiGrp of digroups does not satisfy this property, as explained by Bourn in [9].

Conclusion

In this thesis, we have shown how skew braces provide non-involutive set-theoretic solutions of the Yang-Baxter equation. For this, we studied the properties of skew braces. In particular, we defined a left and a right actions on the underlying set of a skew brace. These actions are actually the main components of the set-theoretic solution associated to a skew brace. Nevertheless, there exist other classes of solutions that we have not considered in our work. Indeed, we just focused on non-degenerate set-theoretic solutions but we could have looked at simple, indecomposable, retractable or multipermutation solutions. There exists also a generalization of skew braces in the theory of Hopf algebras, namely the concept of Hopf braces [2], that can provide solutions of the quantum Yang-Baxter equation. In fact, this thesis is just an insight of a part of the difficult and interesting problem of classifying the solutions of the Yang-Baxter equation. We could have explored some other mathematical paths, since there are many open problems concerning this equation and its solutions.

As a second step, we have studied the skew braces from a categorical point of view. Indeed, we were interested in studying this algebraic structure from different perspectives. We first noticed that skew braces and its morphisms form a category. Since a skew brace is endowed with two group structures, we naturally compared its properties with those of the category of groups and we realized that many of them are common to both structures. Actually, as we have previously shown, the category of skew braces is semi-abelian. This fact combined with the relevant properties of skew braces indicate that many links between these two theories could be established, in both directions. It means that some specific properties of skew braces could be extended to any semi-abelian category, whereas the theory of semi-abelian categories can lead to discover some new properties of skew braces and their homology. Also the above-mentioned Hopf braces have been recently studied from a categorical perspective in [26]. Therefore, there is no doubt that many new interesting interactions still have to be discovered between these two mathematical fields.

Finally, we have presented Bourn's proof of the strong protomodularity of skew braces. It implies that commutator theory is well behaved in this category. Indeed, one can say that the "Smith=Huq" property [36] holds in the category of skew braces, or more precisely that two normal subobjects cooperate if and only if their associated equivalence relations centralize each other. Some other interesting categorical properties of skew braces have been investigated by D. Bourn in [12].

Bibliography

- [1] J. Adámek, J. Rosický, and E. M. Vitale, *Algebraic theories*, Cambridge Tracts in Mathematics, vol. 184, Cambridge University Press, Cambridge, 2011. A categorical introduction to general algebra; With a foreword by F. W. Lawvere.
- [2] I. Angiono, C. Galindo, and L. Vendramin, *Hopf braces and Yang-Baxter operators*, Proceedings of the American Mathematical Society **145** (2017), no. 5, 1981–1995.
- [3] A. Ardizzoni and A. Cigoli, *Notes on Category Theory* (2025).
- [4] V. Bardakov, M. Elhamdadi, and M. Singh, *Yang-Baxter Equation and Related Algebraic Structures*, 2025.arXiv:2506.23175
- [5] M. Barr, *Exact categories* (1971).
- [6] R. J. Baxter, *Partition function of the eight-vertex lattice model*, Annals of Physics **70** (1972), 193–228.
- [7] F. Borceux and D. Bourn, *Mal'cev, protomodular, homological and semi-abelian categories*, Mathematics and its Applications (Dordrecht), vol. 566, Springer, Dordrecht, 2004.
- [8] D. Bourn, *3×3 lemma and protomodularity*, Journal of Algebra **236** (2001), no. 2, 778–795.
- [9] ———, *Commutator theory in strongly protomodular categories*, Theory and Applications of Categories **13** (2004), 27–40, available at <https://eudml.org/doc/124941>.
- [10] ———, *Normal functors and strong protomodularity*, Theory and Applications of Categories **7** (2000), 206–218, available at <https://eudml.org/doc/120565>.
- [11] ———, *Normalization equivalence, kernel equivalence and affine categories*, Some thoughts on the future of category theory, 1991, pp. 43–62.
- [12] ———, *Split epimorphisms and Baer sums of skew left braces*, Journal of Algebra **652** (2024), 188–207.
- [13] D. Bourn, A. Facchini, and M. Pompili, *Aspects of the category SKB of skew braces*, Communications in Algebra **51** (2023), no. 5, 2129–2143.
- [14] D. Bourn and M. Gran, *Centrality and normality in protomodular categories*, Theory Appl. Categ. **9** (2001/02), 151–165. CT2000 Conference (Como).
- [15] D. Bourn and G. Janelidze, *Characterization of protomodular varieties of universal algebras*, Theory and Applications of Categories **11** (2003), 143–147, available at <https://eudml.org/doc/122876>.
- [16] S. Burris and H. P. Sankappanavar, *A course in universal algebra*, Graduate Texts in Mathematics, vol. 78, Springer, Cham, 1981.
- [17] F. Cedó, E. Jespers, and J. Okniński, *Braces and the Yang-Baxter equation*, Communications in Mathematical Physics **327** (2014), no. 1, 101–116.

- [18] F. Cedó and L. Vendramin, *Groups, radical rings, and the Yang-Baxter equation. A combinatorial approach to solutions*, Progress in Mathematics, vol. 361, Birkhäuser, Cham, 2026.
- [19] I. Colazzo, E. Jespers, Ł. Kubat, and A. Van Antwerpen, *Simple solutions of the Yang-Baxter equation*, 2025.arXiv:2312.09687
- [20] I. Colazzo, E. Jespers, A. Van Antwerpen, and C. Verwimp, *Left non-degenerate set-theoretic solutions of the Yang-Baxter equation and semitrusses*, Journal of Algebra **610** (2022), 409–462.
- [21] V. G. Drinfel'd, *On some unsolved problems in quantum group theory*, Quantum groups. Proceedings of workshops, held in the Euler International Mathematical Institute, Leningrad, USSR, Fall 1990, Berlin etc.: Springer-Verlag, 1992, pp. 1–8.
- [22] P. Etingof, T. Schedler, and A. Soloviev, *Set-theoretical solutions to the quantum Yang-Baxter equation*, Duke Mathematical Journal **100** (1999), no. 2, 169–209.
- [23] T. Gateva-Ivanova, *A combinatorial approach to noninvolutive set-theoretic solutions of the Yang-Baxter equation*, Publicacions Matemàtiques **65** (2021), no. 2, 747–808, available at ddd.uab.cat/record/248599.
- [24] T. Gateva-Ivanova and M. Van den Bergh, *Semigroups of I-type*, Journal of Algebra **206** (1998), no. 1, 97–112.
- [25] M. Gran and T. Everaert, *Monotone-light factorization systems and torsion theories*, Bulletin des Sciences Mathématiques **137** (2013), no. 8, 996–1006.
- [26] M. Gran and A. Sciandra, *Hopf braces and semi-abelian categories*, Journal of Algebra **690** (2026), 266–303.
- [27] M. Gran, T. Letourmy, and L. Vendramin, *Hopf formulae for homology of skew braces*, Journal of Pure and Applied Algebra **229** (2025), no. 11, 17. Id/No 108085.
- [28] M. Gran and A. Sciandra, *Hopf braces and semi-abelian categories*, Journal of Algebra **690** (2026), 266–303.
- [29] L. Guarnieri and L. Vendramin, *Skew braces and the Yang-Baxter equation*, Mathematics of Computation **86** (2017), no. 307, 2519–2534.
- [30] S. A. Huq, *Commutator, nilpotency, and solvability in categories*, The Quarterly Journal of Mathematics. Oxford Second Series **19** (1968), 363–389.
- [31] N. Jacobson, *The radical and semi-simplicity for arbitrary rings*, American Journal of Mathematics **67** (1945), 300–320.
- [32] G. Janelidze, L. Márki, and W. Tholen, *Semi-abelian categories*, Journal of Pure and Applied Algebra **168** (2002), no. 2-3, 367–386.
- [33] P. Jedlicka and A. Pilitowska, *Diagonals of solutions of the Yang-Baxter equation*, Forum Mathematicum **38** (2026), no. 2, 321–338.
- [34] T. Letourmy and L. Vendramin, *Schur covers of skew braces*, Journal of Algebra **644** (2024), 609–654.
- [35] J.-H. Lu, M. Yan, and Y.-C. Zhu, *On the set-theoretical Yang-Baxter equation*, Duke Mathematical Journal **104** (2000), no. 1, 1–18, available at hdl.handle.net/10722/156085.
- [36] N. Martins-Ferreira and T. Van der Linden, *A note on the “Smith is Huq” condition*, Applied Categorical Structures **20** (2012), no. 2, 175–187.
- [37] M. Pompili, *Yang-Baxter Equation and Category of Skew Braces* (2022).

- [38] F. Renaud, *Double coverings of racks and quandles* (2021).
- [39] W. Rump, *Braces, radical rings, and the quantum Yang-Baxter equation.*, Journal of Algebra **307** (2007), no. 1, 153–170.
- [40] J. D. H. Smith, *Mal'cev varieties*, Lecture Notes in Mathematics, vol. 554, Springer, Cham, 1976.
- [41] A. Soloviev, *Non-unitary set-theoretical solutions to the quantum Yang-Baxter equation.*, Mathematical Research Letters **7** (2000), no. 5-6, 577–596.
- [42] L. Vendramin, *Skew braces: a brief survey*, Geometric methods in physics XL, workshop, Białowieża, Poland, June 20–25, 2023, Cham: Birkhäuser, 2024, pp. 153–175.
- [43] A. Weinstein and P. Xu, *Classical solutions of the quantum Yang-Baxter equation*, Communications in Mathematical Physics **148** (1992), no. 2, 309–343.
- [44] C. N. Yang, *Some exact results for the many-body problem in one dimension with repulsive delta-function interaction*, Physical Review Letters **19** (1967), 1312–1315, available at edoc.hu-berlin.de/18452/20513.

UNIVERSITÉ CATHOLIQUE DE LOUVAIN

Faculté des sciences

Place des sciences, 2 bte L6.06.01, 1348 Louvain-la-Neuve, Belgique | www.uclouvain.be/sc