Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI CIVITA"
Corso di Laurea Magistrale in Matematica

Tesi di Laurea Magistrale

Yang-Baxter Equation and Category of Skew Braces

Candidato:
Mara Pompili
Matricola 2020279

Relatore:
Prof. Alberto Facchini

Anno Accademico 2021-2022
21 Luglio 2022

Ai miei angeli sulla terra,
Kevin, Emma, Alessandro,
Tommaso, Beatrice, Edoardo,
Beatrice e Camilla.

E ai miei angeli in cielo,
Giancarlo e Romeo

Contents

Introduction

The Yang–Baxter equation is an important equation coming from statistical mechanics, first appearing in the works of C.N. Yang [37] and R. Baxter [5]. A solution of the Yang-Baxter equation is a pair (V, R) with V a vector space and R a linear map $R\colon V \otimes V \to V \otimes V$ such that

$$(R \otimes id)(id \otimes R)(R \otimes id) = (id \otimes R)(R \otimes id)(id \otimes R).$$

In 1992 Drinfeld [16] remarked that was possible to study solutions of the Yang-Baxter equation studying a set-theoretical solutions, i.e. solutions on a basis of V. So a set-theoretical solution of the Yang-Baxter equation is a pair (X, r), where X is a set and $r\colon X \times X \to X \times X$ is a map such that $(r \times id)(id \times r)(r \times id) = (id \times r)(r \times id)(id \times r)$. Recently, subclasses of this type of solutions has receveid a lot of attention, not only for the applications of the Yang-Baxter equation in Physics, but also for its connection with other topics of recent interest in mathematics, like bijective 1-cocycles [17], knot theory, braid group, radical rings [32], regular subgroups of Hopf-Galois extensions [15, 19], and others.

If we write the map r by its components, i.e. $r(x, y) = (f_x(y), g_y(x))$, we say that r is non-degenerate if f_x, g_x are bijective maps. Initially, non-degenerate solutions were studying under the additional property of involutivity, that is adding the request that $r^2 = id$, for example by Etingof, Schedler and Soloviev in [17] and Gateva-Ivanova and Van den Bergh in [21]. After that, Soloviev [36] and Lu, Yan and Xhu [27], understood that, by removing the request for involution, with the same techniques it was possible to obtain results completely similar to those already reached.

In 2007, Rump [32] introduced a new algebraic structure, braces, that helps to study involutive non-degenerate solutions of the Yang-Baxter equation. A brace A is an abelian group $(A, +)$ with a further multiplication $(a, b) \mapsto ab$ such that A turns out to be a group with respect to $a \circ b := ab + a + b$. Rump proved that involutive non-degenerate solutions of the Yang-Baxter equation correspond exactly to braces. However, braces do not cover the results of Soloviev, and Lu, Yan, and Zhu for the non-involutive case. In 2017 Guarnieri and Vendramin [22] generalised the notion of braces, obtaining a one-to-one correspondence between this new algebraic structure and bijective non-degenerate solutions of the Yang-Baxter equation. They introduced what it is called a left skew brace. A skew brace is a triple $(A, *, \circ)$ where $(A, *)$ and $(A, \circ)$ are groups and $a \circ (b * c) = (a \circ b) * a^{-1} * (a \circ c)$ for every $a, b, c \in A$. The simplest examples of left skew braces are:

(1) For any associative ring $(R, +, \cdot)$, the Jacobson radical $(J(R), +, \circ)$, where $\circ$ is the operation on $J(R)$ defined by $x \circ y = xy + x + y$ for every $x, y \in J(R)$.

(2) For any group $(G, *)$, the left skew braces $(G, *, *)$ and $(G, *, *^{op})$.

In the thesis, we will be concern with the study of the algebraic structure of skew braces and their connection to the study of set-theoretical solutions of the Yang-Baxter equation.

In Chapter 1, we define what a left skew braces is, we describe its substructures (subbraces), ideals, and morphisms, and we describe their major properties. In Chapter 2 and 3 we study the category SKB of left skew braces. In particular, we consider the Huq commutator and Smith commutators of two ideals. These are two concepts borned respectivitely in Category Theory and Universal Algebra, and then extended in a number of directions. After giving the definition of the Huq commutator and Smith commutator for two ideals of a skew brace, we describe a set of generetors for them. Then we prove that they coincide. The condition "Huq=Smith" allows us to have a "nice" product between ideals. In this way the lattice of ideals of a skew brace becomes a multiplicative lattice in the sense of [18] and hence the notion of prime ideal, semiprime ideal, Zariski spectrum, nilpotency, solvability, centralizer, center, etc., have a natural meaning. The results of Chapter 3 are based on a paper written with D. Bourn and A. Facchini [7] that has been submitted for pubblication. In Chapter 4 we give an explicit description of the free skew brace over a set. Finally, in Chapter 5, we conclude with studying the Yang-Baxter equation and some other structures related to its solutions.

Chapter 1

Skew Braces

A left skew brace is an algebraic structure introducted by L. Guarnieri and Vendramin [22] in 2017. In this chapter we describe the main properties of left skew braces. Guarnieri and Vendramin defined a left skew brace to generalise the notion of left brace given by W. Rump [32].

1.1 Basic Definitions

Definition 1.1. A *left brace* is an additive abelian group $(A, +)$ with a further multiplication such that

$(B1)$ $a(b + c) = ab + bc$ for every $a, b, c \in A$

$(B2)$ $(A, \circ)$ is a group

where $a \circ b := ab + a + b$.

This is not the original definition of left brace given by W. Rump [32] in 2007. For Rump a left brace is an abelian group $(A, +)$ with a further multiplication $(a, b) \mapsto ab$, such that for all $a, b, c \in A$

$(R1)$ $a(b + c) = ab + ac$

$(R2)$ $(ab + a + b)c = a(bc) + ac + bc$

$(R3)$ the map $x \mapsto ax + x$ is a bijection.

Of course the two definitions are equivalent as the following proposition shows.

Proposition 1.2. *Let $(A, +)$ be an abelian group with a further multiplication $(a, b) \mapsto ab$. Then $(B1) - (B2)$ hold if and only if $(R1) - (R3)$ hold.*

Proof. First observe that the associativity of $\circ$ is equivalent to $(R2)$:

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

$$\Updownarrow$$

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

$$\Updownarrow$$

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

Now assume that $(B1) - (B2)$ hold. Notice that the map $x \mapsto ax + x$ can be rewritten as $x \mapsto -a + a \circ x$. Fix an element $a \in A$, call a' the inverse of a with respect to the operation $\circ$. Consider y another element of A and define $x := (y + a) \circ a'$. Then

$$a \circ (a' \circ (y + a)) - a = y,$$

that is the map is surjective and clearly it is also injective, since
$a \circ x - a = a \circ y - a \iff a \circ x = a \circ y \iff x = y$.
Conversely, assume that $(A, +)$ is an abelian group satisfying the properties $(R1) - (R3)$. We want to prove that $(A, \circ)$ is a group, with $a \circ b = ab + a + b$. We noticed at the beginning of th proof that $\circ$ is associative if $(R2)$ holds. Observe that by $(R1)$ we have

$$ab = a(b + 0) = ab + a0,$$

hence $a0 = 0$. Moreover, with $a = b = 0$ in $(R2)$, we obtain

$$0c = 0(0c) + 0c + 0c \Rightarrow 0 = 0(0c) + 0c,$$

and by $(R3)$ we have $0c = 0$. Thus

$$a \circ 0 = a0 + a + 0 = a$$

$$0 \circ a = 0a + 0 + a = a,$$

namely 0 is also the neutral element of $(A, \circ)$. Moreover let a' be the inverse image of $-a$ via the map $x \mapsto ax + x$, hence

$$a \circ a' = aa' + a + a' = -a + a = 0,$$

i.e. a' is a right inverse of a. Hence

$$a \circ a' \circ a = 0 \circ a = a \circ 0,$$

which gives $a' \circ a = 0$. This completes the proof.

□

Notice that $a(-b) = -ab$, indeed

$$a(-b) + ab = a(-b + b) = a0 = 0.$$

In 2017 L. Vendramin and L. Guarnieri [22] generalised the notion of braces to that of skew braces.

Definition 1.3. A *left skew brace* is a triple $(A, *, \circ)$, where $(A, *)$ and $(A, \circ)$ are groups (not necessarily abelian) such that

$$a \circ (b * c) = (a \circ b) * a^{-1} * (a \circ c), \tag{1.1}$$

for every $a, b, c \in A$. A *right skew brace* is defined similarly, replacing (1.1) by

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

A skew left brace also satisfying the condition of a right brace is called a *two-sided skew brace.*

We indicate with a^{-1}, a' the inverses of a respectively to the $*$ operation and the $\circ$ operation.

Observe that a brace is an example of skew brace. Indeed, if A is a brace, by definition $(A, +)$ and $(A, \circ)$ are groups. Moreover

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

and

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

Hence (1.1) holds.

We are going to present some general results about skew braces. Most of them appears in the original article of L. Vendramin and L. Guarnieri ([22]).

Lemma 1.4 ([22])**.** *Let A be a left skew brace. Then the following hold:*

1. $1_{(A,\circ)} = 1_{(A,*)}$.
2. $a \circ (b^{-1} * c) = a * (a \circ b)^{-1} * (a \circ c)$.
3. $a \circ (b * c^{-1}) = (a \circ b) * (a \circ c)^{-1} * a$.

Proof. The first claim comes from (1.1) with $c = 1_*$,

$$a \circ b = a \circ (b * 1_{(A,*)}) = (a \circ b) * a^{-1} * (a \circ 1_{(A,*)}),$$

hence $a = a \circ 1_{(A,*)}$. By unicity of the identity element, the first claim follows. To prove the second claim, let $d = b * c$. Then (1.1) becomes

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

hence $a \circ (b^{-1} * d) = a * (a \circ b)^{-1} * (a \circ d)$. The last claim is proved similarly. □

From now on, we indicate with 1 the neutral element of both the groups $(A, \circ)$ and $(A, *)$.

Examples 1.5.

1. For any group $(G, *)$, $(G, *, *)$ and $(G, *, *^{\text{op}})$ are two-sided skew braces. If $(G, *)$ is abelian, they coincide.
2. For any associative ring $(R, +, \cdot)$, the Jacobson radical $(J(R), \circ, +)$ is a brace, with $x \circ y = xy + x + y$ for every $x, y \in J(R)$.
3. Consider $\mathbb{Z}/n\mathbb{Z} = \langle g \rangle$ the cyclic group of n elements. Define the second operation as follows: $g^a * g^b := g^{(-1)^b a + b}$, for any $a, b \in \mathbb{N}$. Then $(\mathbb{Z}/n\mathbb{Z}, *, *)$ is a skew two-sided brace, where $*$ is the natural multiplication of $\mathbb{Z}/n\mathbb{Z}$.

Proposition 1.6 ([22])**.** *Let A be a skew brace. Then $\lambda : (A, \circ) \to \operatorname{Aut}(A, *)$, given by $\lambda : a \mapsto \lambda_a$, where $\lambda_a(b) = a^{-1} * (a \circ b)$, is a well defined group homomorphism.*

Proof.

1. *λ_a is an automorphism of $(A, *)$ for every $a \in A$.*

   Let $b, c \in A$. By (1.1) we have:

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

so λ_a is a group homomorphism. Moreover

$$\lambda_a(b) = \lambda_a(c) \iff a \circ b = a \circ c \iff b = c,$$

then λ_a is injective and if b is any element of A, then

$$b = \lambda_a(a' \circ (a * b)),$$

so $\lambda_a \in \mathrm{Aut}(A, *)$.

2. *λ is an homomorphism of groups.*

   We have to prove that

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

   for all $a, b, x \in A$. By definition of λ_a, for the left hand side we have

   $$\lambda_{a \circ b} = (a \circ b)^{-1} * ((a \circ b) \circ x);$$

   on the other hand the right hand side equals

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

   Now, by (1.1), $a \circ (b * b^{-1}) = (a \circ b) * a^{-1} * (a \circ b^{-1})$, hence

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

   By the associativity of $\circ$, we conclude.

□

Remark 1.7. Notice that, $\lambda_a = id_A$ if and only if for every $x \in A$, $a^{-1} * (a \circ x) = x$ if and only if $a \circ x = a * x$ for every $x \in A$.. Hence the kernel of λ is the normal subgroup of $(A, \circ)$

$$\{a \in A \mid a * x = a \circ x \text{ for all } x \in A\}.$$

Lemma 1.8. *Let A be a left skew brace. Then the map $\rho\colon (A, \circ) \to \mathrm{Aut}(A, *)$ given by $\rho\colon a \mapsto \rho_a$, where $\rho_a(b) = a' \circ (a * b)$ is a well-defined group anti-homomorphism. Moreover ρ_a and λ_a are mutually inverse automorphism of $(A, *)$.*

Proof. Notice that $\rho_a(b) = a' \circ (a * b) = (a' \circ a) * (a')^{-1} * (a' \circ b) = \lambda_{a'}(b)$, hence ρ_a is an automorphism of $(A, *)$ for every $a \in A$ and $\rho_{a_1 \circ a_2} = \lambda_{(a_1 \circ a_2)'} = \lambda_{a_2'} \lambda_{a_1'} = \rho_{a_2} \rho_{a_1}$, for every $a_1, a_2 \in A$, i.e. ρ is group anti-homomorphism. Moreover ρ and λ are clearly mutually inverse. □

Remark 1.9. It follows that

$$a \circ b = a * \lambda_a(b), \qquad a * b = a \circ \lambda_a^{-1}(b)$$

Lemma 1.10 ([26])**.** *Let $(A, *)$ be a group and $\lambda : (A, *) \to \mathrm{Aut}(A, *)$, $a \mapsto \lambda_a$ be a map such that*

$$\lambda_{a * \lambda_a(b)} = \lambda_a \lambda_b, \tag{1.2}$$

for every $a, b \in A$. Then A with $a \circ b = a * \lambda_a(b)$ is a left skew brace.

Proof. First of all notice that, with $a = b = 1$ in (1.2), we get $\lambda_1 = id$. This implies that $a \circ 1 = a * \lambda_a(1) = a * 1 = a$ and $1 \circ a = 1 * \lambda_1(a) = 1 * a = a$. Hence 1 is the neutral element also for $(A, \circ)$. Moreover, consider $b = \lambda_a^{-1}(a^{-1})$ in (1.2) becomes $\lambda_a \lambda_{\lambda_a^{-1}(a^{-1})} = id$. Then the inverse with respect to $(A, \circ)$ of an element a is $a' := \lambda_a^{-1}(a^{-1})$, indeed

$$a \circ \lambda_a^{-1}(a^{-1}) = a * \lambda_a(\lambda_a^{-1}(a^{-1})) = a * a^{-1} = 1$$

and

$$\lambda_a^{-1}(a^{-1}) \circ a = \lambda_a^{-1}(a^{-1}) * \lambda_{\lambda_a^{-1}(a^{-1})}(a) = (\lambda_a^{-1}(a))^{-1} * \lambda_a^{-1}(a) = 1.$$

We check now the associativity of " $\circ$ ". For every $a, b, c \in A$ we have

$$a \circ (b \circ c) = a * \lambda_a(b * \lambda_b(c)) = a * \lambda_a(b) * \lambda_a \lambda_b(c),$$

and on the other hand

$$(a \circ b) \circ c = a * \lambda_a(b) * \lambda_{a * \lambda_a(b)}(c) = a * \lambda_a(b) * \lambda_a \lambda_b(c).$$

Finally we check the skew brace condition:

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

where the last equality was obtained multiplying by $a * a^{-1}$. □

1.2 Subbraces and Ideals

Definition 1.11. Let $(A, *, \circ)$ be a left skew brace. Consider X a subset of A. We say that

1. X is a *subbrace* of A if it is a subgroup of $(A, \circ)$ and $(A, *)$. We will write $X \leq A$;

2. X is an *ideal* of A if it is a normal subgroup of both $(A, \circ)$ and $(A, *)$ such that $a * I = a \circ I$ for every $a \in A$. We will write $I \trianglelefteq A$.

Remark 1.12. Notice that a normal subgroup I of $(A, \circ)$ and $(A, *)$ is an ideal of a left skew brace $(A, *, \circ)$ if and only if $\lambda_a(I) \subseteq I$. Indeed if I is an ideal then $\lambda_a(i) = a^{-1} * (a \circ i) = a^{-1} * (a * i_0) = a^{-1} * i_1 * a$ for some $i_0, i_1 \in I$. But since I is normal in $(A, *)$, we have that $\lambda_a(i) \in I$ for every $a \in A$.

Conversely, let $a \in A$ and $i \in I$. Then there exists $i_0 \in I$ such that $\lambda_a(i) = a^{-1} * (a \circ i) = i_0$, hence $a \circ i = a * i_0$.

Proposition 1.13. *There is a one-to-one correspondence between the set of all ideals of a left skew brace A and congruences on A, that is the equivalence relations $\sim$ on Asuch that $a \sim b, c \sim d$ implies $a * c \sim b * d$ and $a \circ c \sim c \circ d$, for every $a, b, c, d \in A$.*

Proof. Let $\sim$ be a congruences of A. Define $I = [1]_\sim$. By the reflexivity of $\sim$, $1 \in I$. Moreover let $a, b \in I$, then $a \sim 1$, and $b \sim 1$, thus $1 \sim b$, so $a \sim b$ and, since $b' \sim b'$ we have, $a \circ b' \sim b \circ b' = 1$. Moreover if $x \sim 1$ and a is any element of A, then $a \sim a$ and $a' \sim a'$ then by compatibility $a' \circ x \circ a \sim a' \circ 1 \circ a = 1$. Similarly, $a^{-1} * x * a \sim a^{-1} * 1 * a = 1$ for every $a \in A$, $x \in I$. So it remains to check that $\lambda_a(x) \in I$ for every $a \in A, x \in I$. We have that $a^{-1} \sim a^{-1}, a \sim a, x \sim 1$, then $a \circ x \sim a \circ 1 = a$ and $a^{-1} * (a \circ x) \sim a^{-1} * a = 1$. Therefore, I is an ideal of A.
Conversely, let I be any ideal and define a relation on A as follows,

$$x \sim_I y \iff x \circ y' \in I,$$

for all $x, y \in A$. It is an equivalence relation:

Reflexivity. $x \circ x' = 1 \in I$;

Symmetry. $x \circ y' \in I \implies (x \circ y')' = y \circ x' \in I$;

Transitivity. $x \circ y' \in I, y \circ z' \in I \implies (x \circ y') \circ (y \circ z') = x \circ z' \in I$.

Let us check the compatibility with the operations. If $a \sim_I b$ and $c \sim_I d$, then $a \circ b' \in I, c \circ d' \in I$. But then $b \circ (c \circ d') \circ b' \in I$ because I is a normal subgroup of $(A, \circ)$, hence $a \circ c \circ (b \circ d)' = a \circ c \circ d' \circ b' = (a \circ b') \circ (b \circ c \circ d' \circ b') \in I$, that is $a \circ c \sim_I b \circ d$. Moreover, since $a \circ I = a * I$, for every $a \in A$ and since I is a normal subgroup of $(A, *)$, we have that $x \sim_I y$ if and only if $x * y^{-1} \in I$. Therefore $a \sim_I b$ and $c \sim_I d$ imply $a * b^{-1} \in I$ and $c * d^{-1} \in I$, hence we can conclude that $a * c * (b * d)^{-1} \in I$ with similar argument used for the compatibility with $\circ$.

Finally, for every ideal I, we have that $I = [1]_{\sim_I}$, since

$$[1]_{\sim_I} = \{a \in A \mid a \sim_I 1\} = \{a \in A \mid a \in I\} = I,$$

and for every equivalence relation $\sim$ compatible with the operation, the equivalence relation $\sim_{[1]_\sim}$ coincide with $\sim$, since, for every $x, y \in A$,

$$x \sim_{[1]_\sim} y \Leftrightarrow x \circ y' \in [1]_\sim \Leftrightarrow x \circ y' \sim 1 \Leftrightarrow x \sim y.$$

□

By definition of ideal, the quotient groups A/I for both operations are the same, then A/I is a skew brace, with the natural operations.

Let A be a left skew brace, B a subbrace and I an ideal. Denote with $B * I$ the set $\{b * i \mid b \in B\, i \in I\}$ and with $B \circ I$ the set $\{b \circ i \mid b \in B\, i \in I\}$.

Lemma 1.14. *Given a left skew brace A, consider B a subbrace and I an ideal. We have:*

(1) *the sets $B * I$ and $B \circ I$ coincide;*

(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. Let B be a subbrace of A and I an ideal of A.

1. Observe that $B * I = \bigcup_{b \in B} b * I$ and $B \circ I = \bigcup_{b \in B} b \circ I$. Since I is an ideal, $b * I = b \circ I$, hence

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

2. Trivial, since $(B * I, *)$ is a subgroup of $(A, *)$ and $(B \circ I, \circ)$ is a subgroup of $(A, \circ)$.

3. Suppose $B = J$ is an ideal of A. Clearly, $(J * I, *)$ is a normal subgroup of $(A, *)$ and $(J \circ I, \circ)$ is a normal subgroup of $(A, \circ)$. Moreover, let $a \in A$. We have

$$\begin{aligned} a \circ (J * I) = a \circ (J \circ I) &= \bigcup_{j \in J} (a \circ j) \circ I = \bigcup_{j \in J} (a * \lambda_a(j)) \circ I \\ &= \bigcup_{j \in J} (a * \lambda_a(j) * I) = a * (I * J). \end{aligned}$$

   Hence $J * I = I * J = I \circ J = J \circ I$ is an ideal of A.

□

From now on, we indicate with BI the subbrace $B * I = B \circ I$. Observe that $B \subseteq BI$ and $I \subseteq BI$.

Proposition 1.15. (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 again a subbrace.*

(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 again an ideal.*

Proof. (1) B_α is a subgroup of $(A, \circ)$ and of $(A, *)$, hence $\bigcap_{\alpha \in S} B_\alpha$ is a subgroup of both $(A, \circ)$ and $(A, *)$.

(2) I_α is a normal subgroup of $(A, \circ)$ and of $(A, *)$, hence $\bigcap_{\alpha \in S} I_\alpha$ is a normal subgroup of both $(A, \circ)$ and $(A, *)$. Moreover, let $x \in \bigcap_{\alpha \in S} I_\alpha$, then $x \in I_\alpha$ implies that $\lambda_a(x) \in I_\alpha$, for all $a \in A$ and for all $\alpha \in S$, hence $\lambda_a(x) \in \bigcap_{\alpha \in S} I_\alpha$. □

Definition 1.16. (1) The *subbrace $\langle X \rangle_{\text{sb}}$ generated by X* is the interesection of all the subbraces that contain X, i.e.

$$\langle X \rangle_{\text{sb}} := \bigcap_{\substack{B \leq A \\ B \subseteq X}} B.$$

(2) The *ideal $\langle X \rangle_{\text{id}}$ generated by X* is the interesection of all the ideals that contain X, i.e.

$$\langle X \rangle_{\text{id}} := \bigcap_{\substack{I \trianglelefteq A \\ I \supseteq X}} I.$$

Proposition 1.17. *Let A be a left skew brace, B a subbrace of A and I an ideal of A. Then $BI = \langle B, I\rangle_{\mathrm{sb}}$.*

Proof. $\langle B, I\rangle_{\mathrm{sb}}$ is a subbrace that contains B and I hence contains all the products $b * i$ with $b \in B$ and $i \in I$. Therefore, $BI \subseteq \langle B, I\rangle_{\mathrm{sb}}$. Conversely, by Lemma 1.14, BI is subbrace of A that contains B and I, hence $\langle B, I\rangle_{\mathrm{sb}} \subseteq BI$, hence the thesis. □

Definition 1.18. An ideal I of a skew brace A is said to be a *principal ideal* if $I = \langle \{x\}\rangle_{\mathrm{id}}$, with $x \in A$. We indicate it as $\langle x\rangle$.

Proposition 1.19. *Let A be a left skew brace and $\{I_\alpha\}_{\alpha\in A}$ a chain of ideals of A. Then $\bigcup_{\alpha\in S} I_\alpha$ is an ideal of A.*

Proof. Let us prove that $(\bigcup_{\alpha\in S} I_\alpha, *)$ is a normal subgroup of $(A, *)$. First notice that $1 \in \bigcup_{\alpha\in S} I_\alpha$ since it belongs to every I_α. Now let $x, y \in \bigcup_{\alpha\in S} I_\alpha$, then there exist $\alpha, \beta \in S$ such that $x \in I_\alpha$ and $y \in I_\beta$. Since $\{I_\alpha\}_{\alpha\in A}$ is linearly ordered, without loss of generality suppose $I_\alpha \subseteq I_\beta$. Hence $x * y^{-1} \in I_\beta$, but then $x * y^{-1} \in \bigcup_{\alpha\in S} I_\alpha$. Moreover, let $x \in \bigcup_{\alpha\in S} I_\alpha$ and $a \in A$. Then there exists $\alpha \in S$ such that $x \in I_\alpha$, but then $a * x * a^{-1} \in I_\alpha \subseteq \bigcup_{\alpha\in S} I_\alpha$. This proves that $(\bigcup_{\alpha\in S} I_\alpha, *)$ is a normal subgroup of $(A, *)$.Similarly it can be proven that $(\bigcup_{\alpha\in S} I_\alpha, \circ)$ is a normal subgroup of $(A, \circ)$.

Finally, let $x \in \bigcup_{\alpha\in S} I_\alpha$ and $a \in A$. We have that $x \in I_\alpha$ for some $\alpha \in S$. Since I_α is an ideal, $\lambda_a(x) \in I_\alpha$ and hence belongs to $\bigcup_{\alpha\in S} I_\alpha$. This concludes the proof. □

The Center of a Left Skew Brace

Define the center $Z(A)$ of a left skew brace A as follow

$$Z(A) := \{a \in A \mid a * x = x * a,\ a \circ x = x \circ a,\ a \circ x = a * x,\ \text{for all}\, x \in A\}.$$

In literature the center is often called the socle.

Proposition 1.20. *Let A be a left skew brace. $Z(A)$ is an ideal of A. Moreover $Z(A) = Z(A, *) \cap Z(A, \circ) \cap \operatorname{Ker} \lambda$.*

Proof. Notice that the condition $a \circ x = a * x$ for every $x \in A$ is equivalent to saying that $\lambda_a = id_{(A,*)}$ for every $a \in Z(A)$. Moreover $a' = a^{-1}$ for every $a \in Z(A)$.

Let us prove that $Z(A)$ is a subgroup of $(A, \circ)$. Clearly $1 \in Z(A)$. Let $a, b \in Z(A)$, then $a \circ b' \in Z(A)$. Indeed

$$\lambda_{a \circ b'} = \lambda_a \lambda_{b'} = \lambda_a \lambda_b^{-1} = id.$$

Moreover for every $x \in A$ we have that:

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

$$(a \circ b) * x = (a * b) * x = a * (b * x) = a * (x * b) = (x * b) * a = x * (a \circ b),$$

$$a' \circ x = (x' \circ a)' = (a \circ x')' = x \circ a,$$

$$a' * x = a^{-1} * x = (x^{-1} * a)^{-1} = (a * x^{-1})^{-1} = x * a^{-1} = x * a'.$$

$Z(A)$ is a subgroup also of $(A, *)$, because in $Z(A)$ the two operations coincide. Clearly $Z(A)$ is a normal subgroup of $(A, \circ)$ and $(A, *)$, because $x' \circ a \circ x = a = x^{-1} * a * x$ for every $a \in Z(A)$ and $x \in A$.

We conclude observing that $\lambda_x(Z(A)) = Z(A)$ for every $x \in A$, therefore $Z(A)$ is an ideal of A. □

Remark 1.21. If A is a left brace in the classic sense as in Definition 1.1, then the center of A is

$$Z(A) = \{a \in A \mid ab = ba = 0 \,\text{for all}\, b \in A\}.$$

1.3 Skew Braces and G-groups

Let us recall the definition and some properties of G-groups.

Definition 1.22. For any two groups G and H we say that H is a *left G-group* if there is a group homomorphism $\alpha : G \to \operatorname{Aut}(H)$.

Equivalently, a G-group is a group H endowed with a mapping $G \times H \to H$, $(g, h) \mapsto gh$, called *left scalar multiplication*, such that

(i) $g(hh') = (gh)(gh')$,

(ii) $(gg')h = g(g'h)$,

(iii) $1_G h = h$,

for every $g, g' \in G$ and every $h, h' \in H$.

Hence for any skew brace $(A, *, \circ)$, we have that $(A, *)$ is an $(A, \circ)$-group with respect to the group homomorphism λ descriped in Proposition 1.6. Conversely, suppose that a set A has two group structures $(A, \circ)$ and $(A, *)$ and that $(A, *)$ is an $(A, \circ)$-group with respect to the group homomorphism $\lambda : (A, \circ) \to \mathrm{Aut}(A, *)$, defined by $\lambda : a \mapsto \lambda_a$, where $\lambda_a(b) = a^{-1} * (a \circ b)$. Then, since λ_a is an automorphism, $\lambda_a(b * c) = \lambda_a(b) * \lambda_a(c)$, i.e. $a^{-1} * (a \circ (b*c)) = a^{-1} * (a \circ b) * a^{-1} * (a \circ c)$, from which $a \circ (b*c) = (a \circ b) * a^{-1} * (a \circ c)$. Hence skew braces are exactly those particular G-groups (H, λ) for which $G = H$ as sets, and λ is defined by $\lambda_a(b) = a^{-1} * (a \circ b)$.

The semidirect product corresponding to such $(A, \circ)$- group $(A, *)$ is the group $P := (A, *) \ltimes (A, \circ)$, i.e. the cartesian product $P := A \times A$ with the group operation defined as

$$(a_1, a_2)(b_1, b_2) = (a_1 * a_2^{-1} * (a_2 \circ b_1), a_2 \circ b_2). \tag{1.3}$$

Conversely, given two groups $(A, \circ)$ and $(A, *)$ on the same set A such that $P := A \times A$ with the operation as in (1.3) is a group, then $(A, *, \circ)$ is a left skew brace.

Proposition 1.23. *Let A be a left skew brace. Then $Z(A) \times Z(A) \subseteq Z(P)$.*

Proof. The center of the group $P = (A, *) \ltimes (A, \circ)$ is the set

$$\{(a, b) \in P \mid (a, b)(x, y) = (x, y)(a, b) \,\text{for all}\, (x, y) \in P\},$$

namely

$$\{(a, b) \mid (a * \lambda_b(x), b \circ y) = (x * \lambda_y(a), y \circ b)\}.$$

Let $(a, b) \in Z(A) \times Z(A)$, then $a * (\lambda_b(x)) = a * x = x * a = x * \lambda_y(a)$ and $b \circ y = y \circ b$, that is $(a, b) \in Z(P)$ as we wanted to prove. □

Proposition 1.24. *A subset X of a brace A is a subbrace of A if and only if $X \times X$ is a subgroup of P.*

Proof. Let X be a subbrace. Consider $(x_1, x_2), (y_1, y_2) \in X \times X$, then

$$(x_1, x_2)(y_1, y_2) = (x_1 * x_2^{-1} * (x_2 \circ y_1), x_2 \circ y_2) \in X \times X$$

since X is a subgroup of $(A, \circ)$ and $(A, *)$.

Conversely, let us suppose that $X \times X$ is a subgroup of P, then for every $x, y \in X$, $(1, x)(1, y) = (1, x \circ y) \in X \times X$ implies that $x \circ y \in X$ and, on the other hand, $(x, 1)(y, 1) = (x * y, 1) \in X \times X$ implies that $x * y \in X$.

□

1.4 Morphisms

Definition 1.25. Let A, B be two left skew braces and $f \colon A \to B$ a mapping. We say that f is a skew brace morphism if:

1. $f(x * y) = f(x) * f(y)$
2. $f(x \circ y) = f(x) \circ f(y)$,

for every $x, y \in A$.

We denote by $\operatorname{Ker} f$ the subset $\{a \in A \mid f(a) = 1\}$ and by $\operatorname{Im} f$ the subset $\{b \in B \mid \exists\, a \in A \text{ s.t. } b = f(a)\}$.

Proposition 1.26. *Let $f \colon A \to B$ be a skew brace morphism, then*

1. $\operatorname{Im} f$ *is a subbrace of B;*
2. $\operatorname{Ker} f$ *is an ideal of A;*
3. *every ideal is the kernel of a skew brace morphism.*

Proof. 1. Let b_1, b_2 be two element of $\operatorname{Im} f$. Then there exist $a_1, a_2 \in A$ such that $b_1 = f(a_1)$, $b_2 = f(a_2)$. Hence

$$b_2 * b_1^{-1} = f(a_2) * f(a_1)^{-1} = f(a_2 * a_1^{-1}),$$

and

$$b_2 \circ b_1' = f(a_2) \circ f(a_1)' = f(a_2 \circ a_1'),$$

so $b_2 * b_1^{-1}, b_2 \circ b_1' \in \operatorname{Im} f$.

2. Let $x, y \in \operatorname{Ker} f$ and $a \in A$. Then

$$f(x \circ y') = f(x) \circ f(y)' = 1,$$

   and

$$f(a' \circ x \circ a) = f(a') \circ f(x) \circ f(a) = f(a') \circ f(a) = f(1) = 1,$$

   hence $\operatorname{Ker} f$ is a normal subgroup of $(A, \circ)$. Similarly $\operatorname{Ker} f$ is a normal subgroup of $(A, *)$. Moreover, if $a \in A$ and $x \in \operatorname{Ker} f$, $f(\lambda_a(x)) = f(a)^{-1} * f(a \circ x) = f(a)^{-1} * f(a) = 1$, i.e. $\lambda_a(x) \in \operatorname{Ker} f$ for every $a \in A$ and every $x \in \operatorname{Ker} f$.

3. It sufficies to consider the projection $A \to A/I$, that maps a into $a \circ I$. Then, by construction, the kernel is I.

□

Proposition 1.27. *A skew braces morphism $f \colon A \to B$ is injective if and only if* $\operatorname{Ker} f = 1$.

Proof. Assume f injective. If $x \in \operatorname{Ker} f$, then $f(a) = 1 = f(1)$, hence $a = 1$. Conversely, let $x, y \in A$ such that $f(x) = f(y)$. Then $f(x * y^{-1}) = 1$, that is $x * y^{-1} \in \operatorname{Ker} f = 1$, so $x * y^{-1} = 1$. □

1.5 Isomorphism Theorems

As we can expect, the classical isomorphism theorems also hold for braces.

Theorem 1.28. *Let $f : A \to B$ be a skew brace morphism. Then*

$$A/\operatorname{Ker} f \cong \operatorname{Im} f. \tag{1.4}$$

Proof. Call K the kernel of f. Our aim is to construct an isomorphism

$$\phi : A/K \to \operatorname{Im} f.$$

Let $\bar{x} \in A/K$ be a coset, and define $\phi(\bar{x}) = f(x)$.
We claim that ϕ is a well defined map. Indeed, let $y \in A$ be another

representative of $\bar{x}$, namely $x * y^{-1} \in K$, which means that $f(x * y^{-1}) = 1$. But then

$$\phi(\bar{x}) * \phi(\bar{y})^{-1} = f(x) * f(y)^{-1} = f(x * y^{-1}) = 1.$$

Moreover ϕ is a skew brace morphism, since, for every $x, y \in A$ we have

- $\phi(\bar{x}) * \phi(\bar{y}) = f(x) * f(y) = f(x * y) = \phi(\overline{x * y}) = \phi(\bar{x} * \bar{y})$;
- $\phi(\bar{x}) \circ \phi(\bar{y}) = f(x) \circ f(y) = f(x \circ y) = \phi(\overline{x \circ y}) = \phi(\bar{x} \circ \bar{y})$.

It remains to prove that ϕ is bijective.

- Injectivity.
  Suppose $\phi(\bar{a}) = 1$. Then, by definition, $f(a) = 1$. This means that $a \in K$, thus $\bar{a} = a * K = K$.
- Surjectivity
  Let $b \in \operatorname{Im} f$. Then, since there exist $a \in A$ s.t. $b = f(a)$, $b = \phi(\bar{a})$.

□

Theorem 1.29. *Let A be a left skew brace. For every subbrace B of A and every ideal I of A, we have that*

$$BI/I \cong B/B \cap I. \tag{1.5}$$

Proof. Define a skew brace morphism $\pi : B \to BI/I$, by $\pi(b) = b * I$. For every elements $b \in B$ $i \in I$, we have $(b * i) * I = b * I = \pi(b)$, therefore π is surjective. Moreover, $\text{Ker}\ \pi = \{b \in B \mid b * I = I\} = \{b \in B \mid b \in I\} = B \cap I$. Hence, by Theorem 1.28, $B/B \cap I \cong BI/I$. □

Theorem 1.30. *Let I, J be ideals of a skew brace A such that $I \subseteq J$. Then*

$$(A/I)/(J/I) \cong A/J. \tag{1.6}$$

Proof. Define a function

$$\phi : A/I \to A/J,$$

by $\phi(a * I) = a * J$.

Let us check that it is well defined. If $a * I = bI \in A/I$, then $a * b^{-1} \in I$ and as $I \subseteq J$, we have that $a * b^{-1} \in J$, so $a * I = b * I$.

Clearly, ϕ is a surjective skew brace morphism. Now an element $a * I \in A/I$ belongs to the kernel of ϕ if and only if $a * J = J$ if and only if $a \in J$. Then Ker $\phi = J/I$.
Hence, by the First Isomorphism Theorem, we have

$$(A/I)/(J/I) \cong A/J.$$

□

Chapter 2

Category of Left Skew Braces

We will denoted by SKB the category of all left skew braces.

We will show some basic properties of SKB, for example that is equivalent to the categor of bijective 1-cocycles. Moreover we will study the Huq Commutator and Smith Commutator in SKB.

2.1 Digroups

In Section 1.3 we proved that left skew braces are particular groups, in the sense that there is a faithful functor $\mathsf{SKB} \to \mathsf{Grp}$, $A \mapsto P = (A, *) \ltimes (A, \circ)$, $f \mapsto f \times f$, because every skew brace morphism $f \colon A \to A'$ induces a corresponding group morphism $f \times f \colon P = A \ltimes A \to P' = A' \ltimes A'$, $(f \times f)(a, b) = (f(a), f(b))$.

Recall that in a skew brace the units of the two groups coincide. So, SKB appears as a fully faithful subcategory $\mathsf{SKB} \hookrightarrow \mathsf{Digp}$ of the category Digp of digroups, where a *digroup* is a triple $(G, *, \circ)$ of a set G endowed with two group structures with same unit. This notion was introduced in [10] by D. Bourn. There are two forgetful functors $U_i : \mathsf{DiGp} \to \mathsf{Grp}$, $i \in \{0, 1\}$, associating respectively the first and the second group structures. They both reflect isomorphisms. Since U_0 is left exact and reflects isomorphisms, it naturally allows the lifting of the semiabelian aspects of the category Grp of groups to the category DiGp. In turn, the left exact fully faithful embedding $\mathsf{SKB} \hookrightarrow \mathsf{DiGp}$ makes SKB a semiabelian category. The notion of semiabelian category was introducted in [24] and it is beyond our discussion, but in a semi-abelian category the notions of Huq Commutator and Smith Commutator simplify. The notion of semiabelian category arised to capture typical algebraic properties valid for groups, rings and algebras, say, just as abelian categories allow for a generalized treatment of abelian-group and module theory.

2.2 Abelian Objects

Recall [20] that an object C of a semi-abelian category $\mathcal{C}$ is *abelian* when the identity of C commutes with itself, or, equivalently, when C can be provided with the structure of an abelian group, that is, there exists a morphism $m\colon C \times C \to C$ in $\mathcal{C}$ such that $m \circ (\mathrm{id}_C, 0) = m \circ (0, \mathrm{id}_C) = \mathrm{id}_C$.

Lemma 2.1. *A left skew brace $(A, *, \circ)$ is an abelian object in the semi-abelian category* SKB *if and only if the two multiplications $\circ$ and $*$ coincide and are commutative.*

Proof. If $\circ$ and $*$ coincide and are commutative, then clearly the morphism $m\colon A \times A \to A$ in SKB defined by $m(a, b) = a * b$ is such that $m \circ (\mathrm{id}_A, 0) = m \circ (0, \mathrm{id}_A) = \mathrm{id}_A$.

Conversely suppose that $(A, *, \circ)$ is a left skew brace and that there is a morphism $m\colon A \times A \to A$ is such that $m \circ (\mathrm{id}_A, 0) = m \circ (0, \mathrm{id}_A) = \mathrm{id}_A$. Applying the faithful functor $\mathsf{SKB} \to \mathsf{Grp}$, $A \mapsto P = (A, *) \ltimes (A, \circ)$, $f \mapsto f \times f$, we get a morphism $m'\colon P \times P \to P$ in Grp such that $m' \circ (\mathrm{id}_P, 0) = m' \circ (0, \mathrm{id}_P) = \mathrm{id}_P$. The unique group morphism with this property is the multiplication $m'\colon P \times P \to P$. But if the multiplication is a group morphism, the group is necessarily abelian. Hence P is an abelian group. Since the two groups $(A, \circ)$ and $(A, *)$ are canonically isomorphic to subgroups of P, it follows that both $(A, \circ)$ and $(A, *)$ are abelian groups. Moreover, if $a, b \in A$, the equality $(a, a) \cdot (b, 1) = (b, 1) \cdot (a, a)$ in P and (1.3) give $a * a^{-1} * (a \circ b) = b * 1^{-1} * (1 \circ a)$, so $a \circ b = b * a = a * b$. Thus $\circ$ and $*$ coincide. □

2.3 Kernel, Cokernel and Product

SKB has a zero object that is the trivial brace with only the identity.

In Chapter 1, we have defined the kernel of a morphism as the set of elements that are mapped in the identity. Consider a morphism of left skew brace $f\colon A \to B$, $K := \operatorname{Ker} f$ the kernel of f, and $i\colon K \hookrightarrow A$ the natural inclusion.

Proposition 2.2. *(K, i) is the kernel of f in the category SKB.*

Proof. Clearly, $fi = 0$. So let $\epsilon \in \operatorname{Hom}_{\mathsf{SKB}}(H, A)$ be such that $f\epsilon = 0$. We need to define $\alpha\colon H \to K$ such that the diagram

$$\begin{tikzcd}
K \arrow[r, hook, "i"] & A \arrow[r, "f"] & B \\
& H \arrow[u, "\epsilon"] \arrow[ul, dashed, "\alpha"] &
\end{tikzcd}$$

commutes. Set $\alpha(h) := \epsilon(h)$ for every $h \in H$. Then α is well defined and $\alpha i = \epsilon$. Moreover, by construction, α is unique. □

Proposition 2.3. *Let $f\colon A \to B$ be a skew brace morphism, Then f is a monomorphism if and only if it is injective.*

Proof. Suppose that f is a monomorphism. Consider the following diagram

$$\begin{tikzcd}
\operatorname{Ker} f \arrow[r, shift left, "i"] \arrow[r, shift right, "0"'] & A \arrow[r, "f"] & B
\end{tikzcd}$$

Then $fi = f0 = 0$ implies $i = 0$. But this implies that $\operatorname{Ker} f = 1$, so f is injective. Conversely, if f is injective, then f is clearly a monomorphism. □

Let $f\colon A \to B$ be a left skew brace morphism. Denote by C the ideal $\langle f(A) \rangle$ of B generated by $f(A)$ and let $p\colon B \to B/C$ be the projection.

Proposition 2.4. *$(B/C, p)$ is the cokernel of f.*

Proof. Claerly $pf(a) = f(a) \circ C = C$. Moreover let (D, q), $q\colon Y \to D$ be such that $qf = 0$. We want to define $\bar{q}\colon Y/C \to D$ such that the following diagram commutes:

$$\begin{tikzcd}
A \arrow[r, "f"] & B \arrow[r, "p"] \arrow[d, "q"] & Y/C \arrow[dl, dashed, "\bar{q}"] \\
& D &
\end{tikzcd}$$

So set $\bar{q}(b \circ C) := q(b)$. It is a well defined morphism because, if by contradiction there exist $b_1, b_2 \in B$ such that $b_1 \circ C = b_2 \circ C$ and $q(b_1) \neq q(b_2)$, then $b_1 \circ b_2' \in C \setminus \operatorname{Ker} q$. Recall that $\operatorname{Ker} q$ is an ideal of B, moreover, since $qf = 0$, $\operatorname{Ker} q \supseteq \operatorname{Im} f$ and so that $C \subseteq \operatorname{Ker} q$ and this is a contradiction. □

Let A, B be two left skew braces. The *product* of A and B is the cartesian product with operations defined componentwise, i.e. it is the cartesian product $(A \times B, *, \circ)$ with $(a_1, b_1) * (a_2, b_2) = (a_1 * b_1, a_2 * b_2)$ and $(a_1, b_1) \circ (a_2, b_2) = (a_1 \circ b_1, a_2 \circ b_2)$. Clealy, $A \times B$ is a skew brace.

Proposition 2.5. *Let A and B be two skew braces. Then $A \times B$ satisfy the universal product, namely for every two skew brace morphism $f \colon C \to A$, $g \colon C \to B$, there exist a unique $\varphi \colon C \to A \times B$ such that the following diagram commutes*

$$\begin{tikzcd}
 & A \times B \arrow[dl, "\pi_A"'] \arrow[dr, "\pi_B"] & \\
A & & B \\
 & C \arrow[ul, "f"] \arrow[ur, "g"'] \arrow[uu, "\varphi"] &
\end{tikzcd}$$

Proof. The claim follows setting $\varphi(c) := (f(c), g(c))$. □

2.4 n-cocycles and Skew Braces

Let us recall some basic definitions on group cohomology. Let G be a group. It is well known that the category of G-groups H with H abelian is isomorphic to the category $\mathbb{Z}[G] - \mathsf{Mod}$ of left $\mathbb{Z}[G]-$modules.

If $(G, \cdot)$ is a group and $(H, +)$ is an abelian G-group, denote with $g.h$ the action of g on h, namely $g.h = \alpha(g)(h)$, where $\alpha \colon G \to \operatorname{Aut}(H)$ is the group homomorphism that makes H a G-group. For every $n \geq 0$, let $C^n(G, H)$ the abelian group of all functions from G^n to H. Its element are called *n-cochains*. Since $G^0 = \{1\}$, we have that $C^0(G, H) \cong H$. Consider the *co-boundary homeomorphisms*

$$d^{n+1} \colon C^n(G, H) \to C^{n+1}(G, H)$$

defined as follows

$$(d^{n+1}\varphi)(g_1 \cdots g_{n+1}) = g_1.\varphi(g_2 \cdots g_{n+1}) - \varphi(g_1 g_2, \cdots g_{n+1}) + \\ + \varphi(g_1, g_2 g_3, \cdots, g_{n+1}) - \cdots + (-1)^{n+1}\varphi(g_1, \cdots g_n).$$

We have that $d^{n+1} \circ d^n = 0$, so this defines a cochain complex whose cohomology can be computed. It can be shown that the above-mentioned definition of group-cohomology in terms of derived functors is isomorphic to

$$H^n(G, H) = Z^n(G, H)/B^n(G, H),$$

where $Z^n(G, H)$ is the kernel $\mathrm{Ker}\,(d^{n+1})$ of d^{n+1} and $B^n(G, H)$ is 0 if $n = 0$ and is the image $\mathrm{Im}(d^n)$ of d^n if $n \geq 1$. The elements of $Z^n(G, H)$ are called *n-cocycles* and the elements of $B^n(G, H)$ are called *n-coboundaries.* In particular, a n-cocycle is a map $\varphi\colon G^n \to H$ such that

$$g_1.\varphi(g_2 \cdots g_{n+1}) + \sum_{i=1}^{n} (-1)^i \varphi(g_1 \cdots g_{i-1} g_{i+1} \cdots g_{n+1}) + (-1)^{n+1}\varphi(g_1 \cdots g_n) = 0$$

If H is not abelian and $n > 1$, the sum above is not well-defined, hence this description does not work for the cohomology of the non-abelian case.

However, it is possible to compute the zero and first comohology for a non-abelian group. Let H be a not-necessarily abelian G-group with $\alpha\colon G \to \mathrm{Aut}(H)$. Now for H we use the multiplicative notation. We can defined both $H^0(G, H)$ and $H^1(G, H)$. Indeed, we have $H^0(G, H) \cong \{a \in A \mid \alpha_g(a) = a \,\text{for all}\, g \in G\}$ and $H^1(G, H)$ is the defined as the set of 1-cocycles modulo an equivalence relation. So let us define what a 1-cocycle is.

Definition 2.6. A 1-*cocycle* is a map $\pi\colon G \to H$ such that, for every $x, y \in G$

$$\pi(xy) = \pi(x)\alpha_x(\pi(y)). \tag{2.1}$$

Let us introduce an equivalence relation between two 1-cocycles $\pi, \theta\colon G \to H$. We say that $\pi \sim \theta$ if there is an element $h \in H$ such that for every $x \in G$ we have $\theta(x) = h^{-1}\pi(x)\alpha_x(h)$. Clearly, $\sim$ is an equivalence relation. Therefore, $H^1(G, H) = \mathrm{Ker}\; d^2/\sim$, where $d^2\colon C^1(G, H) \to C^2(G, H)$ is defined for every $\pi \in C^1(G, H)$ as follows: $d^2(\pi)(xy) = \pi(xy)^{-1}\pi(x)\alpha_x(\pi(y))$, with $x, y \in G$.

A morphism between two 1-cocycles $\pi\colon G \to H$ and $\pi'\colon G' \to H'$ is a pair (f, g) where $f\colon G \to G'$ and $g\colon H \to H'$ are two group morphisms such that the following diagram

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[d, "f"'] & H \arrow[d, "g"] \\ G' \arrow[r, "\pi'"'] & H' \end{tikzcd}$$

commutes and $f(\alpha_x(h)) = \alpha'_{f(x)}(g(h))$, for every $x \in G$, $h \in H$.

Moreover, we say that $\pi\colon G \to H$ is a *bijective* 1-cocycle, if π is a bijection of sets and we denote with $\mathfrak{C}$ the full subcategory of bijective 1-cocycles with objects $\pi\colon G \to H$.

Lemma 2.7 ([3]). *Let H be a G-group, with $\alpha\colon G \to \mathrm{Aut}(H)$ the corresponding homomorphism. Let $\pi\colon G \to H$ be a 1-cocycle. Then*

1. $\pi(1) = 1$.

2. $\pi(g^{-1}) = \alpha_g^{-1}(\pi(g))^{-1}$ *for all $g \in G$.*

3. *If $g \in G$ can be written as $g = g_1^{\epsilon_1} \cdots g_k^{\epsilon_k}$ where each $\epsilon_i \in \{+1, -1\}$, then*
$$\pi(g) = \alpha_{x_1}(\pi(g_1))^{\epsilon_1} \cdot \alpha_{x_2}(\pi(g_2))^{\epsilon_2} \cdots \alpha_{x_k}(\pi(g_k))^{\epsilon_k}.$$
where $x_i = g_1^{\epsilon_1} \cdots g_{i-1}^{\epsilon_{i-1}}$ if $\epsilon_i = 1$ or $x_i = g_1^{\epsilon_1} \cdots g_i^{\epsilon_i}$ if $\epsilon_i = -1$.

Proof.

1. We have that $\pi(x) = \pi(1x) = \pi(1)\alpha_1(\pi(x)) = \pi(1)\pi(x)$, hence $\pi(1) = 1$.

2. It follows directly from $1 = \pi(g^{-1}g) = \pi(g^{-1}) \cdot \alpha_g^{-1}(\pi(g))$.

3. This is just a recursive application of the 1-cocycle condition where we apply part 2. if $\epsilon_i = -1$.

□

Proposition 2.8 ([3]). *There is a one-to-one correspondence between left skew braces and bijective 1-cocycles.*

Proof. Assume that we have a $(G, \circ)$-group $(H, \cdot)$ with the action of G on H given by $\alpha\colon G \to \mathrm{Aut}(H)$ and a bijective 1-cocycle $\pi\colon G \to H$. Define an operation on G as follow: $x * y := \pi^{-1}(\pi(x)\pi(y))$, where π^{-1} is the inverse of π. It is clear that $(G, *)$ is a group and that $1_{(G,*)} = 1_{(G,\circ)}$. Let us check the skew brace condition. Notice that

$$g \circ \pi^{-1}(h) = \pi^{-1}(\pi(g)\alpha_g(h)), \tag{2.2}$$

for every $g \in G$ and every $h \in H$, indeed, by the 1-cocycle condition, we have:

$$\pi^{-1}(\pi(g)\alpha_g(h)) = \pi^{-1}(\pi(g \circ \pi^{-1}(h))) = g \circ \pi^{-1}(h).$$

Moreover, by Lemma 2.7, $1 = \pi(1) = \pi(g * g^{-1}) = \pi(g)\pi(g^{-1})$, hence $\pi(g^{-1}) = \pi(g)^{-1}$, where g^{-1} is the inverse of g by $*$. Then, for every $a, b, c \in G$, we obtain

$$\begin{aligned} a \circ (b * c) &= a \circ \pi^{-1}(\pi(b)\pi(c)) \overset{(2.2)}{=} \pi^{-1}\big(\pi(a)\alpha_a(\pi(b)\pi(c))\big) \\ &= \pi^{-1}\big(\pi(a)\alpha_a(\pi(b))\pi(a)^{-1}\pi(a)\alpha_a(\pi(c))\big) \\ &= \pi^{-1}\big(\pi(a \circ b)\pi(a)^{-1}\pi(a \circ c)\big) \\ &= (a \circ b) * \pi^{-1}(\pi(a^{-1})\pi(a \circ c)) \\ &= (a \circ b) * \pi^{-1}\big(\pi(a^{-1}\pi(a \circ c))\big) \\ &= (a \circ b) * a^{-1} * (a \circ c). \end{aligned}$$

Hence the skew brace condition holds.

Conversely, if $(A, *, \circ)$ is a left skew brace, consider the action $\lambda\colon (A, \circ) \to \mathrm{Aut}(A, *)$ as in Lemma 1.6. Then the map $id\colon (B, \circ) \to (B, *)$ is a bijective 1-cocycle since $a \circ b = a * \lambda_a(b)$. This concludes the proof. □

Indeed, this correspondence is an equivalence of categories. We want to construct two functors

$$\mathsf{SKB} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \mathfrak{C}.$$

Define $\Phi(A, *, \circ) := \big(id_A\colon (A, \circ) \to (A, *)\big)$, where $(A, \circ)$ acts on $(A, *)$ trough λ, then id_A is a bijective 1-cocycle by the previous Proposition. Given $f \in \mathrm{Hom}_{\mathsf{SKB}}(A, B)$, we set $\Phi(f) := (f, f)$. The following diagram

$$\begin{tikzcd} (A, \circ) \arrow[r, "id_A"] \arrow[d, "f"'] & (A, *) \arrow[d, "f"] \\ (B, \circ) \arrow[r, "id_B"'] & (A, *) \end{tikzcd}$$

is commutative and $f(\lambda_{a_1}(a_2)) = f(a_1^{-1} * (a_1 \circ a_2)) = f(a_1)^{-1} * (f(a_1) \circ f(a_2)) = \lambda_{f(a_1)}(f(a_2))$, for every $a_1, a_2 \in A$. Clearly Φ preserves the identities and is compatible with compositions, hence it is a functor.

Conversely, let $\pi\colon (G, \circ) \to (H, \cdot)$ be a bijective 1-cocycle, with α the action of G on H. We saw in the previous Proposition that G is a skew brace with the "$*$" operation given by $x*y = \pi^{-1}(\pi(x)\pi(y))$. Then set $\Psi(\pi) := (G, *, \circ)$ and if $(f, g) \in \mathrm{Hom}_{\mathfrak{C}}(\pi_1, \pi_2)$, with $\pi_i\colon G_i \to H_i$, set $\Psi(f, g) := f$. Clearly for every $x, y \in G_1$, $f(x \circ y) = f(x) \circ f(y)$ since f is a group morphism and we have that $\pi_2(f(x*y)) = g(\pi_1(x*y)) = g(\pi_1(x)\pi_1(y)) = g(\pi_1(x))g(\pi_1(y))$ and $\pi_2(f(x) * f(y)) = \pi_2(f(x))\pi_2(f(y)) = g(\pi_1(x))g(\pi_1(y))$, then by the injectivity of π_2, f is a morphism of skew braces. Therefore also Ψ is a functor.

Proposition 2.9. SKB *and* $\mathfrak{C}$ *are two equivalent categories.*

Proof. We have just constructed the functors Φ, Ψ. It remains to construct two natural isomorphisms $\eta\colon \Phi\Psi \to id_{\mathfrak{C}}$ and $\xi\colon \Psi\Phi \to id_{\mathsf{SKB}}$.

For every $\pi \in \mathfrak{C}$, define η_π as (id_G, π). It turns out to be an isomorphism in $\mathfrak{C}$ and moreover η is a natural trasformation, because, given $(f, g) \in \mathrm{Hom}_{\mathfrak{C}}(\pi_1, \pi_2)$, with $\pi_i\colon G_i \to H_i$, by definition we have that $\Phi\Psi(\pi_1) = id_{G_1}$ and $\Phi\Psi(f, g) = (f, f)$ and the commutativity of the following diagram

$$\begin{tikzcd}
id_{G_1} \arrow[r, "{(id_{G_1},\pi_1)}"] \arrow[d, "{(f,f)}"'] & \pi_1 \arrow[d, "f"] \\
id_{G_2} \arrow[r, "{(id_{G_2},\pi_2)}"'] & \pi_2
\end{tikzcd}$$

follows from $(f, g)(id_{G_1}, \pi_1) = (f, g\pi_1) = (f, \pi_2 f) = (id_{G_2}, \pi_2)(f, f)$.

Finally, for ξ, it is enough to consider, for every $A \in \mathsf{SKB}$, the identity on A to get a natural isomorphism from $\Phi\Psi$ to id_{SKB}. □

Chapter 3

Commutators

Commutators are a prominant object of study in Categorical Algebra and Universal Algebra. In this chapter, we study the Huq commutator and the Smith commutor. We will show that they coincide for skew braces.

Let us recall some notions from Universal Algebra.

Definition 3.1. For A a nonempty set and n a nonnegative integer we define $A_0 = \{\emptyset\}$, and, for $n > 0$, A_n is the set of n-tuples of elements from A. An *n-ary operation* on A is any function f from A_n to A; n is the *arity* of f. A *finitary operation* is an n-ary operation, for some n. The image of $(a_1, ..., a_n)$ under an n-ary operation f is denoted by $f(a_1, ..., a_n)$. An operation f on A is called a *nullary operation* if its arity is zero; it is completely determined by the image $f(\emptyset)$ in A of the only element $\emptyset$ in A_0, and as such it is convenient to identify it with the element $f(\emptyset)$. Thus a nullary operation is thought of as an element of A. An operation f on A is unary, binary, or ternary if its arity is 1,2, or 3, respectively.

Definition 3.2. A *language of algebras* is a set $\mathcal{F}$ of function symbols such that a nonnegative integer n is assigned to each member f of $\mathcal{F}$. This integer is called the arity of f, and f is said to be an n-ary function symbol.

Definition 3.3. If $\mathcal{F}$ is a language of algebras then an *algebra* $\mathbf{A}$ *of type* $\mathcal{F}$ is an ordered pair $\langle A, F\rangle$ where A is a nonempty set and F is a family of finitary operations on A indexed by the language $\mathcal{F}$ such that corresponding to each n-ary function symbol f in $\mathcal{F}$ there is an n-ary operation $f^{\mathbf{A}}$ on A.

Given a class of algebraic structures of the same signature, we can define the notions of homomorphism, subalgebra, and product. G. Birkhoff proved that a class of algebraic structures of the same signature is a variety if and only if it is closed under the taking of homomorphic images, subalgebras and arbitrary products.

A left skew brace is an algebra $\langle A, *, \circ, ^{-1}, ', 1\rangle$, where $*$ and $\circ$ are binary, $^{-1}, '$ are unary and 1 is nullary, satysfing the following conditions:
(SB1): $\langle A, *, ^{-1}\rangle$ is a group;
(SB2): $\langle A, \circ, '\rangle$ is a group;
(SB3): $a \circ (b * c) \approx (a \circ b) * a^{-1} * (a \circ c)$.
Clearly, the class of all left skew braces is a variety.

Let $\mathbf{A}$ be an algebra. A *binary relation* on A is a subset r of A^2. If $(a, b) \in r$, we write arb.

Definition 3.4. Given an algebra $\mathbf{A}$, a binary relation r on A is an *equivalence relation* if, for any a, b, c from A, it satisfies:

1. ara;

2. arb implies bra;

3. arb and brc imply arc.

Definition 3.5. Let $\mathbf{A}$ be an algebra of type $\mathcal{F}$ and let θ an equivalence relation on A. Then θ is a congruence on A if θ satisfies the following compatibility property:
For each n-ary function symbol $f \in \mathcal{F}$ and elements $a_i, b_i \in A$, if $a_i \theta b_i$ holds for $1 \leq i \leq n$ then $f^{\mathbf{A}}(a_1, ..., a_n)\theta f^{\mathbf{A}}(b_1, ..., b_n)$ holds.

Given an algebra A, and a pair of conguences α, β of A, the composition of α and β is the subset of $A \times A$ defined as follows

$$\alpha \circ \beta := \{(a, b) \in A \times A \mid \exists\, c \in A : (a, c) \in \alpha,\ (c, b) \in \beta\}.$$

We say that α and β *permute* if $\alpha \circ \beta = \beta \circ \alpha$. An algebra A is called *congruence permutable* when each pair congruences of A permute. A variety of algebras $\mathcal{V}$ is referred to as congruence permutable when every algebra in $\mathcal{V}$ is congruence permutable.

In [28] it is proven that the following conditions are equivalent for a variety of algebras $\mathcal{V}$:
(a) $\mathcal{V}$ is congruence-permutable.
(b) There is a Mal'tsev term p,
where a *Mal'tsev term* is a function $p\colon X \times X \times X \to X$ such that $p(x, x, z) \approx z$ and $p(x, z, z) \approx x$, for every $x, z \in X$.

Congruence-permutable varieties are called *Mal'tsev varieties.* Any variety that contains a group operation is congruence-permutable, and the Mal'tsev term is $xy^{-1}z$. Hence the variety of left skew braces is a Mal'tsev variety.

3.1 Huq Commutator and Smith Commutator

What we call the Huq commutator is a category-theoretic concept introduced by Huq [23]. In the case of a semi-abelian variety $\mathcal{V}$ of universal algebras it can be defined as follows. Given X in $\mathcal{V}$ and normal subalgebras A and B of X, the Huq commutator $[A, B]_H$ is the smallest normal subalgebra C of X such that the canonical homomorphism $A \amalg B \to X/C$ factors through the canonical homomorphism $A \amalg B \to A \times B$, where $A \amalg B$ is the coproduct of A and B. Hence the existence of such factorization means that the canonical homomorphism $A \times B \to X/C$ is well defined.

The Smith commutator is a concept originally introduced by Smith [34] for congruences in a Mal'tsev variety. Together with its various generalizations, this notion is well known not only in universal algebra but also in category theory. For an algebra X in a Mal'tsev variety with Mal'tsev term $p(x, y, z)$ and two congruences α and β on X, the commutator $[\alpha, \beta]_S$ is the smallest congruence θ on X for which the function

$$p\colon \{(x, y, z) \mid (x, y) \in \alpha,\ (y, z) \in \beta\} \to X/\theta$$

sending (x, y, z) to the θ-class of $p(x, y, z)$ is an homomorphism. When X belongs to a semi-abelian variety $\mathcal{V}$, it is well known that there is a one-to-one correspondence between the normal subalgebras and the congruences on X. From a superficial glance, this may suggest that the congruence approach should give the same results everywhere as the ideal (normal subalgebra) approach, that is, for normal subalgebras A and B of X and their corresponding congruences α and β on X, the congruence corresponding to $[A, B]_H$ coincides with the Smith commutator $[\alpha, \beta]_S$. Well-known examples are the varieties of groups, Lie algebras, associative algebras and non-unital rings. However, this is not the case in general, indeed there are some examples of varieties such that the two commutators do not coincide, for example digroups, near-ring ([25]) and loops ([29]).

Definition 3.6. Let A be a left skew brace and I and J be two ideals of A. The Huq Commutator $[I, J]_H$ of I and J is the smallest ideal K of A such that the canonical homomorphism $\mu\colon I \times J \to A/K$, $\mu(i, j) = i * j * K$ is well-defined.

Proposition 3.7. *([7]) If I and J are two ideals of a left skew brace $(A, *, \circ)$, their Huq commutator $[I, J]_H$ is the ideal of A generated by the union of the following three sets:*

1. *the set $\{\, i' \circ j' \circ i \circ j \mid i \in I,\ j \in J \,\}$;*
2. *the set $\{\, i^{-1} * j^{-1} * i * j \mid i \in I,\ j \in J \,\}$;*
3. *the set $\{\, i^{-1} * j^{-1} * (j \circ i) \mid i \in I,\ j \in J \,\}$.*

Proof. Assume that the mapping $\mu\colon I \times J \to A/K$, $\mu(i, j) = i * j * K$ is a skew brace morphism for some ideal K of A. Then

$$\begin{aligned}(i \circ j) \circ K &= (i \circ K) \circ (j \circ K) = (i * K) \circ (j * K) = \\ &= \mu(i, 1) \circ \mu(1, j) = \mu((i, 1) \circ (1, j)) = \mu(i, j) = \mu((1, j) \circ (i, 1)) = \\ &= \mu((1, j) \circ \mu(i, 1)) = (j * K) \circ (i * K) = (j \circ K) \circ (i \circ K) = (j \circ i) \circ K.\end{aligned}$$

This proves that the set (1) is contained in K.

Similarly,

$$\begin{aligned}(i * j) * K &= (i * K) * (j * K) = \mu(i, 1) * \mu(1, j) = \mu((i, 1) * (1, j)) = \mu(i, j) = \\ &= \mu((1, j) * (i, 1)) = \mu((1, j) * \mu(i, 1)) = (j * K) * (i * K) = (j * i) * K.\end{aligned}$$

This proves that the set (2) is contained in K.

Also,

$$\begin{aligned}(i\circ j)*K &= (i\circ j)\circ K=(i\circ K)\circ(j\circ K)=(i*K)\circ(j*K)=\\ &=\mu(i,1)\circ\mu(1,j)=\mu((i,1)\circ(1,j))=\mu(i,j)=\mu((i,1)*(1,j))=\\ &=\mu(i,1)*\mu(1,j)=(i*K)*(j*K)=(i*j)*K.\end{aligned}$$

This proves that the set (3) is also contained in K.

Conversely, let K be the ideal of A generated by the union of the three sets. It is then very easy to check that the mapping $\mu\colon I\times J\to A/K$, $\mu(i,j)=i*j*K$ is a skew brace morphism. □

Definition 3.8. The Smith Commutator $[I,J]_S$ of I and J is the smallest ideal C of A for which the function

$$p\colon\{(x,y,z)\mid x*y^{-1}\in I\,and\,y*z^{-1}\in J\}\to A/C$$

defined by $p(x,y,z)=x*y^{-1}z*C$ is a well-defined homomorphism.

Proposition 3.9. *If I and J are two ideals of a left skew brace $(A,*,\circ)$, their Smith commutator $[I,J]_S$ is the ideal of A generated by the union of the following four sets:*

1. *the set $\{\,i^{-1}*j^{-1}*i*j\mid i\in I,\ j\in J\,\}$;*
2. *the set $\{((i*x)\circ j)*(i*(x\circ j))^{-1}\mid i\in I,j\in J,x\in A\}$;*
3. *the set $\{\,((j*x)\circ i)*x^{-1}*j^{-1}*x*(x\circ i)^{-1}\mid i\in I,j\in J,x\in A\,\}$;*
4. *the set $\{\,((i*j*x)\circ y)\circ((j*x)\circ y)^{-1}*(x\circ y)*((i*x)\circ y)^{-1}\mid i\in I,j\in J,x,y\in A\,\}$.*

Proof. We must determine when p is a left skew brace morphism, that is, preserves $*$ and $\circ$. It preserves $*$ if and only if $[I,J]_{(A,*)}\subseteq[I,J]_S$, that is, if and only if all elements of the form $i*j*i^{-1}*j^{-1}$ with $i\in I$ and $j\in J$ are in $[I,J]_S$. Moreover, p preserves $\circ$ if and only if $[I,J]_S$ contains all elements of the form

$$(x\circ a)*(y\circ b)^{-1}*(z\circ c)*((x*y^{-1}*z)\circ(a*b^{-1}*c))^{-1},\tag{3.1}$$

with $x * y^{-1}$ and $a * b^{-1}$ in I, and $y * z^{-1}$ and $b * c^{-1}$ in J. Let i, i_0, j, j_0 denote $x * y^{-1}, a * b^{-1}, y * z^{-1}$ and $b * c^{-1}$, respectively. Then (3.1) can be rewritten as

$$((i*j*z)\circ(i_0*j_0*c))*((j*z)\circ(j_0*c))^{-1}*(z\circ c)*((i*z)\circ(i_0*c))^{-1}. \quad (3.2)$$

Applying (1.1), we get

$$\begin{aligned}&((i * j * z) \circ i_0) * (i * j * z)^{-1} * ((i * j * z) \circ j_0) * (i * j * z)^{-1} *\\ &\quad *((i * j * z) \circ c) * (((j * z) \circ j_0) * (j * z)^{-1} * ((j * z) \circ c))^{-1} *\\ &\quad *(z \circ c) * (((i * z) \circ i_0) * (i * z)^{-1} * ((i * z) \circ c))^{-1} =\\ &\quad = ((i * j * z) \circ i_0) * z^{-1} * j^{-1} * i^{-1} * ((i * j * z) \circ j_0) * z^{-1} * j^{-1} * i^{-1} *\\ &\quad *((i * j * z) \circ c) * ((j * z) \circ c)^{-1} * (j * z) * ((j * z) \circ j_0)^{-1} *\\ &\quad *(z \circ c) * ((i * z) \circ c))^{-1} * (i * z) * ((i * z) \circ i_0)^{-1}.\end{aligned} \quad (3.3)$$

Now it suffices to show that given a congruence $\sim$ on A with $i * j \sim j * i$ for all $i \in I$ and $j \in J$, all elements in the three sets (2), (3) and (4) in the statement of the Proposition are congruent to 1 if and only if all elements of the form in (3.3) are congruent to 1.

"If": Notice that if

- $i_0 = j = c = 1$, (3.3) becomes $((i * z) \circ j_0) * (z \circ j_0)^{-1} * i$, hence (2);
- $i = j_0 = c = 1$, (3.3) becomes $((j * z) \circ i_0) * z^{-1} * j^{-1} * z * (z \circ i_0)$, hence (3);
- $i_0 = j_0 = 1$, (3.3) becomes $((i*j*z)*c)*((j*z)\circ c)^{-1}*(z\circ c)*((i*z)\circ c)^{-1}$, hence (4).

"Only if": Suppose that all elements in the three sets (2), (3) and (4) in the statement of the Proposition are congruent to 1, and suppose we have an element

$$\begin{aligned}&((i * j * z) \circ i_0) * z^{-1} * j^{-1} * i^{-1} * ((i * j * z) \circ j_0) * z^{-1} * j^{-1} * i^{-1} *\\ &\quad *((i * j * z) \circ c) * ((j * z) \circ c)^{-1} * (j * z) * ((j * z) \circ j_0)^{-1} *\\ &\quad *(z \circ c) * ((i * z) \circ c)^{-1} * (i * z) * ((i * z) \circ i_0)^{-1}\end{aligned} \quad (3.4)$$

of the form (3.3)).

Let us prove that $(z \circ c) * ((i * z) \circ c)^{-1}$ belongs to I. This is equivalent to proving that $z \circ c \circ ((i * z) \circ c)'$ belongs to I. But $z \circ c \circ ((i * z) \circ c)' =$

$z\circ c\circ c'\circ(i*z)' = z\circ(i*z)'$, and this belongs to I if and only if $z*(i*z)^{-1} = i^{-1}$ belong to I, which is trivially true.

Let us prove that $(j*z)*((j*z)\circ j_0)^{-1}$ belongs to J. This is equivalent to proving that $(j*z)\circ((j*z)\circ j_0)'$ belongs to I. But $(j*z)\circ((j*z)\circ j_0)' = (j*z)\circ j_0'\circ(j*z)'$, which belongs to J because $j_0 \in J$ and J is a normal subgroup of $(A,\circ)$.

Now elements of I and elements of J commute modulo $\sim$, so that the element (3.4) is

$$\begin{aligned}&\sim((i*j*z)\circ i_0)*z^{-1}*j^{-1}*i^{-1}*((i*j*z)\circ j_0)*z^{-1}*j^{-1}*i^{-1}*\\ &\quad *((i*j*z)\circ c)*((j*z)\circ c)^{-1}*(z\circ c)*((i*z)\circ c))^{-1}*\\ &\quad *(j*z)*((j*z)\circ j_0)^{-1}*(i*z)*((i*z)\circ i_0)^{-1}.\end{aligned}$$

In this formula, the second line is an element in the set (4) of the statement of the proposition, so that the element (3.4) is

$$\begin{aligned}&\sim((i*j*z)\circ i_0)*z^{-1}*j^{-1}*i^{-1}*((i*j*z)\circ j_0)*z^{-1}*j^{-1}*i^{-1}*\\ &\quad *(j*z)*((j*z)\circ j_0)^{-1}*(i*z)*((i*z)\circ i_0)^{-1}.\end{aligned}$$

Let us prove that $(i*z)*((i*z)\circ i_0)^{-1}$ belongs to I. This is equivalent to proving that $(i*z)\circ((i*z)\circ i_0)'$ belongs to I. But $(i*z)\circ((i*z)\circ i_0)' = (i*z)\circ i_0'\circ(i*z)'$, which belongs to I because $i_0 \in I$ and I is a normal subgroup of $(A,\circ)$.

Let us prove that $((i*j*z)\circ j_0)*z^{-1}*j^{-1}*i^{-1}$ belongs to J. Its inverse is $i*j*z*((i*j*z)\circ j_0)^{-1}$, and this belongs to J if and only if $i*j*z\circ((i*j*z)\circ j_0)' = (i*j*z)\circ j_0'\circ(i*j*z)'$, and this belongs to J because J is a normal subgroup of $(A,\circ)$.

Similarly $((j*z)\circ j_0)*z^{-1}*j^{-1}$ belongs to J. (Simply take $i=1$ in the previous paragraph.)

Thus the element $(i*z)*((i*z)\circ i_0)^{-1}$ of I and the element $((i*j*z)\circ j_0)*z^{-1}*j^{-1}*i^{-1}*((j*z)\circ j_0)*z^{-1}*j^{-1}$ of J commute modulo $\sim$, and we get that the element (3.4) is

$$\begin{aligned}&\sim((i*j*z)\circ i_0)*z^{-1}*j^{-1}*i^{-1}*(i*z)*((i*z)\circ i_0)^{-1}*\\ &\quad *(i*j*z)\circ j_0)*z^{-1}*j^{-1}*i^{-1}*(j*z)*((j*z)\circ j_0)^{-1}\\ &\sim((j*(i*z))\circ i_0)*z^{-1}*i^{-1}*j^{-1}*(i*z)*((i*z)\circ i_0)^{-1}*\\ &\quad *(i*(j*z))\circ j_0)*(j*z)^{-1}*i^{-1}*(j*z)*((j*z)\circ j_0)^{-1}.\end{aligned}$$

In this formula, the third line is an element in the set (3) of the statement of the proposition. Looking at the elements in the set (2) of the statement, we get that the element (3.4) is $\sim i * ((j * z)) \circ j_0) * (j * z)^{-1} * i^{-1} * (j * z) * ((j * z) \circ j_0)^{-1}$. Set $t := j * z$, getting $i * (t \circ j_0) * t^{-1} * i^{-1} * t * (t \circ j_0)^{-1}$. Now $t * (t \circ j_0)^{-1}$ is in J, because $t \circ J = J * t$, so $t \circ j_0 = j_1 * t$ for some $j_1 \in J$, so $(t \circ j_0) * t^{-1} = j_1$, hence $t * (t \circ j_0)^{-1} = j_1^{-1} \in J$. Therefore $t * (t \circ j_0)^{-1}$ and i^{-1} commute modulo $\sim$, so that the element (3.4) is ~ 1, as we wanted to prove. □

3.2 Huq=Smith

Theorem 3.10. *Let A be a left skew braces, I, J two ideals of A. Then $[I, J]_H = [I, J]_S$*

Proof. It suffices to prove that if $[I, J]_H = 0$, then $[I, J]_S = 0$. Hence, suppose we have a left skew brace $(A, *, \circ)$ for which $i*j = j*i$, $i \circ j = j \circ i$ and $i \circ j = i * j$ for all $i \in I$ and all $j \in J$. Consider the "corestriction" $\lambda|^J$ of the group morphism $\lambda\colon (A, \circ) \to \mathrm{Aut}(A, *)$ defined by $\lambda|^J\colon (A, \circ) \to \mathrm{Aut}(J, *)$, $\lambda|^J_a(j) = a^{-1} * (a \circ j)$ for $a \in A$ and $j \in J$. Then the condition $i \circ j = i * j$ for all $i \in I$ and all $j \in J$ can be re-written as $I \subseteq \ker \lambda|^J$.

In order to prove the theorem, it suffices to prove that the mapping $p\colon \{ (a, b, c) \mid a, b, c \in A,\ a \equiv b \pmod I,\ b \equiv c \pmod J \} \to A$ defined by $p(a, b, c) = a * b^{-1} * c$ is a left skew brace morphism. This is equivalent to proving that $a * b^{-1} * c = a \circ b' \circ c$ for every $a, b, c \in A$ with $a \equiv b \pmod I$ and $b \equiv c \pmod J$. equivalently, write a in the form $a = i * b$ and c in the form $b \circ j$. Then $[I, J]_S$ is zero if and only if $i * (b \circ j) = (i * b) \circ j$ for all $b \in A$, $i \in I$, $j \in J$. Multiplying by $(i * b)^{-1}$ on the left, one finds that $i * (b \circ j) = (i * b) \circ j$ can be rewritten as $\lambda_b(j) = \lambda_{i*b}(j)$, that is, $\lambda|^J$ maps the elements b and $i * b$ to the same element of $\mathrm{Aut}(J)$. In other words, λ is constant on the cosets $I * b = I \circ b$ of any $b \in A$. That is, I is contained in the kernel of $\lambda|^J\colon (A, \circ) \to \mathrm{Aut}(J, *)$, which we know to hold as we have seen in the previous paragraph. □

3.3 The Lattice of Ideals of a Left Skew Brace

Now that we have a good notion of commutator, we can consider the lattice $\mathcal{I}(A)$ of ideals of a left skew brace A. Clearly, $I \wedge J = I \cap J$ and $I \vee J = IJ$. It is a complete multiplicative lattice in the sense of [18], indeed the "commutator operation" $[-,-]\colon \mathcal{I}(A) \times \mathcal{I}(A) \to \mathcal{I}(A)$ is such that $[I, J] \subseteq I \cap J$. Moreover, the following proposition shows that $\mathcal{I}(A)$ is a commutative lattice.

Proposition 3.11. *For every pair of ideals I and J of a left skew brace A, $[I, J] = [J, I]$.*

Proof. It sufficies to prove the statement for a set of generators of $[I, J]$. It is well known that $[I, J]_{(A,\circ)} = [J, I]_{(A,\circ)}$ and that $[I, J]_{(A,*)} = [J, I]_{(A,*)}$. By Proposition 3.7, it remains to prove that if $i*j = i\circ j$, $i*j = j*i$, $i\circ j = j\circ i$ for every $i \in I$, $j \in J$, then $j * i = j \circ i$ for every $i \in I$, $j \in J$. But this is true since for every $i \in I$, $j \in J$ we have this chain of equalities $j * i = i * j = i \circ j = j \circ i$. □

Remark 3.12. The lattice $\mathcal{I}(A)$ satisfies the monotonicity condition, i.e. $I_1 \subseteq I_2$ and $J_1 \subseteq J_2$ imply $[I_1, J_1] \subseteq [I_2, J_2]$. Indeed $I_1 \subseteq I_2$ and $J_1 \subseteq J_2$ imply $[I_1, J_1]_{(A,\circ)} \subseteq [I_2, J_2]_{(A,\circ)}$ and $[I_1, J_1]_{(A,*)} \subseteq [I_2, J_2]_{(A,*)}$. Moreover the set $\{i^{-1} * j^{-1} * (j \circ i) \mid i \in I_1,\ j \in J_1\}$ is contained in the set $\{i^{-1} * j^{-1} * (j \circ i) \mid i \in I_2,\ j \in J_2\}$.

Definition 3.13. An ideal P of A is a *prime ideal* if $P \neq A$ and

$$[I, J] \subseteq P \implies (I \subseteq P \quad \textit{or} \quad J \subseteq P)$$

for every $I, J \in \mathcal{I}(A)$.

The set $\mathsf{Spec}(\mathcal{I}(A))$ of all prime ideals of A is the *Zariski spectrum* of $\mathcal{I}(A)$.

Let I be an element of $\mathcal{I}(A)$. The *lower descending series* of I is the descending series

$$I =: I^1 \supseteq I^2 \supseteq I^3 \supseteq \cdots$$

where $I^{n+1} := [I^n, I]$ for every $n \geq 0$. If $I^n = 1$ for some $n \geq 1$, then I is *nilpotent*. The element I is *idempotent* if $I^2 = [I, I] = 1$.

The *derived series* of I is the descending series

$$I =: I^{(0)} \supseteq I^{(1)} \supseteq I^{(2)} \supseteq \cdots$$

where $I^{(n+1)} := [I^{(n)}, I^{(n)}]$ for every $n \geq 0$. The term $I' := I^2 = [I, I] = I^{(1)}$ is called the *derived ideal* of I. The ideal I is *solvable* if $I^{(n)} = 1$ for some $n \geq 0$.

Definition 3.14. An ideal I of a left skew brace A is *meet-irreducible* if $I = J \cap Z$ implies $I = J$ or $I = Z$ for every $J, Z \in \mathcal{I}(A)$.

Definition 3.15. An ideal $S \in \mathcal{I}(A)$ is *semiprime* if $I^2 \subseteq S$ implies $I \subseteq S$ for every $I \in \mathcal{I}(A)$.

Proposition 3.16. *If I, J, K are ideals of a left skew brace A, then*

$$[I, J * K] = [I, J] * [I, K].$$

Proof. From $J * K \supseteq J, K$, it follows that $[I, J * K] \supseteq [I, J], [I, K]$. It follows that $[I, J * K] \supseteq [I, J] * [I, K] = [I, J] \circ [I, K]$. Now it is known that the equality $[I, JK] = [I, J][I, K]$ holds for normal subgroups I, J, K of a group G. Hence, to conclude the proof, it suffices to prove that if $(A, *, \circ)$ is a left skew brace such that $i * j = j * i = j \circ i = i \circ j$, $i * k = k * i = k \circ i = i \circ k$ for every $i \in I$, $j \in J$ and $k \in K$, then $i * (j \circ k) = i \circ (j \circ k)$ for every i, j, k. Now $i * j = i \circ j$ for every i and j can be restated saying that J is contained in the kernel of the group morphism $\lambda|^I \colon (A, \circ) \to \mathrm{Aut}(I, *)$. Similarly, K is contained in the kernel of that group morphism. Therefore $J \circ K$ is contained in that kernel, that is $i * x = i \circ x$ for every $x \in J \circ K = J * K$, as desired. □

In the languange of multiplicative lattice, the previuos proposition showed that $\mathcal{I}(A)$ is *m-distributive.*

Proposition 3.17. *Any ideal P is prime if and only if is meet-irreducible and semiprime.*

Proof. Clearly, prime ideals are semiprime. Suppose $P = I \cap J$ for some $I, J \in \mathcal{I}$. Then $[I, J] \subseteq I \cap J = P$ implies $I \subseteq P$ or $J \subseteq P$. But $P = I \cap J$ implies $P \subseteq I$ and $P \subseteq J$. Therefore either $P = I$ or $P = J$.

Conversely, assume that P is a meet-irreducible and semiprime ideal. Let $I, J \in \mathcal{I}(A)$ be two ideals such that $I \nsubseteq P$ and $J \nsubseteq P$. We need to show that $[I, J] \nsubseteq P$. Now $IP \supset P$ and $JP \supset P$. Since P is meet-irreducible, $IP \cap JP \supsetneq P$. As P is semiprime, it follows that $(IP \cap JP)^2 \nsubseteq P$. But $(IP \cap JP)^2 = [(IP \cap JP), (IP \cap JP)] \subseteq [IP, JP] = [I, J][I, P][P, J][P, P]$. It follows that $[I, J] \nsubseteq P$. □

Theorem 3.18. *Let A be a left skew brace.* $\mathsf{Spec}(\mathcal{I}(A)) = \mathcal{I}(A) \setminus \{A\}$ *if and only if $\mathcal{I}(A)$ is linearly ordered and every ideal in $\mathcal{I}(A)$ is idempotent.*

Proof. Suppose $\mathsf{Spec}(\mathcal{I}(A)) = \mathcal{I}(A) \setminus \{A\}$. If $\mathcal{I}(A)$ is not linearly ordered, there exist I, J ideals of A such that $I \nsubseteq J$ and $J \nsubseteq I$. Then I and J are two ideals of A such that $I \supset I \cap J$ and $J \supset I \cap J$. This shows that $I \cap J$ is not meet-irreducible, hence is not prime by Proposition 3.17. So we get a contradiction.

Now let I a not idempotent ideal of A. Then $I^2 \subset I$, so I^2 is not semiprime. In particular I^2 is not prime, another contraction.

Conversely, assume $\mathcal{I}(A)$ linearly ordered and that every ideal is idempotent. Let P be any ideal of A, $P \neq A$. In order to show that P is prime, suppose $I, J \in \mathcal{I}(A)$, $I \nsubseteq P$ and $J \nsubseteq P$. Then $I \supset P$ and $J \supset P$. As $\mathcal{I}(A)$ is linearly ordered, it follows that $I \cap J \supset P$. By Remark 3.12, it follows that $[I, J] \supseteq [I \cap J, I \cap J] = I \cap J \supset P$. This proves that P is prime. □

Definition 3.19. An ideal M of a left skew brace A is said to be *maximal* if $M \neq A$ and $M \subset I$ implies $I = A$.

Clearly, maximal ideals are prime.

Proposition 3.20. *Every left skew brace has a maximal ideal.*

Proof. By Proposition 1.19, the Zorn's Lemma applied to the set of all proper ideals of A implies the thesis. □

Following again [18], we can define what the centralizer of an ideal is. Indeed, let I be an ideal of a left skew brace A. The *left annihilator* $\mathrm{l.ann}_A(I)$ of I is $\prod_{[J,I]=1} J$ and similarly the *right annihilator* $\mathrm{r.ann}_A(I)$ of I is $\prod_{[I,J]=1} J$.

By Lemma 3.11, $\mathrm{l.ann}_A(I) = \mathrm{r.ann}_A(I) =: C_A(I)$ and we call it the *centralizer* of I. Moreover, the *center* of A is exactly the centralizer $C_A(A)$ of A.

Chapter 4

The free skew brace

The aim of this chapter is to build the free skew brace over a set X. This chapter is based on the work of J. Orza [30]. Let us recall the definition of a free object for a concrete category.

Let $\mathcal{C}$ be a concrete category with a faithfull functor $U\colon \mathcal{C} \to \mathsf{Set}$.

Definition 4.1. Let X be a set. A *free object* over X is a pair (F, i) where $F \in \operatorname{Ob}(\mathcal{C})$ and $i\colon X \to U(F)$ is an injection such that they satifies the following universal property: for any pair (A, f) with A an object in $\mathcal{C}$ and $f\colon X \to U(A)$, there exists a unique morphism $\tilde{f}\colon F \to A$ in $\mathcal{C}$ such that the following diagram commutes

$$\begin{tikzcd}
X \arrow[rr, "f"] \arrow[dr, hook, "i"'] & & U(A) \\
& U(F) \arrow[ur, dashed, "\tilde{f}"'] &
\end{tikzcd}$$

Whenever $\mathcal{C}$ is a variety, the free object exists for every set X.

First of all we need another characterization of skew braces.

4.1 Initial Construction

Proposition 4.2. *A group $(A, \circ)$, endowed with a pair (ρ, δ) of anti-homomorphisms of groups, with $\rho, \delta\colon (A, \circ) \to \operatorname{Sym}(A)$, is a skew brace if and only if*

$$a \circ \rho_a(b) = b \circ \delta_b(a), \tag{4.1}$$

for every $a, b \in A$.

Proof. We prove that having such ρ, δ as in the statement, is equivalent to having a homomorphism of groups $\alpha \colon A \to \mathrm{Sym}(A)$ and an anti homorphism of groups $\beta \colon A \to \mathrm{Sym}(A)$ such that $a \circ b = \alpha_a(b) \circ \beta_b(a)$ as in Theorem 5.10, hence we get a bijective 1-cocycle anche hence by Proposition 2.8 a left skew brace. We have that $a \circ b = \alpha_a(b) \circ \beta_b(a)$ holds if and only if $a' \circ \alpha_a(b) = b \circ (\beta_b(a))'$, if and only if $a \circ \alpha_{a'}(b) = b \circ (\beta_b(a'))'$. And we can conclude noticing that if G is any group and $F \colon G \to \mathrm{Sym}(G)$, $g \mapsto F_g$, is a homomorphism (resp. anti-homomorphism) of groups, then the map $F' \colon g \mapsto F_{g^{-1}}$ is an anti homomorphism (resp. homomorphism) of groups, and the map $F'' \colon g \mapsto F''_g$ with $F''_g(x) = F_g(x^{-1})^{-1}$ is still a homomorphism of groups. □

Notice that the name ρ is not accidental, indeed for a skew brace $(A, *, \circ)$, we always have $a * b = a \circ \rho_a(b) = b \circ (b' \circ (a * b)) =: b \circ \delta_b(a)$, where ρ is the inverse of λ (see Proposition 1.6).

Let us recall some facts about the free group over a set. Let X be a set and let $X^{-1} = \{x^{-1} \mid x \in X\}$ a copy of X. Let $Z = X \sqcup X^{-1}$. Consider M the monoid generated by S and identify every word that contains pairs of the type xx^{-1}. We obtain then a group $F(X)$ that is the *free group* over X. So a generic element of $F(X)$ is of the form $z_1 \cdots z_n$ with $z_i \in Z$.

So let X be a set. We start defining recursively a set Z in the following way. First we set:

$$Y_1 = X \sqcup X^{-1}$$

where $X^{-1} = \{x^{-1} \mid x \in X\}$ is a disjoint copy of elements of X. Next we define the following sets:

$$\begin{gathered} X_n := \{\rho_a(b) \mid a, b \in Y_{n-1},\, b \neq \rho_{a^{-1}}(c) \,\text{for any}\, c \in Y_{n-1}, \} \\ Y_n := \{\delta_a(b) \mid a, b \in Y_{n-1},\, b \neq \delta_{a^{-1}}(c) \,\text{for any}\, c \in Y_{n-1}, \} \\ Z_n := Z_{n-1} \sqcup (X_n \sqcup Y_n) \sqcup (X_n \sqcup Y_n)^{-1}, \end{gathered}$$

where $\rho_a(b)$ and $\delta_a(b)$ are formal elements. Then we set $Z := \bigcup_{n \geq 1} Z_n$ and we denote with $(G, \cdot)$ the free group $F(Z)$ over Z.

Our aim is to define two anti-homomorphisms from $(G, \cdot)$ to $\mathrm{Sym}(G)$. In order to do that, first we define two maps $\rho, \delta \colon Z \to \mathrm{Sym}(Z)$ as follows: let $a, b \in Z$, set

$$\rho_a(b) = \begin{cases} \rho_a(b) & \text{if}\, b \neq \rho_{a^{-1}}(c), \\ c & \text{if}\, b = \rho_{a^{-1}}(c), \end{cases} \qquad \delta_a(b) = \begin{cases} \delta_a(b) & \text{if}\, b \neq \delta_{a^{-1}}(c), \\ c & \text{if}\, b = \delta_{a^{-1}}(c). \end{cases}$$

Now we extend these maps from Z to $\mathrm{Sym}(G)$. Recall that a generic element of G is of the form $z_1 \cdots z_n$ for $z_i \in Z$. So define recursively:

$$\begin{aligned} \rho_z(z_1 \cdots z_n) &:= \rho_z(z_1)\rho_{\delta_{z_1}(z)}(z_2 \cdots z_n); \\ \delta_z(z_1 \cdots z_n) &:= \delta_z(z_1)\delta_{\rho_{z_1}(z)}(z_2 \cdots z_n); \end{aligned}$$

with $z, z_1, \cdots z_n \in Z$ and hence we extend them from G to $\mathrm{Sym}(G)$ in such a way to have an anti homomorphism of groups, namely

$$\begin{aligned} \rho_{z_1 \cdots z_n}(g) &:= \rho_{z_n}\rho_{z_{n-1}} \cdots \rho_{z_1}(g), \\ \delta_{z_1 \cdots z_n}(g) &:= \delta_{z_n}\delta_{z_{n-1}} \cdots \delta_{z_1}(g), \end{aligned}$$

for every $g \in G, z_1 \cdots z_n \in Z$.

Lemma 4.3. *For every $a, b, c \in G$, we have*

$$\begin{aligned} \rho_a(bc) &= \rho_a(b)\rho_{\delta_b(a)}(c), \\ \delta_a(bc) &= \delta_a(b)\delta_{\rho_b(a)}(c). \end{aligned}$$

Proof. We divide the proof into three steps.

1. $\rho_z(ab) = \rho_z(a)\rho_{\delta_a(z)}(b)$; $\delta_z(ab) = \delta_z(a)\delta_{\rho_a(z)}(b)$, for every $a, b \in G, z \in Z$.

   We proceed by induction on the length of a. If $a \in Z$ we have nothing to prove. So suppose $a = z_1 \cdots z_n$, with $z_i \in Z$. We have:

$$\begin{aligned} \rho_z(ab) &= \rho_z\big((z_1 \cdots z_n)b\big) = \rho_z(z_1)\rho_{\delta_{z_1}(z)}(z_2 \cdots z_n b) \\ &\overset{\text{ind.}}{=} \rho_z(z_1)\rho_{\delta_{z_1}(z)}(z_2 \cdots z_n)\rho_{\delta_{z_2 \cdots z_n}\delta_{z_1}(z)}(b) \\ &= \rho_z(z_1 \cdots z_n)\rho_{\delta_{z_1 \cdots z_n}(z)}(b) \\ &= \rho_z(a)\rho_{\delta_a(z)}(b). \end{aligned}$$

   And similarly for δ.

2. $\rho_a(zc) = \rho_a(z)\rho_{\delta_z(a)}(c)$; $\delta_a(zc) = \delta_a(c)\delta_{\rho_z(a)}(c)$, for every $a, c \in G$ and $z \in Z$.

   We proceed by induction on the lenght of a. If $a \in Z$, it is nothing but how we extended ρ and δ. Suppose then that $a = z_1 \cdots z_n$, with $z_i \in Z$. We have:

$$\begin{aligned}\rho_a(zc) = \rho_{z_1\cdots z_n}(zc) = \rho_{z_n}\rho_{z_1\cdots z_{n-1}}(zc) &\overset{\text{ind.}}{=} \rho_{z_n}\big(\rho_{z_1\cdots z_{n-1}}(z)\rho_{\delta_z(z_1\cdots z_{n-1})}(c)\big)\\ &\overset{1.}{=} \rho_{z_n}\rho_{z_1\cdots z_{n-1}}(z)\rho_{\delta_{\rho_{z_1\cdots z_{n-1}}(z)}(z_n)}\rho_{\delta_z(z_1\cdots z_{n-1})}(c)\\ &\overset{1.}{=} \rho_{z_1\cdots z_n}\rho_{\delta_z(z_1\cdots z_{n-1})\delta_{\rho_{z_1\cdots z_{n-1}}(z)}(z_n)}(c)\\ &= \rho_a(z)\rho_{\delta_z(a)}(c).\end{aligned}$$

   And similarly for δ.

3. $\rho_a(bc) = \rho_a(b)\rho_{\delta_b(a)}(c)$; $\delta_a(bc) = \delta_a(b)\delta_{\rho_b(a)}(c)$, for every $a, b, c \in G$.

   We proceed by induction on the length of b. If $b \in Z$, it is precisely 2., so suppose as usual $b = z_1 \cdots z_n$, with $z_i \in Z$. We have:

$$\begin{aligned}\rho_a\big((z_1 \cdots z_n)c\big) &\overset{2.}{=} \rho_a(z_1)\rho_{\delta_{z_1}(a)}(z_2 \cdots z_n c)\\ &\overset{\text{ind.}}{=} \rho_a(z_1)\rho_{\delta_{z_1}(a)}(z_2 \cdots z_n)\rho_{\delta_{z_2\cdots z_n}\delta_{z_1}(a)}(c)\\ &= \rho_a(b)\rho_{\delta_b(a)}(c).\end{aligned}$$

   And similarly for δ.

□

Lemma 4.4. *Let A be a group and let $\rho, \delta \colon A \to \mathrm{Sym}(A)$ be two anti-homomorphisms of groups such that for every $a, b, c \in A$*

$$\rho_a(bc) = \rho_a(b)\rho_{\delta_b(a)}(c), \quad \delta_a(bc) = \delta_a(b)\delta_{\rho_b(a)}(c).$$

Let X be a set of generators of A as a monoid. If $x\rho_x(y) = y\delta_y(x)$ for very $x, y \in X$, then $a\rho_a(b) = b\delta_b(a)$ for every $a, b \in A$.

Proof. As before, we divides the proof into two steps.

1. $x\rho_x(a) = a\delta_a(x)$; $a\rho_a(x) = x\delta_x(a)$, for every $x \in X, a \in A$.

We proceed by induction on the length of a. If $a \in Z$, it is precisely the hyphotesis. Suppose that $a = z_1 \cdots z_n$, with $z_i \in Z$. Then:

$$\begin{aligned} x\rho_x(z_1 \cdots z_n) &= x\rho_x(z_1)\rho_{\delta_{z_1}(x)}(z_2 \cdots z_n) \\ &= z_1\delta_{z_1}(x)\rho_{\delta_{z_1}(x)}(z_2 \cdots z_n) \\ &= a\delta_{z_2 \cdots z_n}\delta_{z_1}(x) = a\delta_a(x). \end{aligned}$$

The other equality can be deduced using the same calculation, exchanging the role of ρ and δ.

2. $a\rho_a(b) = b\delta_b(a)$, for every $a, b \in A$.

   We proceed by induction on the length of b. If $b \in Z$, we have proved it in the previous step. Suppose that $b = z_1 \cdots z_n$, with $z_i \in Z$. Then:

$$\begin{aligned} a\rho_a(z_1 \cdots z_n) &= a\rho_a(z_1)\rho_{\delta_z(a)}(z_2 \cdots z_n) \\ &= z_1\delta_{z_1}(a)\rho_{\delta_{z_1}(a)}(z_2 \cdots z_n) \\ &= b\delta_{z_2 \cdots z_n}\delta_{z_1}(a) = b\delta_b(a). \end{aligned}$$

□

It is not necessarly true that with our definition of ρ and δ on G, we have that $a\rho_a(b) = b\delta_b(a)$. So let $\sim$ be the minimal equivalence relation on A such that $x\rho_x(y) \sim y\delta_y(x)$ and such that if $a \sim b$ and $c \sim d$, then $ac \sim bd, \rho_a(c) \sim \rho_b(d)$ and $\delta_a(c) \sim \delta_b(d)$.

Proposition 4.5. *The quotient group $({}^{G}/_{\sim}, \cdot, \rho, \delta)$ is a left skew brace.*

Proof. We want to apply Proposition 4.2. By construction, ρ, δ are well-defined anti-homomorphisms of groups from ${}^{G}/_{\sim}$ to $\mathrm{Sym}({}^{G}/_{\sim})$. By Lemma 4.3, ρ, δ satisfy the hypothesis of Lemma 4.4, so we have that for every $a, b \in A$, $a\rho_a(b) = b\delta_b(a)$. So the claim follows by Proposition 4.2. □

4.2 The Free Skew Brace

Before concluding, we need a result about skew brace morphism. Recall that have a skew brace $(A, *, \circ)$ is equivalent to have a group $(A, \circ)$ with two anti-homomorphism of groups from A to $\mathrm{Sym}(A)$.

Lemma 4.6. *Let $(A_1, \circ, \rho^1, \delta^1), (A_2, \circ, \rho^2, \delta^2)$ be two left skew braces and let $f\colon (A_1, \circ), \to (A_2, \circ)$ be a group morphism. Then f is a skew brace morphism if and only if $f(\rho^1_a(b)) = \rho^2_{f(a)}(f(b))$, for every $a, b \in A_1$ if and only if $f(\delta^1_a(b)) = \delta^2_{f(a)}(f(b))$, for every $a, b \in A_1$.*

Proof. Suppose that $f\colon A_1 \to A_2$ is a skew brace morphism. Then, for every $a, b \in A_1$ we have $f(\rho^1_a(b)) = f(a' \circ (a * b)) = f(a)' \circ (f(a) * f(b)) = \rho^2_{f(a)}(f(b))$. Conversely, if $f(\rho^1_a(b)) = \rho^2_{f(a)}(b)$, for every $a, b \in A_1$, then, by definition of $*$, $f(a * b) = f(a \circ \rho^1_a(b)) = f(a) \circ f(\rho^1_a(b)) = f(a) \circ \rho^2_{f(a)}(b) = f(a) * f(b)$. And similarly for the other implication. □

Theorem 4.7. *Let X be a set. With the constructions of $G, \rho, \delta, \sim$ defined above, we have that $({}^{G}/_{\sim}, \cdot, \rho, \delta)$ is the free skew brace over X.*

Proof. Let $f\colon X \to A$ be a map, with $(A, \circ, \mu, \gamma)$ a skew brace. By Lemma 4.6, it sufficies to extend f to a group morphism $\tilde{f}\colon (G, \cdot) \to (A, \circ)$ such that it satisfies $\tilde{f}(\rho_h(g)) = \mu_{\tilde{f}(h)}(\tilde{f}(g))$, for every $g, h \in G$.

First we extend f to Z as follows:

- We extend f to Z_1: $\tilde{f}(x^{-1}) := f(x)'$, for every $x^{-1} \in X^{-1}$;

- Assuming that we have defined $\tilde{f}$ on Z_{n-1}. A generic element in Z_{n-1} is of the form $\rho_x(y)$ or $\delta_x(y)$ with $x, y \in Z_{n-1}$, so we define $\tilde{f}(\rho_x(y)) := \mu_{\tilde{f}(x)}(\tilde{f}(y))$ and $\tilde{f}(\delta_x(y)) := \gamma_{\tilde{f}(x)}(\tilde{f}(y))$.

Then we extend f to G by defining $\tilde{f}(z_1 \cdots z_n) := \tilde{f}(z_1) \cdots \tilde{f}(z_n)$, for every $z_1, \cdots, z_n \in Z$.

By construction, $\tilde{f}$ is group morphism. We have to prove that $\tilde{f}(\rho_h(g)) = \mu_{\tilde{f}(h)}(\tilde{f}(g))$. Let us proceed by steps:

- First we prove that $\tilde{f}(\rho_{z_1 \cdots z_n}(z)) = \mu_{\tilde{f}(z_1 \cdots z_n)}(\tilde{f}(z))$ for every $z_1, \cdots, z_n, z \in Z$. By induction on n we have that:

$$\begin{aligned}\tilde{f}(\rho_{z_1 \cdots z_n}(z)) &= \tilde{f}\big(\rho_{z_n}(\rho_{z_1 \cdots z_{n-1}}(z))\big) = \mu_{\tilde{f}(z_n)}\big(\tilde{f}(\rho_{z_1 \cdots z_{n-1}}(z))\big) \\ &= \mu_{\tilde{f}(z_n)} \mu_{\tilde{f}(z_1 \cdots z_{n-1})}(\tilde{f}(z)) = \mu_{\tilde{f}(z_1 \cdots z_n)}(\tilde{f}(z))\end{aligned}$$

And similarly $\tilde{f}(\delta_h(z)) = \gamma_{\tilde{f}(h)}(\tilde{f}(z))$, for every $h \in G, z \in Z$.

- Now we prove that $\tilde{f}(\rho_h(g)) = \mu_{\tilde{f}(h)}(\tilde{f}(g))$ and $\tilde{f}(\delta_h(g)) = \gamma_{\tilde{f}(h)}(\tilde{f}(g))$

for every $g, h \in G$. Suppose $g = z_1 \cdots z_n$, by induction on n, we have

$$\begin{aligned}\tilde{f}(\rho_h(z_1 \cdots z_n)) &= \tilde{f}(\rho_h(g')\rho_{\delta_{z_1 \cdots z_{n-1}}(h)}(z_n)) \\ &= \tilde{f}(\rho_h(z_1 \cdots z_{n-1}))\tilde{f}(\rho_{\delta_{z_1 \cdots z_{n-1}}(h)}(z_n)) \\ &= \mu_{\tilde{f}(h)}(\tilde{f}(z_1 \cdots z_{n-1}))\mu_{\tilde{f}(\delta_{z_1 \cdots z_{n-1}}(h))}(f(z_n)) \\ &= \mu_{\tilde{f}(h)}(\tilde{f}(z_1 \cdots z_{n-1}))\mu_{\gamma_{\tilde{f}(h)}(\tilde{f}(z_1 \cdots z_{n-1}))}(f(z_n)) \\ &= \mu_{\tilde{f}(h)}(\tilde{f}(g)).\end{aligned}$$

Finally we extend $\tilde{f}$ to ${}^{G}/_{\sim}$ in the natural way and $\tilde{f}\colon {}^{G}/_{\sim} \to A$ is a well-defined map since A, being a skew brace, satisfies (4.1). Moreover, by construction, $\tilde{f}\colon {}^{G}/_{\sim} \to A$ is a skew brace morphism and it is the unique one such that $f = \tilde{f}i$, with $i\colon X \to {}^{G}/_{\sim}$ the canonical inclusion. □

Chapter 5

The Yang-Baxter Equation

In this chapter we study the main properties of the Yang-Baxter equation, in order to show their connection with skew braces.

5.1 Set-theoretical Solutions of the Yang-Baxter Equation

Definition 5.1. A *set-theoretic solution of the Yang-Baxter equation* is a pair (X, r), where X is a set and

$$r\colon X \times X \to X \times X, \qquad r(x,y) = (f_x(y), g_y(x))$$

is a map such that

$$r_{12}r_{23}r_{12} = r_{23}r_{12}r_{23}, \tag{5.1}$$

where $r_{12} = r \times id$ and $r_{23} = id \times r$.

The behaviour of the Yang-Baxter equation can be described by the following picture:

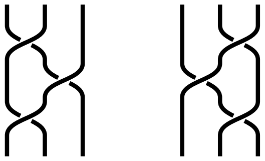

Figure 5.1: The Yang–Baxter equation.

The conditions (5.1) can be written more explicitely as follows:

$$\begin{aligned} r_{12}r_{23}r_{12}(x,y,z) &= r_{12}r_{23}(f_x(y),g_y(x),z)\\ &= r_{12}(f_x(y),f_{g_y(x)}(z),g_zg_y(x))\\ &= (f_{f_x(y)}f_{g_y(x)}(z),g_{f_{g_y(x)}(z)}f_x(y),g_zg_y(x)), \end{aligned}$$

$$\begin{aligned} r_{23}r_{12}r_{23}(x,y,z) &= r_{23}r_{12}(x,f_y(z),g_z(y))\\ &= r_{23}(f_xf_y(z),g_{f_y(z)}(x),g_z(y))\\ &= (f_xf_y(z),f_{g_{f_y(z)}(x)}g_z(y),g_{g_z(y)}g_{f_y(z)}(x)). \end{aligned}$$

Then (X,r) is a solution if and only if f and g are such that

$$f_{f_x(y)}f_{g_y(x)}(z) = f_xf_y(z) \tag{5.2}$$

$$g_{f_{g_y(x)}(z)}f_x(y) = f_{g_{f_y(z)}(x)}g_z(y) \tag{5.3}$$

$$g_zg_y(x) = g_{g_z(y)}g_{f_y(z)}(x), \tag{5.4}$$

for any $x,y,z \in X$.

Examples 5.2. Let X be a set and $r\colon X\times X \to X\times X$ be defined by $r(x,y)=(f(y),g(x))$. By (5.3), r is a solution if and only if $g\circ f = f\circ g$.

In such a case, r is called the *permutation solution.*

Definition 5.3. A set-theoretical solution of the YBE (X,r) is called:

- *left non-degenerate* if the maps f_x are bijective for every $x\in X$;
- *right non-degenerate* if the maps g_x are bijective for every $x\in X$;
- *non-degenerate* if it is both left and right non-degenerate;
- *involutive* if $r^2 = id$;
- *bijective* if r is bijective.

Examples 5.4. Let X be a set. $r(x,y)=(y,x)$ is an involutive non-degenerate solution.

Examples 5.5. Let G be a group.

1. (G,r_1) with $r_1(x,y)=(y,y^{-1}xy)$ is a bijective non-degenerate solution of the YBE;

2. (G, r_2) with $r_2(x,y) = (x^2y, y^{-1}x^{-1}y)$ is a non-degenerate solution of the YBE.

Examples 5.6. Let $r(x,y) = (f(y), g(x))$ be the permutation solution. Then r is bijective if and only if $f, g \in \mathrm{Sym}(X)$, and in this case r is also non-degenerate. Indeed, an inverse of r is $s(x,y) = (g^{-1}(y), f^{-1}(x))$.

Moreover r is involutive if and only if $fg = id_X$.

Proposition 5.7. *Let X be a set and $\triangle\colon X \times X \to X$ a binary operation on X. The map $r\colon X \times X \to X \times X$, defined by $r(x,y) = (y, y\triangle x)$ is a set-theoretical solution of the Yang-Baxter equation if and only if $\triangle$ is self distributive, i.e. for every $x, y, z \in X$, $x\triangle(y\triangle z) = (x\triangle y)\triangle(x\triangle z)$.*

Proof. Call $f_x(y) = f(y) = y$ and $g_x(y) = x\triangle y$. Conditions (5.2) and (5.3) are trivial. Condition (5.4) is equivalent to saying that $z\triangle(y\triangle x) = (z\triangle y)\triangle(z\triangle x)$.

□

5.2 Braiding Operators

We want to consider now the case when X is a group and try to compare some known notions to the set of solutions of the Yang-Baxter equations.

Theorem 5.8. *([27]) Let G be a group and $\alpha, \beta\colon G \to \mathrm{Sym}(G)$ respectivetely a homomorphism and an antihomomorphism of groups such that they satisfy the compatibility condition*

$$uv = \alpha_u(v)\beta_v(u), \tag{5.5}$$

for every $u, v \in G$. Then

$$r(u,v) = (\alpha_u(v), \beta_v(u))$$

is invertible and is a solution of the Yang-Baxter equation on the set G.

Proof. We verify the relation (5.1). By previous computations we have that

$$r_{12}r_{23}r_{12}(u,v) = \big(\alpha_{\alpha_u(v)}(\alpha_{\beta_v(u)}(w)), \beta_{\alpha_{\beta_v(u)}(w)}(\alpha_u(v)), \beta_w(\beta_v(u))\big);$$

and

$$r_{23}r_{12}r_{23}(u,v,w) = \big(\alpha_u(\alpha_v(w)), \alpha_{\beta_{\alpha_v(w)}(u)}(\beta_w(v)), \beta_{\beta_w(v)}(\beta_{\alpha_v(w)}(u))\big).$$

Denote

$$r_{12}r_{23}r_{12}(u,v) =: (u_1,v_1,w_1), \qquad r_{23}r_{12}r_{23}(u,v) =: (u_2,v_2,w_2).$$

The compatibilty condition (5.5) implies that $u_1v_1w_1 = u_2v_2w_2 = uvw$, indeed

$$u_1v_1w_1 = \alpha_u(v)\alpha_{\beta_v(u)}(w)\beta_w(\beta_v(u)) = \alpha_u(v)\beta_v(u)w = uvw;$$

$$u_2v_2w_2 = \alpha_u(\alpha_v(w))\beta_{\alpha_v(w)}(u)\beta_w(v) = u\alpha_v(w)\beta_w(v) = uvw.$$

Hence it sufficies to prove that $u_1 = v_1$ and $w_1 = w_2$, but this is true by the properties of α and β.

Moreover, we can construct an inverse of r.
Let $r(u,v) = (x,y)$, with $x = \alpha_u(v)$ and $y = \beta_v(u)$. Then we have that $u = \beta_{v^{-1}}(y)$, $v = \alpha_{u^{-1}}(x)$ and, by compatibility, $uv = xy$. Observe that

$$\alpha_y(v^{-1})u = \alpha_y(v^{-1})\beta_{v^{-1}}(y) = yv^{-1} = x^{-1}u,$$

hence $\alpha_y(v^{-1}) = x^{-1}$, so $v^{-1} = \alpha_{y^{-1}}(x^{-1})$. Similarly

$$v\beta_x(u^{-1}) = \alpha_{u^{-1}}(x)\beta_x(u^{-1}) = u^{-1}x = vy^{-1}$$

hence $u^{-1} = \beta_{x^{-1}}(y^{-1})$.
Therefore we conclude saying that, since $r(y^{-1},x^{-1}) = (\alpha_{y^{-1}}(x^{-1}), \beta_{x^{-1}}(y^{-1})) = (v^{-1},u^{-1})$, if we consider $\iota(x,y) := (y^{-1},x^{-1})$, we have that $\iota r \iota$ is the inverse of r. □

Next we give two alternative descriptions of our construction.

Definition 5.9. Let G be a group with multiplication $m\colon G\times G \to G$. A *braiding operator* on G is a bijective map $\sigma\colon G\times G \to G\times G$ satisfying

1. for any $u,v,w \in G$,

$$\sigma(uv,w) = (id\times m)\sigma_{12}\sigma_{23}(u,v,w), \tag{5.6}$$

$$\sigma(u,vw) = (m\times id)\sigma_{23}\sigma_{12}(u,v,w); \tag{5.7}$$

2. for any $u \in G$,

$$\sigma(1,u) = (u,1), \qquad \sigma(u,1) = (1,u); \tag{5.8}$$

3. for any $u, v \in G$,

$$m\sigma(u,v) = uv. \tag{5.9}$$

Theorem 5.10. *([27]) Over any group G, the following data are equivalent:*

1. *(α, β): an homomorhism and anti-homomorphism of groups $G \to \mathrm{Sym}(G)$ such that $uv = \alpha_u(v)\beta_v(u)$, for every $u, v \in G$;*
2. *σ: a braiding operator on G*
3. *$\pi\colon G \to A$: a bijective 1-cocycle.*

Proof. Case 1: $(\alpha, \beta) \iff \sigma$. The equivalence between (α, β) and σ is given by $\sigma(u,v) = (\alpha_u(v), \beta_v(u))$.
First we assume that α, β are a homomorphism and an anti homomorphism of groups that satisfy (5.5) and we verify that σ is a braiding operator.

Let us check the properties of a braiding operator.

1. For every $u, v, w \in G$, we have that

$$\sigma(uv, w) = (\alpha_{uv}(w), \beta_w(uv)) = (u_1, v_1);$$

on the other hand we have

$$\begin{aligned}(id \times m)\sigma_{12}\sigma_{23}(u,v,w) &= (id \times m)\sigma_{12}(u, \alpha_v(w), \beta_w(v))\\ &= (id \times m)(\alpha_u(\alpha_v(w)), \beta_{\alpha_v(w)}(u), \beta_w(v))\\ &= (\alpha_{uv}(w), \beta_{\alpha_v(w)}(u)\beta_w(v))\\ &= (u_2, v_2).\end{aligned}$$

By compatibility condition (5.5), we have that $u_1v_1 = uvw = u\alpha_v(w)\beta_w(v) = u_2v_2$, hence $v_1 = v_2$, since $u_1 = u_2$.
Analogously, $\sigma(u, vw) = (\alpha_u(vw), \beta_{vw}(u) = u_3v_3$ and

$$(m \times id)\sigma_{23}\sigma_{12}(u,v,w) = (\alpha_u(v)\alpha_{\beta_v(u)}(w), \beta_w(\beta_v(u)) = u_4v_4,$$

with $v_4 = v_3$ because $u_3 = v_3$ and $u_3v_3 = uvw = u_4v_4$, again by the compatibility condition.

2. For every $u \in G$, we have that $\sigma(1,u) = (\alpha_1(u), \beta_u(1)) = (u, \beta_u(1))$. Moreover if we consider (5.5) with $u = 1$ we obtain $v = v\beta_v(1)$, that implies $\sigma(1,u) = (u,1)$ and similarly $\sigma(u,1) = (1,u)$.

3. The third property is precisely the compatibility condition.

This completes the proof that σ is a braiding operator.
Conversely, assume that σ is a braiding operator. Then, comparing the first coordinates of (5.6), we see that $\alpha_{uv}(w) = \alpha(u, \alpha_v(w))$ for every $u, v, w \in G$. Moreover the first equality in (5.8) implies $\alpha(u,1) = u$, for every $u \in G$. This proves that α is a homomorphism. Similarly β is an anti-homomorphism. Moreover, as said above, the compatibility condition is equivalent to (5.8).

Case 2: $(\alpha, \beta) \iff (A, \pi)$. Given $\alpha, \beta \colon G \to \mathrm{Sym}(G)$, a homomorphism and an antihomomorphism of groups, take $A = G$ with the following operation

$$u * v = u\alpha_{u^{-1}}(v). \tag{5.10}$$

Replaicing v with $\alpha_u(v)$ in (5.10), we obtain

$$u * \alpha_u(v) = u\alpha_{u^{-1}}(\alpha_u(v)) = u\alpha_1(v) = uv,$$

which means exactly that $\pi = id \colon G \to A$ is a bijective 1-cocycle. It remains to show that $(A, *)$ is a G-group.
Clearly, $1 * u = \alpha_1(u) = u$, that is 1 is a left unit and $u * \alpha_u(u^{-1}) = u\alpha_{u^{-1}}(\alpha_u(u^{-1})) = uu^{-1} = 1$, that is $\alpha_u(u^{-1})$ is a right inverse of u with respect to $*$. Notice that, by compatibility condition, we have that $v\beta_v(u)^{-1} = u^{-1}\alpha_u(v)$, that implies $u * v = v\beta_v(u^{-1})^{-1}$. Hence $u * 1 = \beta_1(u^{-1})^{-1} = u$, that is 1 is a right unit and

$$\beta_{u^{-1}}(u)^{-1} * u = u\beta_u(\beta_{u^{-1}}(u))^{-1} = u\beta_1(u)^{-1} = uu^{-1} = 1,$$

that is $\beta_{u^{-1}}(u)^{-1}$ is a left inverse of u. Remember that by the compatibility condition $1 = uu^{-1} = \alpha_u(u^{-1})\beta_{u^{-1}}(u)$, hence $\beta_{u^{-1}}(u)^{-1} = \alpha_u(u^{-1})$, so we have found an inverse for each $u \in G$.
To prove the associativity of $*$ and that $\alpha_u \in \mathrm{Aut}(A)$ for every $u \in G$, we first use the compatibility condition (5.5) to get

$$\alpha_u(vx)\beta_{vx}(u) = uvx = \alpha_u(v)\beta_v(u)x = \alpha_u(v)\alpha_{\beta_v(u)}(x)\beta_x(\beta_v(u)), \tag{5.11}$$

thus, since β is an anti-homomorphism,

$$\alpha_u(vx) = \alpha_u(v)\alpha_{\beta_v(u)}(x). \tag{5.12}$$

Now fix $v, w \in G$, we have that $\alpha_u(v * w) = \alpha_u(v\alpha_{u^{-1}}(v))$. Taking $x = \alpha_{v^{-1}}(w)$, we obtain that

$$\begin{aligned}\alpha_u(v * w) = \alpha_u(vx) &\overset{(5.12)}{=} \alpha_u(v)\alpha_{\beta_v(u)}(x)\\ &= \alpha_u(v)\alpha_{\beta_v(u)}(\alpha_{v^{-1}}(w)) = \alpha_u(v)\alpha_{\beta_v(u)v^{-1}}(w)\\ &\overset{(5.5)}{=} \alpha_u(v)\alpha_{\alpha_u(v)^{-1}u}(w) = \alpha_u(v) * \alpha_u(w),\end{aligned} \tag{5.13}$$

that is α_u is an endomorphism, and indeed an isomorphism, of A. Finally, the associativity of $*$ follows from

$$\begin{aligned}u * (v * w) = u\alpha_{u^{-1}}(v * w) &\overset{(5.13)}{=} u(\alpha_{u^{-1}}(v) * \alpha_{u^{-1}}(w))\\ &= u\alpha_{u^{-1}}(v)\alpha_{\alpha_{u^{-1}}(v)^{-1}u^{-1}}(w) = (u * v)\alpha_{(u*v)^{-1}}(w)\\ &= (u * v) * w.\end{aligned}$$

Conversely, let A be a G-group and $\pi\colon G \to A$ a bijective 1-cocycle, with $(u, a) \mapsto u \cdot a$ the action of G on A. Define $\alpha\colon G \to \mathrm{Sym}(G)$, $u \mapsto \alpha_u$ with $\alpha_u(v) := \pi^{-1}(u \cdot \pi(v))$, for every $u, v \in G$. The map α is group morphism since

$$\begin{aligned}\alpha_u(\alpha_v(w)) &= \pi^{-1}(u \cdot \pi(\alpha_v(w))) = \pi^{-1}(u \cdot (v \cdot \pi(w)))\\ &= \pi^{-1}(uv \cdot \pi(w)) = \alpha_{uv}(w)\end{aligned}$$

for every $u, v, w \in G$. Moreover, we define β according to the compatibility condition, that is $\beta_v(u) := \alpha_u(v)^{-1}uv$. It remains to show that β is an anti-homomorphism of groups. In order to prove that, observe

$$\pi^{-1}(\pi(u)(u \cdot a)) = \pi^{-1}(\pi(u\pi^{-1}(a))) = u\pi^{-1}(a); \tag{5.14}$$

for every $u, v \in G, a \in A$. Denote by $u * v$ the element $\pi^{-1}(\pi(u)\pi(v)) \in G$. Taking $a = u^{-1} \cdot \pi(v)$ in (5.14), we obtain

$$u\alpha_{u^{-1}}(v) = u\pi^{-1}(u^{-1} \cdot \pi(v)) = \pi^{-1}(\pi(u)\pi(v)) = u * v. \tag{5.15}$$

Since A is a G- group, we have, for every $u, v, w \in G$, that

$$\begin{aligned}\alpha_u(v * w) &= \pi^{-1}(u \cdot \pi(u * w)) = \pi^{-1}(u \cdot \pi(v)\pi(w))\\ &= \pi^{-1}((u \cdot \pi(v))(u \cdot \pi(w))) = \pi^{-1}(u \cdot \pi(v)) * \pi^{-1}(u \cdot \pi(w))\\ &= \alpha_u(v) * \alpha_u(w) = \alpha_u(v)\alpha_{\alpha_u(v)^{-1}}(\alpha_u(w)).\end{aligned}$$

As in (5.11) the following equalities hold for every $u, v, x \in G$. $\alpha_u(vx)\beta_{vx}(u) = uvx = \alpha_u(v)\beta_v(u)x = \alpha_u(v)\alpha_{\beta_v(u)}(x)\beta_x(\beta_v(u))$. Hence it sufficies to show that $\alpha_u(vx) = \alpha_u(v)\alpha_{\beta_v(u)}(x)$. By compatibility condition, $\alpha_u(v)^{-1}u = \beta_v(u)v^{-1}$. So fix $u, v, x \in G$ and consider $w := \alpha_v(x)$, in such a way to have $v * w = vx$. Then

$$\begin{aligned}\alpha_u(vx) = \alpha_u(v * w) &\overset{(5.15)}{=} \alpha_u(v)\alpha_{\alpha_u(v)^{-1}}(\alpha_u(w))\\ &= \alpha_u(v)\alpha_{\alpha_u(v)^{-1}u}(w) = \alpha_u(v)\alpha_{\beta_v(u)v^{-1}}(w)\\ &= \alpha_u(v)\alpha_{\beta_v(u)}(\alpha_{v^{-1}}(w)) = \alpha_u(v)\alpha_{\beta_v(u)}(x)\end{aligned}$$

And this completes the proof. □

Corollary 5.11. *Any braiding operator is invertibile and satisfies the Yang-Baxter condition* (5.1)*.*

5.3 Skew Braces and Solutions of the Yang-Baxter Equation

Theorem 5.12 ([22])**.** *Let A be a left skew brace. Then*

$$r_A\colon A \times A \to A \times A, \quad r_A(a,b) = (\lambda_a(b), \lambda_a(b)' \circ a \circ b), \tag{5.16}$$

is a bijective non-degenerate solution of the Yang-Baxter equation.

Proof. By Corollary 5.11, every braiding operator is a bijective non-degenerate solution of the Yang-Baxter equation. Thus it is enough to prove that r_A is a braiding operator on $(A, \circ)$. For simplicity, for the entire proof we will use r instead of r_A.

We have that $mr(a,b) = \lambda_a(b) \circ \lambda_a(b)' \circ a \circ b = a \circ b$, for all $a, b \in A$. Moreover, since λ is an homomorphism from $(A, \circ)$ to $\mathrm{Aut}(A, *)$, for every $a \in A$ we obtain $r(a, 1) = (1, \lambda_a(1)' \circ a) = (1, a)$ and $r(1, a) = (a, \lambda_1(a)' \circ a) = (a, 1)$. If $a, b, c \in A$, then

$$\begin{aligned}(id \times m)r_{12}r_{23}(a,b,c) &= (id \times m)r_{12}\big(a, \lambda_b(c), \lambda_b(c)' \circ b \circ c\big)\\ &= (id \times m)\big(\lambda_a\lambda_b(c), (\lambda_a\lambda_b(c))' \circ a \circ \lambda_b(c), \lambda_b(c)' \circ b \circ c\big)\\ &= \big(\lambda_a\lambda_b(c), (\lambda_a\lambda_b(c))'a \circ b \circ c\big)\\ &= \big(\lambda_{a\circ b}(c), (\lambda_{a\circ b}(c))' \circ (a \circ b) \circ c\big)\\ &= r(a \circ b, c).\end{aligned}$$

From Remark 1.9 we obtain for every $a, b, c \in A$

$$\lambda_a(b \circ c) = \lambda_a(b * \lambda_b(c)) = \lambda_a(b) * \lambda_{a \circ b}(c).$$

From this formula we deduce that

$$\begin{aligned}\lambda_a(b) \circ \lambda_{\lambda_a(b)' \circ a \circ b}(c) &= \lambda_a(b) \circ \lambda^{-1}_{\lambda_a(b)}(\lambda_a \lambda_b(c)) = \lambda_a(b) * \lambda_{\lambda_a(b)}(\lambda^{-1}_{\lambda_a(b)}(\lambda_a \lambda_b(c))) \\ &= \lambda_a(b) * \lambda_{a \circ b}(c) = \lambda_a(b \circ c).\end{aligned}$$

Then

$$\begin{aligned}(m \times id) r_{23} r_{12}(a, b, c) &= (m \times id) r_{23}\big(\lambda_a(b), \lambda_a(b)' \circ a \circ b, c\big) \\ &= (m \times id)\big(\lambda_a(b), \lambda_{\lambda_a(b)' \circ a \circ b}(c), \lambda_{\lambda_a(b)' \circ a \circ b}(c)' \circ \lambda_a(b)' \circ a \circ b \circ c\big) \\ &= \big(\lambda_a(b \circ c), (\lambda_a(b \circ c))' \circ \lambda_a(b) \circ \lambda_a(b)' \circ a \circ b \circ c\big) \\ &= \big(\lambda_a(b \circ c), (\lambda_a(b \circ c))' \circ a \circ (b \circ c)\big) \\ &= r(a, b \circ c).\end{aligned}$$

□

Indeed, this map works also functorially. Let SYBE be the category of non-degenerate solutions of the Yang-Baxter equation, where a morphism between two solutions (X, r) and (Y, s) is a map $f \colon X \to Y$ such that this diagram

$$\begin{tikzcd} X \times X \arrow[r, "f \times f"] \arrow[d, "r"'] & Y \times Y \arrow[d, "s"] \\ X \times X \arrow[r, "f \times f"] & Y \times Y \end{tikzcd}$$

commutes.

Define $F \colon \mathsf{SKB} \to \mathsf{SYBE}$ by

$$F(A, *, \circ) := (A, r_A)$$

and

$$F(A \xrightarrow{f} B) := f.$$

$F(f)$ is a morphism in SYBE. Indeed, consider the following diagram:

$$\begin{tikzcd} A \times A \arrow[r, "f \times f"] \arrow[d, "r_A"'] & B \times B \arrow[d, "r_B"] \\ A \times A \arrow[r, "f \times f"] & B \times B \end{tikzcd}$$

For every $a_1, a_2 \in A$,we have that

$$\begin{aligned}(f \times f)r_A(a_1, a_2) &= (f \times f)\big(\lambda^A_{a_1}(a_2), \lambda^A_{a_1}(a_2)' \circ a_1 \circ a_2\big)\\ &= \big(f(\lambda^A_{a_1}(a_2)), f(\lambda^A_{a_1}(a_2)' \circ a_1 \circ a_2)\big)\\ &= \big(\lambda^B_{f(a_1)}(f(a_2)), \lambda^B_{f(a_1)}(f(a_2))' \circ f(a_1) \circ f(a_2)\big)\end{aligned}$$

and, on the other hand,

$$\begin{aligned}r_B((f \times f)(a_1, a_2)) &= r_B(f(a_1), f(a_2))\\ &= \big(\lambda^B_{f(a_1)}(f(a_2)), \lambda^B_{f(a_1)}(f(a_2))' \circ f(a_1) \circ f(a_2)\big).\end{aligned}$$

It is easy to see that F respects compositions and identies, therefore it is a functor.

Proposition 5.13. *Let $(A, *, \circ)$ be a left skew brace. Then r_A is involutive if and only if $(A, *)$ is abelian.*

Proof. Let $a, b \in A$. Recall that $r_A(a, b) = (\lambda_a(b), \lambda_a(b)' \circ a \circ b)$. Let us compute r_A^2.

$$\begin{aligned}r^2_A(a, b) &= r_A(\lambda_a(b), \lambda_a(b)' \circ a \circ b)\\ &= \Big(\lambda_{\lambda_a(b)}\big(\lambda_a(b)' \circ a \circ b\big), \lambda_{\lambda_a(b)}\big(\lambda_a(b)' \circ a \circ b\big)' \circ \lambda_a(b) \circ \lambda_a(b)' \circ a \circ b\Big)\\ &= \Big(\lambda_{\lambda_a(b)}\big(\lambda_a(b)' \circ a \circ b\big), \lambda_{\lambda_a(b)}\big(\lambda_a(b)' \circ a \circ b\big)' \circ a \circ b\Big)\end{aligned}$$

On the other hand, $\lambda_{\lambda_a(b)}(\lambda_a(b)' \circ a \circ b) = (\lambda_a(b))^{-1} * (a \circ b) = (a \circ b)^{-1} * a * (a \circ b)$, hence

$$r^2_A(a, b) = \Big((a \circ b)^{-1} * a * (a \circ b), \big((a \circ b)^{-1} * a * (a \circ b)\big)' \circ a \circ b\Big).$$

Hence r_A is involutive if and only if $(a \circ b)^{-1} * a * (a \circ b) = a$ and $\big((a \circ b)^{-1} * a * (a \circ b)\big)' \circ a \circ b = b$ if and only if $a * (a \circ b) = (a \circ b) * a$, for every $a, b \in A$. So for every element c of A, we have that $a * c = a * (a \circ (a' \circ c)) = (a \circ (a' \circ c)) * a = c * a$. Therefore the thesis. □

Our next goal is to build a skew brace from a solution of the Yang-Baxter equation. Let X be a set and denote with $F(X)$ the *free group* over X. We denote by $i \colon X \hookrightarrow F(X)$ the natural embedding. Let S be a set of words in X, so S naturally gives a subset of $F(X)$. We define *the group presentation*

$\langle X;\, S\rangle$ of generators in X and relations in S, the quotient group $F(X)/N_S$, where N_S is the normal closure of S in $F(X)$, i.e. the smallest normal subgroup of $F(X)$ that contains S. Recall that the normal closure of a set S in an arbitrary group G is precisely the subgroup generated by all the elements of the form $g^{-1}sg$, with $g \in G$ and $s \in S$, so

$$N_S = \{g_1^{-1}s_1^{\epsilon_1}g_1 \cdots g_k^{-1}s_k^{\epsilon_k}g_k \mid k \geq 0;\, g_i \in G;\, s_i \in S,\, \epsilon_i = \pm 1\}.$$

Consider (X, r) a non-degenerate solution of the Yang-Baxter equation, with $r(x, y) = (f_x(y), g_y(x))$.

We define the groups

$$(G(X, r), \circ) := \langle X \mid x \circ y = f_x(y) \circ g_y(x),\, \text{for}\, x, y \in X\rangle,$$

called the *structure group* and

$$(A(X, r), *) := \langle X \mid x * f_x(y) = f_x(y) * f_{f_x(y)}g_y(x)\, \text{for}\, x, y \in X\rangle,$$

called the *derived group.*

We denote by $i_G\colon X \to G(X, r)$ and $i_A\colon X \to A(X, r)$ the two natural maps.

Lemma 5.14 ([3]). *Let (X, r) be a non-degenerate solution of the Yang-Baxter equation, with $r(x, y) = (f_x(y), g_y(x))$. The map $f\colon X \to \mathrm{Sym}(X)$, $x \mapsto f_x$ can be extended with a unique homomorphism of groups $\mathbf{f}\colon G(X, r) \to \mathrm{Sym}(X)$, namely $\mathbf{f}_{i_G(x)}(y) = f_x(y)$, for every $x, y \in X$.*

It also induces a unique homomorphism of groups $\overline{\mathbf{f}}\colon G(X, r) \to \mathrm{Aut}(A(X, r))$ such that $\overline{\mathbf{f}}_{i_G(x)}(i_A(y)) = i_A(f_x(y))$, for any $x, y \in X$.

Moreover, the map $g\colon X \to \mathrm{Sym}(X)$, $x \mapsto g_x$ can be extended with a unique anti-homomorphism of groups $\mathbf{g}\colon G(X, r) \to \mathrm{Sym}(X)$.

Proof. It is well known that the map f can be uniquely extended to a morphism of groups $f\colon F(X) \to \mathrm{Sym}(X)$.

This map f induces a unique morphism $\mathbf{f}\colon G(X, r) \to \mathrm{Sym}(X)$ if it preserves the defining relations of $G(X, r)$, i.e. if $f_{xy} = f_{f_x(y)g_y(x)}$, for every $x, y \in X$, but this is true by (5.2). The situation is described by the following commutative diagram:

$$\begin{tikzcd}
G(X,r) \arrow[rr, dashed, "\mathbf{f}"] & & \mathrm{Sym}(X) \\
& X \arrow[ul, "i_G"] \arrow[ur, "f"'] \arrow[d, hook, "i"] & \\
& F(X) \arrow[uul, two heads] \arrow[uur, "f"'] &
\end{tikzcd}$$

Similarly, g is extended to a unique anti-homomorphism $\mathbf{g}\colon G(X,r) \to \mathrm{Sym}(X)$ since by (5.4) $g_x g_y = g_{g_x(y)} g_{f_y(x)}$.

Now we have to prove that $f\colon X \to \mathrm{Sym}(X)$ induces a morphism $\overline{\mathbf{f}}\colon G(X,r) \to \mathrm{Aut}(A(X,r))$. First we check that $f_x\colon X \to X$ induces a unique morphism $\overline{f_x}\colon A(X,r) \to A(X,r)$ such that $f_x|_{A(X,r)} = i_A(\overline{f_x})$.

The map $i_A f_x\colon X \to A(X,r)$ can be uniquely extended to a morphism $f_x\colon F(X) \to A(X,r)$. The morphism f_x induces a unique morphism $\overline{f_x}\colon A(X,r) \to A(X,r)$ if and only if

$$f_x(y) * f_x(f_y(z)) = f_x(f_y(z)) * f_x\big(f_{f_y(z)} g_z(x)\big)$$

for any $y, z \in X$. But this is true since:

$$\begin{aligned}
f_x(y) * f_x f_y(z) &= f_x(y) * f_{f_x(y)} f_{g_y(x)}(z) \qquad \text{(by (5.2))} \\
&= f_{f_x(y)} f_{g_y(x)}(z) * f_{f_{f_x(y)} f_{g_y(x)}(z)} g_{f_{g_y(x)}(z)} f_x(y) \\
&= f_x f_y(z) * f_{f_x f_y(z)} f_{g_{f_y(z)}(x)} g_z(y) \quad \text{(by (5.2) and by (5.3))} \\
&= f_x f_y(z) * f_x f_{f_y(z)} g_z(y) \qquad \text{(by (5.2))}.
\end{aligned}$$

Therefore we proved that $i_A f_x$ induces a unique morphism $\overline{f_x}$ such that the following diagram

$$\begin{tikzcd}
X \arrow[r, "f_x"] \arrow[d, "i_A"'] & X \arrow[d, "i_A"] \\
A(X,r) \arrow[r, "\overline{f_x}"'] & A(X,r)
\end{tikzcd}$$

commutes.

Similarly we are going to prove that $f_x^{-1}\colon X \to X$ induces a unique morphism $\overline{f_x^{-1}}\colon A(X,r) \to A(X,r)$ such that the diagram

$$\begin{tikzcd}
X \arrow[r, "f_x^{-1}"] \arrow[d, "i_A"'] & X \arrow[d, "i_A"] \\
A(X,r) \arrow[r, "\overline{f_x^{-1}}"'] & A(X,r)
\end{tikzcd} \tag{5.17}$$

commutes. As before it is enough to check that

$$f_x^{-1}(y) * f_x^{-1}(f_y(z)) = f_x^{-1}(f_y(z)) * f_x^{-1}\big(f_{f_y(z)}g_z(x)\big) \tag{5.18}$$

for every y, zX.

In order to prove it, we need two more properties on f and g. Condition (5.2) implies that $f_x f_{f_x^{-1}(y)} = f_y f_{g_{f_x^{-1}(y)}(x)}$, then

$$f_x^{-1} f_y = f_{f_x^{-1}(y)} f^{-1}_{g_{f_x^{-1}(y)}(x)}. \tag{5.19}$$

Moreover, (5.2) and (5.3) imply that $f_{g_{f_x^{-1} f_{f_x(y)}(z)}(x)} g_{f^{-1}_{g_y(x)}(z)}(x) = g_z f_x(y)$, then

$$f^{-1}_{g_{f_x^{-1} f_y(z)}(x)} g_z(y) = g_{f^{-1}_{g_{f_x^{-1}(y)}(x)}(z)}(x). \tag{5.20}$$

Through these identities we get

$$\begin{aligned}
f_x^{-1}(y) * f_x^{-1} f_y(z) &\overset{(5.19)}{=} f_x^{-1}(y) * f_{f_x^{-1}(y)} f^{-1}_{g_{f_x^{-1}(y)}(x)}(z) \\
&= f_{f_x^{-1}(y)} f^{-1}_{g_{f_x^{-1}(y)}(x)}(z) * f_{f_{f_x^{-1}(y)} f^{-1}_{g_{f_x^{-1}(y)}(x)}(z)} g_{f^{-1}_{g_{f_x^{-1}(y)}(x)}(z)} f_x^{-1}(y) \\
&\overset{(5.19)}{=} f_x^{-1} f_y(z) * f_{f_x^{-1} f_y(z)} g_{f^{-1}_{g_{f_x^{-1}(y)}(x)}(z)} f_x^{-1}(y) \\
&\overset{(5.20)}{=} f_x^{-1} f_y(z) * f_{f_x^{-1} f_y(z)} f^{-1}_{g_{f_x^{-1} f_y(z)}(x)} g_z(y) \\
&\overset{(5.19)}{=} f_x^{-1} f_y(z) * f_x^{-1} f_{f_y(z)} g_z(x).
\end{aligned}$$

Hence we proved (5.18). Moreover, since the morphism $id_{A(X,r)}\colon A(X,r) \to A(X,r)$ is the unique morphism such that the diagram

$$\begin{tikzcd}
X \arrow[r, "id_X"] \arrow[d, "i_A"'] & X \arrow[d, "i_A"] \\
A(X,r) \arrow[r, "id_{A(X,r)}"'] & A(X,r)
\end{tikzcd}$$

commutes, it is clear that $\overline{f_x}\overline{f_x^{-1}} = \overline{f_x^{-1}}\overline{f_x} = id_{A(X,r)}$, so $\overline{f_x}$ is an automorphism of $A(X,r)$. So we have obtained a well defined map $\overline{f}\colon X \to \mathrm{Aut}(A(X,r))$.

Finally observe that if a map $h \in \mathrm{Sym}(X)$ induces a morphism $\overline{h}\colon A(X,r) \to A(X,r)$ such that

$$\begin{tikzcd} X \arrow[r, "h"] \arrow[d, "i_A"'] & X \arrow[d, "i_A"] \\ A(X,r) \arrow[r, "\overline{h}"'] & A(X,r) \end{tikzcd}$$

commutes, then $\overline{h}$ is the unique morphism that satisfies this condition. Therefore, by (5.2), we can say that

$$\overline{f}_x\overline{f}_y = \overline{f}_{f_x(y)}\overline{f}_{g_y(x)},$$

for any $x, y \in X$, therefore there exists a unique morphism $\overline{\mathbf{f}}\colon G(X,r) \to \mathrm{Aut}(A(X,r))$ such that $\overline{\mathbf{f}}_{i_G(x)}(i_A(y)) = i_A(f_x(y))$, for every $x, y \in X$, and this concludes the proof. □

We need a previous result about 1-cocycles.

Theorem 5.15. *([3]) Let G be a group defined by a group presentation $G = \langle X \mid S\rangle$ and let H be a G-group with $\alpha\colon G \to \mathrm{Aut}(H)$ the corresponding action.*

Then a map $\pi\colon X \to H$ induces a 1-cocycle $\Pi\colon G \to H$ if and only if $\overline{\pi}(s) = 1$ for every $s \in S$, where $\overline{\pi}(x) = \pi(x)$ for every $x \in X$ and $\overline{\pi}(x_1^{e_1} \cdots x_n^{e_n}) = \alpha_{g_1}(\pi(x_1))^{e_1} \cdots \alpha_{g_n}(x_n)^{e_n}$ with $e_i \in \{\pm 1\}$ and $g_i = x_1^{e_1} \cdots x_{i-1}^{e_{i-1}}$ if $e_i = 1$ and $g_i = x_1^{e_1} \cdots x_i^{e_i}$ if $e_i = -1$.

Proof. Suppose to have a 1-cocycle $\Pi\colon G \to H$ such that $\Pi|X = \pi$, then, since $G = F(X)/N_S$, $\Pi(N_S) = 1$ and hence $\Pi(s) = 1$ for every $s \in S$.

Conversely, given a map $\pi\colon X \to H$, we extended π to a map $\overline{\pi}\colon F(X) \to H$ as in the statement of the Theorem and we assume that $\overline{\pi}(s) = 1$ for any $s \in S$. A direct calculation shows that with this extension of π, $\overline{\pi}$ is a 1-cocycle with respect to the action

$$F(X) \hookrightarrow F(X)/N_S \xrightarrow{\alpha} \mathrm{Aut}(H).$$

Define $\Pi\colon G \to H$ by $\Pi(gN_S) := \overline{\pi}(g)$. To show that it is a well defined map, we have to prove that $\overline{\pi}(n) = 1$ for every $n \in N_S$. First, if $s \in S$, then $\overline{\pi}(s^{-1}) = \alpha_s^{-1}(\overline{\pi}(s))^{-1} = \alpha_s^{-1}(1)^{-1} = 1$. Moreover, if $s \in S \cup S^{-1}$ and $u \in F(X)$, then

$$\begin{aligned}\overline{\pi}(u^{-1}su) &= \overline{\pi}(u^{-1})\alpha_{u^{-1}}(\overline{\pi}(s))\alpha_{u^{-1}s}(\overline{\pi}(u))\\ &= \overline{\pi}(u^{-1})\alpha_{u^{-1}}(1)\alpha_{u^{-1}}\alpha_1(\overline{\pi}(u))\\ &= \overline{\pi}(u^{-1})\alpha_{u^{-1}}(\overline{\pi}(u))\\ &= \overline{\pi}(u^{-1}u) = 1,\end{aligned}$$

where $\alpha_n = id_H$ for every $n \in N_S$ since α is a group homomorphism. Hence, by induction, for every $n = u_1^{-1}s_1u_1 \cdots u_k^{-1}s_ku_k \in N_S$, $\overline{\pi}(n) = 1$. So let $uN = vN$ two different representatives of an element in G. Then $v = un$ for some $n \in N_S$ and hence

$$\Pi(vN_S) = \overline{\pi}(v) = \overline{\pi}(u)\alpha_u(\overline{\pi}(n)) = \overline{\pi}(u) = \Pi(uN_S).$$

So Π is a well-defined map. We conclude showing that Π is a 1-cocycle, indeed, let $uN_S, vN_S \in G$, then

$$\Pi(uN_SvN_S) = \Pi(uvN_S) = \overline{\pi}(uv) = \overline{\pi}(u)\alpha_u(\overline{\pi}(v)) = \Pi(uN)\alpha_{uN_S}(\Pi(vN_S)).$$

□

Lemma 5.16. *([3]) Let (X, r) be a non-degenerate solution of the Yang-Baxter equation. Then, the map $T\colon i_G(X) \to i_G(X)$ given by $T(i_G(x)) = i_G(f_x^{-1}(x))$, for all $x \in X$, is bijective with inverse $T^{-1}(i_G(x)) = i_G(g_x^{-1}(x))$ for all $x \in X$.*

Proof. Let us check that T is well-defined. So let $x, y \in X$ be such that $i_G(x) = i_G(y)$. We have to prove that $i_G(f_x^{-1}(x)) = i_G(f_y^{-1}(y))$.

By Lemma 5.14, $f\colon X \to \operatorname{Sym}(X)$ extends to a morphism $\mathbf{f}\colon G(X, r) \to \operatorname{Sym}(X)$ such that $f_x = \mathbf{f}_{i_G(x)}$. Hence, if $i_G(x) = i_G(y)$, then $f_x = f_y$ implies that $f_x^{-1} = f_y^{-1}$ and hence $i_G(f_x^{-1}(x)) = i_G(f_y^{-1}(x))$. Similarly, since $g\colon X \to \operatorname{Sym}(X)$ extends to an anti-homomorphism $\mathbf{g}\colon G(X, r) \to \operatorname{Sym}(X)$, we also have $g_x = \mathbf{g}_{i_G(x)}$ and, if $i_G(x) = i_G(y)$, then $g_x = g_y$ implies that $i_G(g_x(u)) = i_G(g_y(u))$ for every $u \in X$. Now, let $r(u, x) =$

$(f_u(x), g_x(u))$ and $r(u,y) = (f_u(y), g_y(u))$ with $u \in X$, then $i_G(u)i_G(x) = i_G(f_u(x))i_G(g_x(u))$ and $i_G(u)i_G(y) = i_G(f_u(y))i_G(g_y(u))$, so, since $i_G(x) = i_G(y)$ and $i_G(g_x(u)) = i_G(g_y(u))$, we obtain that $i_G(f_u(x)) = i_G(f_u(y))$ for any $u \in X$, therefore we get

$$i_G(f_x^{-1}(x)) = i_G(f_y^{-1}(x)) = i_G(f_y^{-1}(y)).$$

In an analogous way, one can check that $T' \colon i_G(X) \to i_G(X)$, $i_G(x) \mapsto i_G(g_x^{-1}(x))$, is well defined.

So it remains to prove that T and T' are one the inverse of the other. Notice that $r(x, f_x^{-1}(x)) = (x, g_{f_x^{-1}(x)}(x))$ for any $x \in X$, hence $i_G(f_x^{-1}(x)) = i_G(g_{f_x^{-1}(x)}(x))$ for every $x \in X$. Therefore

$$\begin{aligned} T'T(i_G(x)) &= T'(i_G(f_x^{-1}(x))) = i_G(g^{-1}_{f_x^{-1}(x)}(f_x^{-1}(x))) \\ &= i_G(g^{-1}_{f_x^{-1}(x)} g_{f_x^{-1}(x)}(x)) = i_G(x), \end{aligned}$$

for any $x \in X$.

Similarly, since $r(g_x^{-1}(x), x) = (f_{g_x^{-1}(x)}(x), x)$, for any $x \in X$, $i_G(g_x^{-1}(x)) = i_G(f_{g_x^{-1}(x)}(x))$. Therefore

$$\begin{aligned} TT'(i_G(x)) &= T(i_G(g_x^{-1}(x))) = i_G(f^{-1}_{g_x^{-1}(x)}(g_x^{-1}(x))) \\ &= i_G(f^{-1}_{g_x^{-1}(x)} f_{g_x^{-1}(x)}(x)) = i_G(x), \end{aligned}$$

for any $x \in X$, and this concludes the proof. □

Theorem 5.17 ([3]). *Let (X, r) be a non-degenerate solution of the Yang-Baxter equation. Then we can define a product $*$ over $G(X, r)$ such that $(G(X, r), *, \circ)$ is a left skew brace and $(G(X, r), *) \cong A(X, r)$.*

Proof. As in Chapter 1, we indicate with g' the inverse of g in $G(X, r)$.

By Proposition 2.8, to have a skew brace it is enough to show that there is a bijective 1-cocycle from $G(X, r)$ to $A(X, r)$.

Consider $\overline{\mathbf{f}} \colon G(X, r) \to \operatorname{Aut}(A(X, r))$ as in Lemma 5.14 and its restriction to X, $\overline{f} \colon X \to \operatorname{Aut}(A(X, r)$. Define $\pi \colon X \to A(X, r)$ by $\pi(x) = i_A(x)$.

By Theorem 5.15, π induces a 1-cocycle $\Pi \colon G(X, r) \to A(X, r)$ if

$$\overline{\pi}((xy)^{-1} f_x(y) g_y(x)) = 1$$

for every $x, y \in X$, where $\overline{\pi}\colon F(X) \to A(X,r)$ is defined in Theorem 5.15. By definition,

$$\begin{aligned}
\overline{\pi}(xy) &= \overline{\pi}(x) * \overline{f}_x(\overline{\pi}(y)) = i_A(x) * \overline{f}_x(i_A(y)) \\
&= i_A(x) * i_A(f_x(y)) = i_A(f_x(y)) * i_A(f_{f_x(y)}g_y(x)) \\
&= i_A(f_x(y)) * \overline{f}_{f_x(y)}\big(i_A(g_y(x))\big) \\
&= \overline{\pi}(f_x(y)) * \overline{f}_{f_x(y)}\big(\overline{\pi}(g_y(x))\big) = \overline{\pi}(f_x(y)g_y(x))
\end{aligned}$$

for any $x, y \in X$. Hence

$$\begin{aligned}
\overline{\pi}((xy)^{-1}f_x(y)g_y(x)) &= \overline{\pi}((xy)^{-1}) * \overline{f}_{xy}^{-1}(\overline{\pi}(f_x(y)g_y(x))) \\
&= \overline{\pi}((xy)^{-1}) * \overline{f}_{xy}^{-1}(\overline{\pi}(xy)) \\
&= \overline{\pi}((xy)^{-1}(xy)) = \overline{\pi}(1) = 1.
\end{aligned}$$

Therefore, there exists a well defined 1-cocycle $\Pi\colon G(X,r) \to A(X,r)$ such that $\Pi(i_G(x)) = i_A(x)$, for every $x \in X$.

Observe that, from $1 = \Pi(i_G(x)' \circ i_G(x)) = \Pi(i_G(x)') * \overline{\mathbf{f}}_{i_G(x)'}(\Pi(i_G(x)))$, we have

$$\Pi(i_G(x)') = (\overline{\mathbf{f}}_{i_G(x)}^{-1}(i_A(x)))^{-1} \overset{(5.17)}{=} (i_A(f_x^{-1}(x)))^{-1}, \tag{5.21}$$

for every $x \in X$. Moreover, if $i_G(x) = i_G(y)$, then $i_A(x) = i_A(y)$.

Now we have to construt an inverse for Π.

We define $\theta\colon (F(X), \cdot) \to (G(X,r), \circ)$ by

$$\theta(1) = 1, \qquad \theta(x) = i_G(x), \qquad \theta(x^{-1}) = i_G(g_x^{-1}(x))' \tag{5.22}$$

for every $x \in X$, with x^{-1} the inverse of x and recursively define

$$\theta(x_1^{e_1} \cdots x_{n+1}^{e_{n+1}}) = \theta(x_1^{e_1} \cdots x_n^{e_n}) \circ \theta(\mathbf{f}^{-1}_{\theta(x_1^{e_1} \cdots x_n^{e_n})}(x_{n+1})^{e_{n+1}}), \tag{5.23}$$

with $\mathbf{f}\colon G(X,r) \to \mathrm{Sym}(X)$ defined in Lemma 5.14. First observation: consider now a generic element $u \in F(X)$, and $x_1, x_2 \in X$, $e_1, e_2 \in \{\pm 1\}$. First notice that, by definition, $\theta(ux_1^{e_1}) = \theta(u) \circ \theta(\mathbf{f}^{-1}_{\theta(u)}(x_1)^{e_1})$, then we have that

$$\begin{aligned}
\theta(ux_1^{e_1}x_2^{e_2}) &= \theta(ux_1^{e_1}) \circ \theta(\mathbf{f}^{-1}_{\theta(ux_1^{e_1})}(x_2)^{e_2}) \\
&= \theta(u) \circ \theta(\mathbf{f}^{-1}_{\theta(u)}(x_1)^{e_1}) \circ \theta(\mathbf{f}^{-1}_{\theta(u) \circ \theta(\mathbf{f}^{-1}_{\theta(u)}(x_1)^{e_1})}(x_2)^{e_2}) \\
&= \theta(u) \circ \theta(\mathbf{f}^{-1}_{\theta(u)}(x_1)^{e_1}\mathbf{f}^{-1}_{\theta(u)}(x_2)^{e_2}) \\
&= \theta(u) \circ \theta(\mathbf{f}^{-1}_{\theta(u)}(x_1^{e_1}x_2^{e_2})).
\end{aligned} \tag{5.24}$$

Second observation: let $x, y \in X$, we get

$$\begin{aligned}\theta(uf_x(y)) &= \theta(x) \circ \theta\big(\mathbf{f}^{-1}_{\theta(x)}(f_x(y))\big) = i_G(x) \circ \theta\big(\mathbf{f}^{-1}_{i_G(x)}(f_x(y))\big) \\ &= i_G(x) \circ \theta\big(f_x^{-1}(f_x(y))\big) = i_G(x) \circ i_G(y) \\ &= i_G(f_x(y)) \circ i_G(g_y(x)) = \theta(f_x(y)) \circ \theta(g_y(x)) \\ &= \theta(f_x(y)f_{f_x(y)}(g_y(x))),\end{aligned} \tag{5.25}$$

and this implies that

$$\begin{aligned}&\theta\Big(xf_x(y)\big(f_x(y)f_{f_x(y)}g_y(x)\big)^{-1}\Big) \\ &\overset{(5.24)}{=} \theta\big(xf_x(y)\big) \circ \theta\Big(\mathbf{f}^{-1}_{\theta(xf_x(y))}\big((f_x(y)f_{f_x(y)}g_y(x))^{-1}\big)\Big) \\ &\overset{(5.25)}{=} \theta\big(f_x(y)f_{f_x(y)}(g_y(x))\big) \circ \theta\Big(\mathbf{f}^{-1}_{\theta(f_x(y)f_{f_x(y)}g_y(x))}\big((f_x(y)f_{f_x(y)}g_y(x))^{-1}\big)\Big) \\ &\overset{(5.24)}{=} \theta\Big(f_x(y)f_{f_x(y)}g_y(x)\big((f_x(y)f_{f_x(y)}g_y(x))^{-1}\big)\Big) = \theta(1) = 1.\end{aligned}$$

We proved that θ is trivial over the relations of $A(X, r)$. So, as in Theorem 5.15, θ extends to a well-defined map $\Theta\colon A(X, r) \to G(X, r)$ such that $\Theta(i_A(x)) = i_G(x)$ and $\Theta(a * b) = \Theta(a) \circ \Theta(\bar{\mathbf{f}}^{-1}_{\Theta(a)}(b))$ for any $a, b \in A(X, r)$.

It remains to show that Θ and Π are inverse of each other. First we check it on the generators. Let $x \in X$, by definition of Θ and Π, we have that

$$\Pi(\Theta(i_A(x))) = \Pi(i_G(x)) = i_A(x),$$

and

$$\Theta(\Pi(i_G(x))) = \Theta(i_A(x)) = i_G(x).$$

Now we check it on the inverse of the generators. Let $x \in X$,

$$\begin{aligned}\Theta(\Pi(i_G(x)')) \overset{(5.21)}{=} \Theta(i_A(f_x^{-1}(x))^{-1}) &\overset{(5.22)}{=} i_G(g^{-1}_{f_x^{-1}(x)}f_x^{-1}(x))' \\ &= T^{-1}(T(i_G(x)')) = i_G(x)',\end{aligned}$$

where T, T^{-1} are the maps defined in Lemma 5.16. Moreover

$$\Pi(\Theta(i_A(x)^{-1})) \overset{(5.22)}{=} \Pi(i_G(g_x^{-1}(x))') \overset{(5.21)}{=} i_A(f^{-1}_{g_x^{-1}(x)}g_x^{-1}(x))^{-1},$$

on the other hand, $i_G(f^{-1}_{g_x^{-1}(x)}g_x^{-1}(x)) = T^{-1}T(i_G(x)) = i_G(x)$ by Lemma 5.16 and, as we have just noticed, this implies that $i_A(f^{-1}_{g_x^{-1}(x)}g_x^{-1}(x)) = i_A(x)$, therefore, $\Pi(\Theta(i_A(x)^{-1})) = i_A(x)^{-1}$.

Finally, let $i_G(x_1)^{e_1}\circ\cdots\circ i_G(x_n)^{e_n}$ a generic element of $G(X,r)$, with $x_i \in X$, $e_i \in \{1,'\}$. We prove by induction that $\Theta(\Pi(i_G(x_1)^{e_1}\circ\cdots\circ i_G(x_n)^{e_n})) = i_G(x_1)^{e_1}\circ\cdots\circ i_G(x_n)^{e_n}$. We have already check the case $n=1$. Assume that the case n is true, and we shall prove the case $n+1$.

$$\begin{aligned}
&\Theta\Pi(i_G(x_1)^{e_1}\circ\cdots\circ i_G(x_{n+1})^{e_{n+1}})\\
&=\Theta\Big(\Pi(i_G(x_1)^{e_1}\circ\cdots\circ i_G(x_n)^{e_n})*\overline{\mathbf{f}}_{i_G(x_1)^{e_1}\circ\cdots\circ i_G(x_n)^{e_n}}(\Pi(x_{n+1}^{e_{n+1}}))\Big)\\
&\overset{(5.23)}{=}\Theta\Pi(i_G(x_1)^{e_1}\circ\cdots\circ i_G(x_n)^{e_n})\circ\\
&\quad\circ\Theta(\overline{\mathbf{f}}^{-1}_{\Theta\Pi(i_G(x_1)^{e_1}\circ\cdots\circ i_G(x_n)^{e_n})}\overline{\mathbf{f}}_{i_G(x_1)^{e_1}\circ\cdots\circ i_G(x_n)^{e_n}}(\Pi(x_{n+1}^{e_{n+1}})))\\
&=i_G(x_1)^{e_1}\circ\cdots\circ i_G(x_n)\circ\Theta(\overline{\mathbf{f}}^{-1}_{i_G(x_1)^{e_1}\circ\cdots\circ i_G(x_n)^{e_n}}\overline{\mathbf{f}}_{i_G(x_1)^{e_1}\circ\cdots\circ i_G(x_n)^{e_n}}(\Pi(x_{n+1}^{e_{n+1}})))\\
&=i_G(x_1)^{e_1}\circ\cdots\circ i_G(x_n)\circ\Theta\Pi(i_G(x_{n+1}^{e_{n+1}}))\\
&=i_G(x_1)^{e_1}\circ\cdots\circ i_G(x_n)^{e_n}\circ i_G(x_{n+1})^{e_{n+1}},
\end{aligned}$$

where, in the first equalities, we use the fact that Π is a 1-cocycle and in the third and fifth equalities we use the inductive hypothesis.

It remains to do the same thing to prove that $\Pi\Theta = id_{A(X,r)}$. So let $i_A(x_1)^{e_1}*\cdots i_A(x_n)^{e_n}$ a generic element of $A(X,r)$, with $x_i\in X$ and $e_i\in\{1,-1\}$. We proceed by induction assuming that the case n is true.

$$\begin{aligned}
&\Pi\Theta(i_A(x_1)^{e_1}*\cdots i_A(x_{n+1})^{e_{n+1}})\\
&\overset{(5.23)}{=}\Pi\Big(\Theta(i_A(x_1)^{e_1}*\cdots i_A(x_n)^{e_n})\circ\Theta(\overline{\mathbf{f}}^{-1}_{\Theta(i_A(x_1)^{e_1}*\cdots i_A(x_n)^{e_n})}(i_A(x_{n+1})^{e_{n+1}}))\Big)\\
&=\Pi\Theta(i_A(x_1)^{e_1}*\cdots i_A(x_n)^{e_n})*\\
&\quad*\overline{\mathbf{f}}_{\Theta(i_A(x_1)^{e_1}*\cdots i_A(x_n)^{e_n})}\Big(\Pi\Theta(\overline{\mathbf{f}}^{-1}_{\Theta(i_A(x_1)^{e_1}*\cdots i_A(x_n)^{e_n})}(i_A(x_{n+1})^{e_{n+1}}))\Big)\\
&\overset{(5.17)}{=}i_A(x_1)^{e_1}*\cdots i_A(x_n)^{e_n}*\\
&\quad*\overline{\mathbf{f}}_{\Theta(i_A(x_1)^{e_1}*\cdots i_A(x_n)^{e_n})}\Big(\Pi\Theta\big(i_A(f^{-1}_{\Theta(i_A(x_1)^{e_1}*\cdots i_A(x_n)^{e_n})}(x_{n+1})^{e_{n+1}}\big)\Big)\\
&=i_A(x_1)^{e_1}*\cdots i_A(x_n)^{e_n}*\\
&\quad*\overline{\mathbf{f}}_{\Theta(i_A(x_1)^{e_1}*\cdots i_A(x_n)^{e_n})}\Big(i_A(f^{-1}_{\Theta(i_A(x_1)^{e_1}*\cdots i_A(x_n)^{e_n})}(x_{n+1})^{e_{n+1}}\Big)\\
&\overset{(5.17)}{=}i_A(x_1)^{e_1}*\cdots i_A(x_n)^{e_n}*\\
&\quad*\overline{\mathbf{f}}_{\Theta(i_A(x_1)^{e_1}*\cdots i_A(x_n)^{e_n})}\Big(\overline{\mathbf{f}}^{-1}_{\Theta(i_A(x_1)^{e_1}*\cdots i_A(x_n)^{e_n})}(i_A(x_{n+1})^{e_{n+1}})\Big)\\
&=i_A(x_1)^{e_1}*\cdots i_A(x_n)^{e_n}*i_A(x_{n+1})^{e_{n+1}},
\end{aligned}$$

where in the third and fourth equalities we used the inductive hypothesis and on the second one we use the definition of Π.

This concludes the proof.

Theorem 5.18. *([35]) Let (X, r) be a non-degenerate solution of the Yang-Baxter equation. Then there exists a unique left skew brace structure over $G(X, r)$ such that*

$$r_{G(X,r)}(i_G \times i_G) = (i_G \times i_G)r,$$

with $i_G\colon X \to G(X, r)$. Moreover, if A is a left skew brace and $f\colon X \to A$ is a map such that $(f \times f)r = r_A(f \times f)$, then there exists a unique skew brace morphism $\varphi\colon G(X, r) \to A$ such that $f = \varphi i$ and $(\varphi\times\varphi)r_{G(X,r)} = r_A(\varphi\times\varphi)$.

□

We constructed the skew brace structure of $G(X, r)$ through a bijective 1-cocycle, but doing computations we can forget about π and use directly the $*$ operation over $G(X, r)$. By definition of 1-cocycle, $g \circ h = g * \overline{\mathbf{f}}_g(h)$ for every $g, h \in G$, so in other words $g * h = g \circ (\overline{\mathbf{f}}_g)^{-1}(h)$.

Remark 5.19. Let (X, r) be a non-degenerate solution. In general, $i_G\colon X \to G(X, r)$ is not injective. For instance, consider $X = \{1, 2, 3, 4\}, \sigma = (12), \tau = (34)$. Then (X, r), $r(x, y) = (\sigma(y), \tau(x))$ is a non-degenerate solutions. But the canonical map $i_G\colon X \to G(X, r)$, $x \mapsto i_G(x)$ is not injective since $r(1, 2) = (1, 1)$ and hence $i_G(1) = i_G(2)$ even if 1 is not 2.

Hence looking at the structure group we may loose information. So recently instead of study the structure group, it can be helpful study the structure monoid, that is the monoid $M(X, r)$ generated by X and such that $xy = f_x(y)g_y(x)$. Then for any solution $i_M : X \to M(X, r)$ is injective. For further information see for example [14, 12].

Bibliography

[1] D. Bachiller, F. Cedó, and E. Jespers, *Solutions of the Yang-Baxter equation*, (2012), arXiv:1503.02814.

[2] D. Bachiller, F. Cedó, and J. Okninski, *Braces and the Yang-Baxter equation*, Comm. Math. Phys., **327** (2014), 101–116.

[3] D. Bachiller, *Study of the algebraic structure of left braces and the Yang- Baxter equation, Phd thesis,* (2016), Universitat Autonoma de Barcelona. Departament de Matematiques, `https://ddd.uab.cat/record/165965.`

[4] D. Bachiller, *Extensions, matched products, and simple braces,* J. Pure Appl. Algebra,**227** (2018), 1670–1691.

[5] R. Baxter, *Eight-vertex model in lattice statistics and one-dimensional anisotropic Heisenberg chain*, Annals of Phys. **76** (1973), no. 1, 1–24.

[6] F. Borceux and D. Bourn, *Mal'cev, Protomodular, Homological and Semi-Abelian Categories*, Kluwer, Mathematics and Its Applications, vol. 566, 2004, 479 pp.

[7] D. Bourn, A. Facchini, M. Pompili, Aspects of the Category SKB of Skew Braces, arXiv:2205.04171v1

[8] D. Bourn and G. Janelidze, *Characterization of protomodular varieties of universal algebras,*Theory Appl. Categ. **11** (2003), No. 6, 143–147.

[9] D. Bourn, *Normal subobjects and abelian objects in protomodular categories*, Journal of Algebra, **228** (2000), 143–164.

[10] D. Bourn, *Normal functors and strong protomodularity*, Theory Appl. Categ. **7**(9) (2000), 206–218.

[11] D. Bourn, *Commutator theory in regular Mal'tsev categories*, in: Galois theory, Hopf algebras, and Semiabelian categories, G.Janelidze, B.Pareigis and W.Tholen editors, Fields Institute Communications, vol. 43, Amer. Math. Soc. (2004), 61–75.

[12] T. Brzeziński, *Towards semi-trusses*, Rev. Roumaine Math. Pures Appl. **63** (2018), 75–89.

[13] S. Burris and H. P. Sankappanavar, *A course in universal algebra*, Graduate Texts in Mathematics, 78. Springer-Verlag, New York-Berlin, 1981.

[14] F. Catino, I. Colazzo, P. Stefanelli, *Semi-braces and the Yang-Baxter equation*, J. Algebra **483** (2017), 163–167.

[15] F. Catino, R. Rizzo, *Regular subgroups of the afine group and radical circle algebra*, Bull. Aust. Math. Soc. **79** (2009), no. 1, 103–107.

[16] V.G. Drinfeld, *Quantum groups,* Proceedings of the International Congress of Mathematicians, Vol 1, 2 (Berkeley, Calif., 1986), Amer. Math. Soc., Providence, RI, 1987, pp. 798–820.

[17] P. Etingof, T. Schedler, and A. Soloviev, *Set-theoretical solutions to the quantum Yang-Baxter equation,* Duke Math. J. **100** (1999), no. 2, 169–209.

[18] A. Facchini, *Algebraic structures from the point of view of complete multiplicative lattices,* arXiv:2201.03295.

[19] S. C. Featherstonhaugh, A. Caranti, and L. N. Childs, *Abelian Hopf Galois structures on prime-power Galois field extensions,* Trans. Amer. Math. Soc. **364** (2012), no. 7, 3675–3684.

[20] M. Gary, *Abelian Objects*, Pac. Journ. of Math., **23**, no. 1, (1967), 69–78.

[21] T. Gateva-Ivanova and M. Van den Bergh, *Semigroups of I-type,* J. Algebra **206** (1998), no. 1, 97–112.

[22] L. Guarnieri and L. Vendramin, *Skew braces and the Yang-Baxter equation,* Math. Comp. **86** (2017), no. 307, 2519–2534.

[23] S.A. Huq, *Commutator, nilpotency and solvability in categories*, Quart. J. Oxford, **19**, (1968), 363–389.

[24] G. Janelidze, L. Márki and W. Tholen, *Semi-abelian categories,* J. Pure Appl. Alg. **168** (2002), 367–386.

[25] G. Janelidze, L. Márki and S. Veldsman, *Commutators for near-rings: Huq $\neq$ Smith,* Algebra Universalis **76** (2016), no. 2, 223–229.

[26] A. Konovalov, A. Smoktunowicz and L. Vendramin, *On skew braces and their ideals,* Exp. Math. **30** (2021), no. 1, 95–104.

[27] J-H. Lu, M. Yan, and Y-C. Zhu, *On the set-theoretical Yang Baxter-Equation*, Duke Math. J., **104** (2000), 1–18.

[28] A. Malt'sev, *On the general theory of algebraic systems,*, Mat. Sb. N. S., **35** (1954), 3–20.

[29] N. Martins-Ferreira, T. Van Der Linden, *A note on the "Smith is Huq" condistion*, Appl. Cat. Struct., **20**, no. 2 (2012), 175–187.

[30] J. Orza, *A construction of the free skew brace*, `https://arxiv.org/abs/2002.12131`.

[31] M. J. Arroyo Paniagua, A. Facchini, *G-Groups and biuniform abelian normal subgroups,* Adv. in Group Theory and Appl., **2** (2016), 79–111.

[32] W. Rump, *Braces, radical rings, and the quantum Yang-Baxter equation*, J. Algebra **307** (2007), 153–170.

[33] W. Rump, *Classification of cyclic braces*, J. Pure Appl. Algebra **209**(3) (2007), 671–685.

[34] J. D. H. Smith, *Mal'tsev Varieties*, Lecture Notes in Math. **554**, Springer-Verlag, Berlin-New York, 1976.

[35] A. Smoktunowicz and L. Vendramin, *On skew braces (with an appendix by N. Byott and L. Vendramin)*, J. Comb. Algebra **2** (2018), no. 1, 47–86.

[36] A. Soloviev, *Non-unitary set-theoretical solutions to the quantum Yang-Baxter equation,* Math. Res. Lett. **7** (2000), no. 5-6, 577–596.

[37] C. N. Yang, *Some exact results for the many-body problem in one dimension with repulsive delta-function interaction,* Phys. Rev. Lett., **19** (1967), 1312–1315,