Advances in Group Theory and Applications
© 2018 AGTA - www.advgrouptheory.com/journal
5 (2018), pp. 33–90 ISSN: 2499-1287
DOI: 10.4399/97888255161422

Left Braces: Solutions of the Yang-Baxter Equation [*]

Ferran Cedó

(*Received Nov. 22, 2017; Accepted Dec. 23, 2017 — Communicated by E. Jespers*)

Dedicated to my mother Agustina Giné Guinjoan

Abstract

This is a survey on the theory of left braces, an algebraic structure introduced by Rump as a generalization of Jacobson radical rings to study non-degenerate involutive set-theoretic solutions of the Yang-Baxter equation.

Mathematics Subject Classification (2010): 20D10, 20D15, 20E22, 20F14, 20F16, 20F18, 20F28, 20F38, 20M10, 16N20, 16T25, 81R50

Keywords: left brace; Yang-Baxter equation; set-theoretic solution; Jacobson radical; holomorph; regular subgroup; monoid of I-type; group of I-type; bijetive 1-cocycle; Garside monoid; Garside group

1 Introduction

In [48] Rump introduced braces as a generalization of Jacobson radical rings to study non-degenerate involutive set-theoretic solutions of the Yang-Baxter equation. In his subsequent papers [47],[49],[50],[51], [52], he initiated the development of the theory of this new structure.

[*] Research partially supported by the grant MINECO MTM2014-53644-P and AGAUR 2017SGR1725

In [21], an equivalent definition of left brace was introduced and used to solve some open problems proposed in [31] on set-theoretic solutions of the Yang-Baxter equation and also to generalize important results in [20],[24] related with the Yang-Baxter equation. Later this definition was generalized to a non-commutative case, the skew left braces [35]. Bachiller in his Ph.D. thesis [2] showed the power of the theory of braces (and skew braces) solving difficult open problems. He also found interesting links with other algebraic structures such as Hopf-Galois extensions. The results of this thesis can be also found in [3],[4],[5],[6],[7]. After this the study and development of the theory of left braces has increased quickly.

2 Basic definitions and properties

Definition 2.1 *A left brace is a set* B *with two operations* $+$ *and* $\cdot$ *such that* $(B, +)$ *is an abelian group,* $(B, \cdot)$ *is a group and*

$$a(b + c) + a = ab + ac, \tag{2.1}$$

for all $a, b, c \in B$. *We call* $(B, +)$ *the additive group and* $(B, \cdot)$ *the multiplicative group of the left brace.*

A right brace is defined similarly, replacing condition (2.1) by

$$(a + b)c + c = ac + bc. \tag{2.2}$$

It is easy to check that in a left brace B, the multiplicative identity 1 of the multiplicative group of B is equal to the neutral element 0 of the additive group of B.

Definition 2.2 *Let* B *be a left brace. The opposite brace of* B *is the right brace* B^{op} *with the same additive group as* B *and multiplicative group equal to the opposite group of the multiplicative group of* B. *The opposite brace of a right brace is defined similarly.*

Thus there is a bijective correspondence between left braces and right braces.

Definition 2.3 *A two-sided brace is a left brace* B *that also is a right brace, in other words, a left brace* B *such that*

$$(a + b)c + c = ac + bc,$$

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

The next result is an easy consequence of the definition of brace, it gives a characterization of two-sided braces and provides many examples.

Proposition 2.4 (Rump) *If* $(B, +, \cdot)$ *is a two-sided brace then* $(B, +, *)$ *is a Jacobson radical ring, where* $*$ *is the operation on* B *defined by*

$$a * b = ab - a - b$$

for $a, b \in B$. *Conversely, if* $(R, +, \cdot)$ *is a Jacobson radical ring then* $(R, +, \circ)$ *is a two-sided brace, where* $a \circ b = ab + a + b$, *for* $a, b \in R$.

Example 2.5 Let A be an abelian additive group. We define a multiplication on A by the rule $ab = a + b$, for all $a, b \in A$. Then $(A, +, \cdot)$ is a two-sided brace. We say that A is a trivial brace. Its corresponding radical ring has zero multiplication.

Let B be a left brace. For every $a \in B$, we define a function

$$\lambda_a \colon B \longrightarrow B$$

by $\lambda_a(b) = ab - a$, for all $b \in B$.

Lemma 2.6 *Let* B *be a left brace.*

(i) $\lambda_a(x + y) = \lambda_a(x) + \lambda_a(y)$, *for all* $a, x, y \in B$, *that is* λ_a *is an automorphism of the additive group of* B.

(ii) $\lambda_a \lambda_b = \lambda_{ab}$, *for all* $a, b \in B$, *that is the map* $\lambda \colon (B, \cdot) \longrightarrow \mathrm{Aut}(B, +)$, *defined by* $\lambda(a) = \lambda_a$ *is a homomorphism of groups.*

Proof — **(i)** Let $a, x, y \in B$. Then

$$\lambda_a(x + y) = a(x + y) - a = ax + ay - a - a = \lambda_a(x) + \lambda_a(y).$$

(ii) Let $a, b, x \in B$. Then

$$\lambda_a \lambda_b(x) = \lambda_a(bx - b) = a(bx - b) - a = abx - ab = \lambda_{ab}(x).$$

The proof is complete. □

Definition 2.7 *Let* B *be a left brace. The lambda map of* B *is the left action*

$$\lambda \colon (B, \cdot) \longrightarrow \mathrm{Aut}(B, +)$$

defined by $\lambda(a)=\lambda_a$ *and* $\lambda_a(b)=ab-a$, *for all* $a,b\in B$.

Definition 2.8 *Let* B *be a left brace. A subbrace of* B *is a subgroup* S *of the additive group of* B *which is also a subgroup of the multiplicative group of* B.

Note that if S is a subbrace of a left brace B, then $\lambda_a(b)\in S$ for all $a,b\in S$.

Definition 2.9 *Let* B *be a left brace. A left ideal of* B *is a subgroup* L *of the additive group of* B *such that* $\lambda_a(b)\in L$ *for all* $a\in B$ *and all* $b\in L$.

Note that if L is a left ideal of a left brace B, then

$$ab^{-1}=-\lambda_{ab^{-1}}(b)+a\in L,$$

for all $a,b\in L$. Therefore L also is a subgroup of the multiplicative group of B, and thus it is a subbrace of B.

Definition 2.10 *Let* B *be a left brace. An ideal of* B *is a normal subgroup* I *of the multiplicative group of* B *such that* $\lambda_a(b)\in I$, *for all* $a\in B$ *and* $b\in I$.

Note that if I is an ideal of a left brace B, then

$$a-b=bb^{-1}a-b=\lambda_b(b^{-1}a)\in I,$$

for all $a,b\in I$. Therefore I also is a subgroup of the additive group of B. Hence every ideal of a left brace B is a left ideal of B.

Definition 2.11 *Let* I *be an ideal of a left brace* B. *Let* B/I *be the quotient group of the multiplicative group of* B *modulo its normal subgroup* I. *Let*

$$c\in B \quad \textit{and} \quad b\in I.$$

Note that

$$cb=c+\lambda_c(b)\in c+I$$

and also

$$c+b=c\lambda_c^{-1}(b)\in cI.$$

Thus $cI=c+I$ *and therefore* G/I *also is the quotient group of the additive group of* B *modulo the additive subgroup* I. *It is easy to see that* $(B/I,+,\cdot)$ *is a left brace. This is called the quotient brace of* B *modulo* I.

Definition 2.12 *Let* B *be a left brace. We define* $B^1 = B^{(1)} = B$ *and for every positive integer* n*, the additive subgroups*

$$B^{n+1} = B * B^n = \langle a * b \mid a \in B,\ b \in B^n \rangle_+$$

and

$$B^{(n+1)} = B^{(n)} * B = \langle a * b \mid a \in B^{(n)},\ b \in B \rangle_+,$$

where $a * b = ab - a - b = (\lambda_a - id_B)(b)$*. Here* $\langle S \rangle_+$ *denotes the subgroup of the additive group of* B *generated by the subset* S *of* B*.*

Note that the operation $*$ defined as above in a left brace B is not associative in general. Thus the two series,

$$B \supseteq B^2 \supseteq \ldots \supseteq B^n \supseteq \ldots$$

and

$$B \supseteq B^{(2)} \supseteq \ldots \supseteq B^{(n)} \supseteq \ldots,$$

do not coincide in general.

Proposition 2.13 (Rump) *Let* B *be a left brace. Then for every positive integer* n*,* B^n *is a left ideal of* B *and* $B^{(n)}$ *is an ideal of* B*.*

Proof — We will prove the result by induction on n. The result is clear for $n = 1$. Let n be a positive integer. Suppose that B^n is a left ideal and $B^{(n)}$ is an ideal of B. Let $a, b \in B$, $c \in B^n$ and $d \in B^{(n)}$. Then

$$\begin{aligned}\lambda_a(b * c) &= \lambda_a(\lambda_b(c) - c) = \lambda_{aba^{-1}}(\lambda_a(c)) - \lambda_a(c) \\ &= (aba^{-1}) * \lambda_a(c) \in B^{n+1},\end{aligned}$$

because $\lambda_a(c) \in B^n$ by the induction hypothesis, and similarly

$$\lambda_a(d * b) = (ada^{-1}) * \lambda_a(b) \in B^{(n+1)},$$

because $ada^{-1} \in B^{(n)}$ by the induction hypothesis. Hence

$$B^{n+1} \quad \text{and} \quad B^{(n+1)}$$

are left ideals of B. Furthermore, if $h \in B^{(n+1)}$, then

$$aha^{-1} = \lambda_a(\lambda_h(a^{-1}) - a^{-1} + h) = \lambda_a(h * a^{-1} + h) \in B^{(n+1)}.$$

Therefore, the result follows by induction. □

Definition 2.14 *Let* B *be a left brace. The socle of* B *is*

$$\begin{aligned}\operatorname{Soc}(B) &= \{a \in B \mid ab = a + b, \text{ \textit{for all} } b \in B\}\\ &= \{a \in B \mid \lambda_a = id_B\} = \operatorname{Ker}(\lambda).\end{aligned}$$

Proposition 2.15 (Rump) *Let* B *be a left brace. Then* $\operatorname{Soc}(B)$ *is an ideal of* B*.*

Proof — Since $\operatorname{Soc}(B) = \operatorname{Ker}(\lambda)$ is a normal subgroup of $(B, \cdot)$, it is sufficient to show that it is invariant by λ_b for all $b \in B$. Let

$$a \in \operatorname{Soc}(B) \quad \text{and} \quad b \in B.$$

Then

$$\lambda_b(a) = ba - b = bab^{-1}b - b = bab^{-1} + b - b = bab^{-1} \in \operatorname{Soc}(B),$$

where the third equality holds because $bab^{-1} \in \operatorname{Soc}(B)$. Thus the result follows. □

Definition 2.16 *Let* B_1 *and* B_2 *be two left braces. A map*

$$f\colon B_1 \longrightarrow B_2$$

is a homomorphism of left braces if

$$f(a+b) = f(a) + f(b)$$

and

$$f(ab) = f(a)f(b),$$

for all $a, b \in B_1$*. The kernel of* f *is* $\operatorname{Ker}(f) = \{a \in B_1 \mid f(a) = 1\}$.

Let

$$f\colon B_1 \longrightarrow B_2$$

be a homomorphism of left braces. Note that $\operatorname{Ker}(f)$ is a normal subgroup of the multiplicative group of the left brace B_1. Let

$$a \in B_1 \quad \text{and} \quad b \in \operatorname{Ker}(f).$$

Then

$$f(\lambda_a(b)) = f(ab - a) = f(a)f(b) - f(a) = f(a) - f(a) = 0 = 1.$$

Hence $\mathrm{Ker}(f)$ is an ideal of B_1. Note also that $\mathrm{Im}(f) = \{f(a) \mid a \in B_1\}$ is a subbrace of B_2. If f is bijective, we say that f is an isomorphism. Two left braces B_1, B_2 are isomorphic if there is an isomorphism

$$f\colon B_1 \longrightarrow B_2.$$

The notation $B_1 \simeq B_2$ will mean that the left braces B_1 and B_2 are isomorphic.

Let B be a left brace and let I be an ideal of B. Note that we have a natural short exact sequence of left braces

$$0 \longrightarrow I \longrightarrow B \longrightarrow B/I \longrightarrow 0.$$

We say that B is an extension of the left brace I by the left brace B/I.

In the context of Proposition 2.4 we now show that ideals of a two-sided brace coincide with the ideals of the corresponding Jacobson radical ring.

Let R be a Jacobson radical ring. Let I be an ideal of the ring R. We shall see that I is an ideal of the two-sided brace $(R, +, \circ)$. Let $x \in I$ and $a, a' \in R$ be elements such that $a \circ a' = a' \circ a = 0$, that is a' is the inverse of a in the group $(R, \circ)$. We have

$$\begin{aligned} a \circ x \circ a' &= (ax + a + x)a' + ax + a + x + a' \\ &= axa' + aa' + xa' + ax + a + x + a' \\ = axa' + xa' + ax + x + a \circ a' &= axa' + xa' + ax + x \in I. \end{aligned}$$

Hence I is a normal subgroup of $(R, \circ)$. Furthermore

$$\lambda_a(x) = a \circ x - a = ax + x + a - a = ax + x \in I.$$

Thus I is an ideal of the left brace R.

Conversely, let J be an ideal of the brace R. In order to prove that J is an ideal of the ring R it is enough to show that $ax, xa \in J$ for all $x \in J$ and all $a \in R$. Let $x \in J$ and $a \in R$. Let $a' \in R$ be the inverse of a in the group $(R, \circ)$. We have

$$ax = a \circ x - a - x = \lambda_a(x) - x \in J$$

and

$$xa = x \circ a - a - x = \lambda_a(a' \circ x \circ a) - x \in J.$$

Therefore J indeed is an ideal of the ring R.

Note also that if I is an ideal of the radical ring R, then the ring R/I is the radical ring corresponding to the quotient brace of the two-sided brace R modulo I.

As in group theory one can prove the following isomorphism theorems.

Theorem 2.17 (First isomorphism theorem) *Given any homomorphism of left braces* $f\colon B_1 \longrightarrow B_2$*, there exists a unique isomorphism*

$$\widetilde{f}\colon B_1/\operatorname{Ker}(f) \longrightarrow \operatorname{Im}(f)$$

such that the diagram

$$\begin{tikzcd}
B_1 \arrow[r, "f"] \arrow[d, "\pi"'] & B_2 \\
B_1/\mathit{Ker}(f) \arrow[r, "\widetilde{f}"] & \mathit{Im}(f) \arrow[u, "\iota"']
\end{tikzcd}$$

commutes, that is $f = \iota \circ f \circ \pi$*, where* π *is the natural homomorphism and* ι *is the inclusion mapping.*

Theorem 2.18 (Second isomorphism theorem) *Let* B *be a left brace, let* H *be a subbrace of* B*, and let* N *be an ideal of* B*. Then,* HN *is a subbrace of* B*,* $H \cap N$ *is an ideal of* H *and* $HN/N \simeq H/(H \cap N)$*.*

Theorem 2.19 (Third isomorphism theorem) *Given a left brace* B *and an ideal* N *of* B*, there is a natural bijection between the subbraces of* B *containing* N *and the subbraces of* B/N*:* $H \leftrightarrow H/N$*, and if* H *is and ideal of* B *containing* N*, then the isomorphism*

$$(G/N)/(H/N) \simeq G/H.$$

holds.

3 Construction of left braces

Let B_1, B_2 be two left braces. Then it is easy to see that the direct product $B_1 \times B_2$ of the multiplicative groups of the left braces B_1 and B_2 with the sum defined componentwise is a left brace called the direct product of the braces B_1 and B_2.

We shall construct the semidirect product of two left braces as introduced by Rump in [51]. Let B_1, B_2 be left braces. Let

$$\eta \colon B_2 \longrightarrow \mathrm{Aut}(B_1)$$

be a homomorphism of groups from the multiplicative group of B_2 to the group of automorphisms of the left brace B_1 (see Definition 2.16).

Consider the semidirect product $B_1 \rtimes B_2$ of the multiplicative groups B_1 and B_2 via η. Define in $B_1 \rtimes B_2$ a sum by

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$

for $a_1, a_2 \in B_1$ and $b_1, b_2 \in B_2$. It is clear that $(B_1 \rtimes B_2, +)$ is an abelian group. We prove that the group $B_1 \rtimes B_2$ with this sum is a left brace. Indeed, let $a_1, a_2, a_3 \in B_1$ and $b_1, b_2, b_3 \in B_2$. Then

$$\begin{aligned}
&(a_1,b_1)((a_2,b_2)+(a_3,b_3))+(a_1,b_1)\\
&= (a_1,b_1)(a_2+a_3,b_2+b_3)+(a_1,b_1)\\
&= (a_1\eta(b_1)(a_2+a_3),b_1(b_2+b_3))+(a_1,b_1)\\
&= (a_1(\eta(b_1)(a_2)+\eta(b_1)(a_3)),b_1(b_2+b_3))+(a_1,b_1)\\
&= (a_1(\eta(b_1)(a_2)+\eta(b_1)(a_3))+a_1,b_1(b_2+b_3)+b_1)\\
&= (a_1\eta(b_1)(a_2)+a_1\eta(b_1)(a_3),b_1b_2+b_1b_3)\\
&= (a_1\eta(b_1)(a_2),b_1b_2)+(a_1\eta(b_1)(a_3),b_1b_3)\\
&= (a_1,b_1)(a_2,b_2)+(a_1,b_1)(a_3,b_3).
\end{aligned}$$

Hence, $B_1 \rtimes B_2$ is a left brace. We call this left brace the semidirect product of the left braces B_1 and b_2, via η.

We shall construct the wreath product of two left braces. Let B_1, B_2 be two left braces. Suppose that the multiplicative group of B_2 is a group of permutations of a set S. We have that

$$H = \{f \colon S \longrightarrow B_1 \mid |\{s \in S \mid f(s) \neq 1\}| < \infty\}$$

is a left brace with the operations

$$(f_1 \cdot f_2)(s) = f_1(s) \cdot f_2(s)$$

and

$$(f_1 + f_2)(s) = f_1(s) + f_2(s),$$

for all $f_1, f_2 \in H$ and $s \in S$. Consider the action of $(B_2, \cdot)$ on H given by the homomorphism

$$\sigma\colon (B_2, \cdot) \longrightarrow \mathrm{Aut}(H, +, \cdot)$$

defined by $\sigma(b)(f)(s) = f(b^{-1}(s))$, for all $b \in B_2$, $f \in H$ and $s \in S$. Let $b_1, b_2 \in B_2$, $f_1, f_2 \in H$ and $s \in S$. Note that

$$\begin{aligned}\sigma(b_1)(f_1 \cdot f_2)(s) &= (f_1 \cdot f_2)(b_1^{-1}(s)) = (f_1)(b_1^{-1}(s)) \cdot (f_2)(b_1^{-1}(s))\\ &= \sigma(b_1)(f_1)(s) \cdot \sigma(b_1)(f_2)(s) = (\sigma(b_1)(f_1) \cdot \sigma(b_1)(f_2))(s),\end{aligned}$$

$$\begin{aligned}\sigma(b_1)(f_1 + f_2)(s) &= (f_1 + f_2)(b_1^{-1}(s)) = (f_1)(b_1^{-1}(s)) + (f_2)(b_1^{-1}(s))\\ &= \sigma(b_1)(f_1)(s) + \sigma(b_1)(f_2)(s) = (\sigma(b_1)(f_1) + \sigma(b_1)(f_2))(s)\end{aligned}$$

and

$$\begin{aligned}\sigma(b_1 b_2)(f_1)(s) &= f_1(b_2^{-1} b_1^{-1}(s)) = \sigma(b_2)(f_1)(b_1^{-1}(s))\\ &= \sigma(b_1)(\sigma(b_2)(f_1))(s).\end{aligned}$$

Thus σ is a well-defined action.

The wreath product $B_1 \wr B_2$ of the left braces B_1 and B_2 is a left brace which is the semidirect product of left braces $H \rtimes B_2$ via σ.

Note that given two left braces B_1, B_2, we may consider the multiplicative group B_2 as a group of permutations on itself by left multiplication. The corresponding wreath product $B_1 \wr B_2$ is called the regular wreath product of B_1 and B_2.

The matched product of two left braces was introduced in [5] as a natural extension of the matched product (or bicrossed product) of groups [41]. In [8] the iterated matched product of left ideals is constructed. We will call this simply the matched product of left braces.

Theorem 3.1 (see [8], Theorem 2.4) *Let* $B_1, \dots, B_n$ *be left braces with* $n \geqslant 2$. *Let*

$$\alpha^{(j,i)}\colon (B_j, \cdot) \longrightarrow \mathrm{Aut}(B_i, +)$$

be actions satisfying the following conditions.

(1) *The equality*

$$\alpha_b^{(j,k)}\alpha^{(i,k)}_{\alpha^{(j,i)}_{b^{-1}}(a)}=\alpha_a^{(i,k)}\alpha^{(j,k)}_{\alpha^{(i,j)}_{a^{-1}}(b)},$$

holds for all $a\in B_i$ *and* $b\in B_j$, *and for all* $i,j,k\in\{1,\dots,n\}$, *where* $\alpha^{(i,j)}(a)=\alpha_a^{(i,j)}$.

(2) *For every* $i\in\{1,\dots,n\}$, $\alpha^{(i,i)}$ *is the lambda map of* B_i, *that is,* $\alpha_x^{(i,i)}(y)=xy-x$, *for all* $x,y\in B_i$.

Then there exists a unique structure of left brace on $B_1\times\dots\times B_n$ *such that*

(i) *the equality* $(a_1,\dots,a_n)+(b_1,\dots,b_n)=(a_1+b_1,\dots,a_n+b_n)$ *holds for all* $a_i,b_i\in B_i$ *and* $i=1,\dots,n$;

(ii) $\lambda_{(0,\dots,0,a_i,0,\dots,0)}(0,\dots,0,b_j,0,\dots,0)=(0,\dots,0,\alpha_{a_i}^{(i,j)}(b_j),0,\dots,0)$, *for all* $a_i\in B_i$, $b_j\in B_j$ *and all* $i,j\in\{1,\dots,n\}$.

Furthermore, each $\{0\}\times\dots\times\{0\}\times B_i\times\{0\}\times\dots\times\{0\}$ *is a left ideal of this left brace. We denote this left brace by* $B_1\bowtie\dots\bowtie B_n$ *and we say that it is the matched product of the left braces* $B_1,\dots,B_n$ *via the actions* $\alpha^{(i,j)}$.

Remark 3.2 As in group theory, we also have the concepts of inner direct product, inner semidirect product and inner matched product.

Let B be a left brace. If $I_1,\dots,I_n$ are ideals of B such that the additive group of B is the direct sum of the additive groups of $I_1,\dots,I_n$, we say that B is the inner direct product of $I_1,\dots,I_n$. In this case,

$$B\simeq I_1\times\dots\times I_n.$$

If I is an ideal of B and L is a left ideal of B such that the additive group of B is the direct sum of the additive groups of I and L, then we say that B is the inner semidirect product of I and L. In this case

$$B\simeq I\rtimes L,$$

via the conjugation action. If the additive group of B is the direct sum of the additive groups of left ideals $L_1,L_2,\dots,L_n$, then we say that B is the inner matched product of $L_1,L_2,\dots,L_n$. In this case

$$B\simeq L_1\bowtie L_2\bowtie\dots\bowtie L_n,$$

via the actions $\alpha^{(i,j)}\colon (L_i,\cdot) \to \mathrm{Aut}(L_j,+)$ defined by $\alpha^{(i,j)}(a) = \alpha_a^{(i,j)}$ and $\alpha_a^{(i,j)}(b) = \lambda_a(b)$, for all $a \in L_i$ and $b \in L_j$.

We finish this section with another important construction of left braces, the asymmetric product of two left braces introduced by Catino, Colazzo and Stefanelli in [15].

Let A_1 and A_2 be two (additive) abelian groups. Recall that a (normalized) symmetric 2-cocyle on A_1 with values in A_2 is a map

$$b\colon A_1 \times A_1 \longrightarrow A_2$$

such that

(i) $b(0,0) = 0$;

(ii) $b(a_1,a_2) = b(a_2,a_1)$;

(iii) $b(a_1+a_2,a_3) + b(a_1,a_2) = b(a_1,a_2+a_3) + b(a_2,a_3)$, for all $a_1,a_2,a_3 \in A_1$.

As a consequence, we get that $b(a,0) = b(0,a) = 0$, for all $a \in A_1$.

Theorem 3.3 (see [15], Theorem 3) *Let* B_1 *and* B_2 *be two left braces. Let*

$$b\colon B_1 \times B_1 \longrightarrow B_2$$

be a symmetric 2-cocycle on $(B_1,+)$ *with values in* $(B_2,+)$, *and let*

$$\alpha\colon (B_2,\cdot) \longrightarrow \mathrm{Aut}(B_1,+,\cdot)$$

be a homomorphism of groups such that

$$s\cdot b(t_2,t_3)+b(t_1\cdot\alpha_s(t_2+t_3),t_1)=b(t_1\cdot\alpha_s(t_2),t_1\cdot\alpha_s(t_3))+s, \quad (3.1)$$

where $\alpha_s = \alpha(s)$, *for all* $s \in B_2$ *and* $t_1,t_2,t_3 \in B_1$. *Then the addition and multiplication over* $B_1 \times B_2$ *given by*

$$(t_1,s_1) + (t_2,s_2) = (t_1+t_2, s_1+s_2+b(t_1,t_2)),$$

$$(t_1,s_1)\cdot(t_2,s_2) = (t_1\cdot\alpha_{s_1}(t_2), s_1\cdot s_2),$$

define a structure of left brace on $B_1 \times B_2$. *We call this left brace the asymmetric product of* B_1 *by* B_2 *(via* b *and* α*) and denote it by* $B_1 \rtimes_\circ B_2$.

Note that the lambda map of $B_1 \rtimes_\circ B_2$ is defined by

$$\lambda_{(t_1,s_1)}(t_2,s_2) = \left(\lambda_{t_1}\alpha_{s_1}(t_2), \lambda_{s_1}(s_2) - b(\lambda_{t_1}\alpha_{s_1}(t_2), t_1)\right), \qquad (3.2)$$

and its socle is

$$\begin{aligned} &\mathrm{Soc}(B_1 \rtimes_\circ B_2)\\ &= \{(t,s) \mid \lambda_s = \mathrm{id}_{B_2},\ \lambda_t \circ \alpha_s = \mathrm{id}_{B_1},\ b(t,t') = 0 \text{ for all } t' \in B_1\}. \end{aligned}$$

Moreover, the subset $B_1 \times \{0\}$ is a normal subgroup of $(B_1 \rtimes_\circ B_2, \cdot)$, and $\{0\} \times B_2$ is a left ideal of $B_1 \rtimes_\circ B_2$.

A particular case of this theorem is when we assume that b is a symmetric bilinear form. In this case, conditions (i)–(iii) are automatic, and condition (3.1) becomes

$$\lambda_s(b(t_2,t_3)) = b(\lambda_{t_1}\alpha_s(t_2), \lambda_{t_1}\alpha_s(t_3)),$$

which is equivalent to the two conditions:

$$\lambda_s(b(t_2,t_3)) = b(\alpha_s(t_2), \alpha_s(t_3)), \qquad (3.3)$$

$$b(t_2,t_3) = b(\lambda_{t_1}(t_2), \lambda_{t_1}(t_3)), \qquad (3.4)$$

for all $s \in B_2$ and $t_1, t_2, t_3 \in B_1$.

4 Left nilpotent, right nilpotent and solvable left braces

Left nilpotent left braces and right nilpotent left braces were introduced in [17]. Solvable left braces were introduced in [9].

Definition 4.1 *Let B be a left brace. We say that B is left nilpotent if there exists a positive integer n such that $B^n = \{0\}$. A left brace B is right nilpotent if there exists a positive integer such that $B^{(n)} = \{0\}$ (see Definition 2.12).*

Remark 4.2 Smoktunowicz in [55], Theorem 1, proved that a finite left brace B is left nilpotent if and only if its multiplicative group $(B,\cdot)$ is nilpotent. In particular, every left brace of order a power of a prime is left nilpotent.

Note that if B is a right nilpotent nonzero left brace, then there exists a positive integer n such that $B^{(n)} \neq \{0\}$ and $B^{(n+1)} = \{0\}$. Let

$$a \in B^{(n)} \quad \text{and} \quad b \in B.$$

We have that $ab - a - b = a * b = 0$ and thus $ab = a + b$. Hence $a \in \mathrm{Soc}(B)$. Therefore $B^{(n)} \subseteq \mathrm{Soc}(B)$. In particular, $\mathrm{Soc}(B) \neq \{0\}$.

There are many examples of nonzero left braces of order a power of a prime with zero socle (see for example [3],[8],[15]). Therefore these are examples of left nilpotent left braces which are not right nilpotent.

Consider the trivial left braces $K = \mathbb{Z}/(2) \times \mathbb{Z}/(2)$ and $\mathbb{Z}/(3)$. Let

$$\alpha\colon \mathbb{Z}/(3) \longrightarrow \mathrm{Aut}(K, +)$$

be the action defined by $\alpha(x) = \alpha_x$ and

$$\alpha_x(y, z) = (y, z) \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^x,$$

for all $x \in \mathbb{Z}/(3)$ and all $y, z \in \mathbb{Z}/(2)$. Then the semidirect product

$$B_3 = K \rtimes \mathbb{Z}/(3)$$

is a left brace which is not left nilpotent. Now we have

$$\begin{aligned} &((y_1, z_1), x_1) * ((y_2, z_2), x_2) \\ &= ((y_1, z_1), x_1) \cdot ((y_2, z_2), x_2) - ((y_1, z_1), x_1) - ((y_2, z_2), x_2) \\ &= ((y_1, z_1) + \alpha_{x_1}(y_2, z_2), x_1 + x_2) - ((y_1, z_1), x_1) - ((y_2, z_2), x_2) \\ &= (\alpha_{x_1}(y_2, z_2) - (y_2, z_2), 0), \end{aligned}$$

for all $y_i, z_i \in \mathbb{Z}/(2)$ and all $x_i \in \mathbb{Z}/(3)$. Hence $B_3^{(2)} = K \times \{0\}$ and, since

$$((y_1, z_1), 0) * ((y_2, z_2), x_2) = ((0, 0), 0),$$

we get that $B_3^{(3)} = \{0\}$. Therefore B_3 is right nilpotent.

Recall that a trivial brace is a left brace B such that any $a, b \in B$ satisfy $a \cdot b = a + b$. We also say that B has trivial structure. Thus B is a trivial brace if and only if $B^2 = \{0\}$.

Let B be a left brace. Note that $B^2 = B^{(2)}$ is an ideal of B by Proposition 2.13. Observe that B/B^2 has trivial brace structure because

$$a \cdot b - a - b = a * b \in B^2.$$

Moreover, if I is an ideal of B, B/I has trivial structure if and only if $B^2 \subseteq I$.

Definition 4.3 *A solvable left brace is any left brace B which has a series*

$$0 = B_0 \subseteq B_1 \subseteq \ldots \subseteq B_m = B$$

such that B_i is an ideal of B_{i+1}, and such that B_{i+1}/B_i is a trivial brace for any $i \in \{0, 1, \ldots, m-1\}$.

Using the same arguments as in group theory, one can prove the following results.

Proposition 4.4 *Any subbrace, and any quotient of a left (right) nilpotent left brace is left (right) nilpotent.*

Proposition 4.5

(a) *Define $d_1(B) = B^2$, and $d_{i+1}(B) = d_i(B)^2$ for every positive integer i. Then, B is a solvable brace if and only if $d_k(B) = 0$ for some k.*

(b) *Let B be a left brace, and let I be an ideal of B. If I and B/I are solvable left braces, then B is also solvable.*

(c) *Any subbrace, and any quotient of a solvable left brace is solvable.*

Remark 4.6 Note that for every left brace B,

$$d_n(B) \subseteq B^{n+1} \cap B^{(n+1)}.$$

Hence every left nilpotent left brace is solvable, and every right nilpotent left brace is solvable. We have seen in Remark 4.2 that there exists a finite left nilpotent left brace B_1 which is not right nilpotent, and there exists a finite right nilpotent left brace B_2 which is not left nilpotent. Hence the left brace $B_1 \times B_2$ is neither left nilpotent nor right nilpotent. But clearly $B_1 \times B_2$ is solvable.

5 Simple left braces

In this section we will present some techniques to construct finite simple left braces. For the complete list of known simple finite left braces see [5],[8],[9].

Definition 5.1 *A nonzero left brace* B *is said to be simple if* $\{0\}$ *and* B *are the only ideals of* B*.*

To study finite left braces, the next result is fundamental. It is a consequence of [29], Theorem 2.15, and [24], Theorem 2.1.

Theorem 5.2 (Etingof, Schedler, Soloviev) *Let* B *be a finite left brace. Then the multiplicative group of* B *is solvable.*

Proof — Let B be a finite left brace. Note that the Sylow subgroups of the additive group of B are left ideals of B. In fact, if

$$|B| = p_1^{m_1} \dots p_n^{m_n},$$

where p_i are the different prime divisors of the order of B, and B_{p_i} is the Sylow p_i-subgroup of the additive group of B, then B_{p_i} also is a Sylow p_i-subgroup of the multiplicative group of B and

$$B_{p_i} + B_{p_j} = B_{p_i} B_{p_j} = B_{p_j} B_{p_i},$$

for all $i \neq j$. Thus $B_{p_1}, \dots, B_{p_n}$ form a Sylow system for the multiplicative group of B. Hence, by Satz VI.2.3 of [38], the multiplicative group of B is solvable. □

As a consequence of [48], Proposition 8, we have the following result.

Theorem 5.3 (Rump) *Let* B *be a nonzero finite left brace of order a power of a prime* p*. Then* B^2 *is a proper ideal of* B*.*

Recall that the Sylow subgroups of a finite nilpotent group are normal subgroups. In particular, if B is a finite left brace with nilpotent multiplicative group, then the Sylow subgroups of the additive group are ideals of B. Therefore we have the following result.

Corollary 5.4 (Rump) *Let* B *be a finite simple left brace. If the multiplicative group of* B *is nilpotent, then* B *is a trivial brace of prime order.*

The first examples of finite non-trivial simple left braces were constructed by Bachiller in [5]. The smallest of these is a simple left brace with multiplicative group isomorphic to the symmetric group of degree 4, Sym_4, and additive group isomorphic to $(\mathbb{Z}/(2))^3 \times \mathbb{Z}/(3)$.

We know that every finite left brace is the inner matched product of the Sylow subgroups of its additive group, since these are left ideals. Thus a natural way to construct finite simple left braces is to choose suitable finite left braces $B_1, \dots, B_n$ of orders $p_1^{m_1}, \dots, p_n^{m_n}$, where $p_1, \dots, p_n$ are n distinct primes, and to choose suitable actions

$$\alpha^{(j,i)} \colon (B_j, \cdot) \longrightarrow \mathrm{Aut}(B_i, +)$$

satisfying the conditions in Theorem 3.1, such that the matched product $B_1 \bowtie \dots \bowtie B_n$ is simple. This is the approach to construct finite simple left braces in [5],[8].

The simple left braces constructed in [5] have order

$$p_1 p_2^{k(p_1-1)+1},$$

for any positive integer k, and any pair of different primes p_1 and p_2 with $p_2 | (p_1 - 1)$. Every such left brace is a matched product of a trivial brace of order p_1 and a left brace, that we call of Hegedűs type, of order $p_2^{k(p_1-1)+1}$.

Let s be an integer greater than 1. Let

$$p_1, p_2, \dots, p_s$$

be different prime numbers and let $r_1, r_2, \dots, r_s$ be positive integers. Assume that $p_1, \dots, p_{s-1}$ are odd. If $p_s = 2$, then we also assume that $r_s = 1$. Let $0 \leqslant r_i' \leqslant r_i$. Then in [8] a simple left brace is constructed with additive group

$$(\mathbb{Z}/(p_1^{r_1}))^{p_1^{r_1'}(p_2^{r_2}-1)+1} \times \dots \times (\mathbb{Z}/(p_{s-1}^{r_{s-1}}))^{p_{s-1}^{r_{s-1}'}(p_s^{r_s}-1)+1}$$
$$\times (\mathbb{Z}/(p_s^{r_s}))^{p_s^{r_s'}(p_1^{r_1}-1)+1}.$$

It is a matched product of left braces of Hegedűs type.

The first example of left braces of Hegedűs type comes from [37], where Hegedűs constructed regular subgroups of the affine group $\mathrm{AGL}(n, p)$ containing only the trivial translation. In [16] Catino and Rizzo showed that these regular subgroups can be viewed as left braces. This gives the first example of left braces of Hegedűs type contained in the folowing result (see [5]).

For every prime p, we denote by $\mathbb{F}_p$ the field of p elements.

Theorem 5.5 (Hegedűs, Catino, Rizzo) *Let p be a prime number, and let n be a positive integer. Assume that we are given a quadratic form Q on $\mathbb{F}_p^n$, and an element f of order p of the orthogonal group of Q. Then, the abelian group $\mathbb{F}_p^{n+1}$ with lambda map given by*

$$\lambda_{(\vec{x},x_{n+1})}(\vec{y},y_{n+1}) := (f^{q(\vec{x},x_{n+1})}(\vec{y}), y_{n+1} + b(\vec{x}, f^{q(\vec{x},x_{n+1})}(\vec{y}))),$$

for $\vec{x},\vec{y} \in \mathbb{F}_p^n$ and $x_{n+1}, y_{n+1} \in \mathbb{F}_p$, defines a structure of left brace, where

$$q(\vec{x},x_{n+1}) := x_{n+1} - Q(\vec{x})$$

and b is the associated bilinear form

$$b(\vec{x},\vec{y}) := Q(\vec{x}+\vec{y}) - Q(\vec{x}) - Q(\vec{y}).$$

Moreover, if Q is non-degenerate, then the socle of this brace is equal to zero.

This was generalized from the field $\mathbb{F}_p$ to the case of the local rings $\mathbb{Z}/(p^r)$ in [8], Theorem 3.1, obtaining the left brace of Hegedűs type with additive group $(\mathbb{Z}/(p^r))^{n+1}$, denoted by

$$H(p^r, n, Q, f),$$

where Q is a quadratic form over $(\mathbb{Z}/(p^r))^n$ (considered as a free module over the ring $\mathbb{Z}/(p^r)$) and f is an element of order $p^{r'}$ in the orthogonal group of Q, for some $0 \leqslant r' \leqslant r$, and

$$\lambda_{(\vec{x},x_{n+1})}(\vec{y},y_{n+1}) := (f^{q(\vec{x},x_{n+1})}(\vec{y}), y_{n+1} + b(\vec{x}, f^{q(\vec{x},x_{n+1})}(\vec{y}))),$$

for $\vec{x},\vec{y} \in (\mathbb{Z}/(p^r))^n$ and $x_{n+1}, y_{n+1} \in \mathbb{Z}/(p^r)$, where

$$q(\vec{x},x_{n+1}) := x_{n+1} - Q(\vec{x})$$

and b is the associated bilinear form

$$b(\vec{x},\vec{y}) := Q(\vec{x}+\vec{y}) - Q(\vec{x}) - Q(\vec{y}).$$

Note that these left braces are rather complicated and it seems difficult to find actions satisfying the conditions in Theorem 3.1. Thus we should understand better the structure of these finite simple left braces.

On the other hand Catino, Colazzo and Stefanelli in [15] showed that the left brace of Hegedűs type $H(p, n, Q, f)$ is in fact the asymmetric product of two trivial braces,

$$(\mathbb{Z}/(p))^n \rtimes_\circ \mathbb{Z}/(p)$$

via the action

$$\alpha\colon \mathbb{Z}/(p) \longrightarrow \mathrm{Aut}((\mathbb{Z}/(p))^n),$$

defined by $\alpha(z)(\vec{x}) = f^z(\vec{x})$, and the bilinear form b associated to $-Q$. This was generalized in [9] showing that $H(p^r, n, Q, f)$ is the asymmetric product of two trivial braces

$$(\mathbb{Z}/(p^r))^n \rtimes_\circ \mathbb{Z}/(p^r)$$

via the action

$$\alpha\colon \mathbb{Z}/(p^r) \longrightarrow \mathrm{Aut}((\mathbb{Z}/(p^r))^n),$$

defined by $\alpha(z)(\vec{x}) = f^z(\vec{x})$, and the bilinear form b associated to $-Q$.

By using these ideas, in [9], Theorem 6.2, it is shown that the finite simple left braces constructed in [8], Theorem 3.6, are asymmetric products of two trivial braces. Furthermore, the examples of finite simple left braces constructed in [5] can be generalized using the asymmetric product, obtaining in [9] a new family of finite left braces of the form

$$((\mathbb{Z}/(p))^n \rtimes A) \rtimes_\circ \mathbb{Z}/(p),$$

where A is any finite trivial brace and p is a prime such that $p|(q-1)$ for all prime divisors q of the order of A.

Example 5.6 (Bachiller) This is the first example of non-trivial simple left brace constructed by Bachiller, but presented as an asymmetric product.

Let $A = \mathbb{Z}/(3)$. Let $\mathbb{F}_2$ be the field of two elements. Consider the ring $R = \mathbb{F}_2[x]/(x^2+x+1)$, and denote $\xi := \overline{x} \in R$. Let $c \in \mathrm{Aut}(R, +)$ be defined by

$$c(r) = \xi r,$$

for all $r \in R$. Let $f \in \mathrm{Aut}(R, +)$ be defined by

$$f(r(\xi)) = r(\xi^2),$$

for all $r(\xi) \in R$. Note that

$$fc(r(\xi)) = f(\xi r(\xi)) = \xi^2 r(\xi^2) = c^2 f(r(\xi)),$$

for all $r(\xi) \in R$. Hence $fc = c^2 f$.

Since the characteristic polynomial of c is $x^2 + x + 1 \in \mathbb{F}_2[x]$, $c - \mathrm{id}$ is invertible.

Let $b \colon R \times R \longrightarrow \mathbb{F}_2$ be the unique bilinear form such that the matrix of b with respect to the basis $\mathcal{B} = (1, \xi)$ is

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{F}_2).$$

Hence b is non-degenerate. Note that the matrices of f and c with respect the basis $\mathcal{B}$ are

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

respectively. Since

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

we have that f and c are in the orthogonal group of b.

Let $T = R \rtimes A$ be the semidirect product of the trivial braces R and A via the action

$$\beta \colon A \longrightarrow \mathrm{Aut}(R, +)$$

defined by $\beta_a(u) = c^a(u)$, where $\beta(a) = \beta_a$, for all $a \in \mathbb{Z}/(3)$ and all $u \in R$.

We define the map α: $(\mathbb{Z}/(2), +) \longrightarrow \mathrm{Aut}(T, +, \cdot)$ by

$$\alpha_\mu(u, a) = (f^\mu(u), 2^\mu a),$$

where $\alpha(\mu) = \alpha_\mu$, for all $\mu \in \mathbb{F}_2$, all $a \in \mathbb{Z}/(3)$ and all $u \in R$. (here we have $\alpha_\mu \in \mathrm{Aut}(T, +, \cdot)$ because $fc = c^2 f$).

Let $b' \colon T \times T \longrightarrow \mathbb{F}_2$ be the symmetric bilinear form defined by

$$b'((u,a),(v,a')) = b(u,v),$$

for all $a, a' \in \mathbb{Z}/(3)$ and all $u, v \in R$. Since f and c are in the orthogonal group of b, the conditions (3.3) and (3.4) are satisfied by b' and α. Hence we can form the asymmetric product $B = T \rtimes_\circ \mathbb{F}_2$ of T by $\mathbb{F}_2$, via b' and α. Since $c - \mathrm{id}$ is invertible, one can check that B is a simple left brace.

Note that the multiplicative groups of all the finite simple left braces presented above are solvable groups of derived length at most 3. In [9], Theorem 5.3, using the asymmetric product and the wreath product of left braces, finite simple left braces with multiplicative group of arbitrary derived length are constructed.

Using the following result, which is a particular case of Theorem 2.6 in [8], one can construct more finite simple left braces.

Theorem 5.7 (Bachiller, Cedó, Jespers, Okniński) *Let B be a matched product of two finite simple left braces B_1, B_2 of relatively prime orders via the actions*

$$\alpha^{(j,i)} \colon (B_j, \cdot) \longrightarrow \mathrm{Aut}(B_i, +),, \quad (i, j \in \{1, 2\}).$$

Then the left brace B is simple if and only if $\alpha^{(1,2)}$ and $\alpha^{(1,2)}$ are nontrivial.

6 Extensions of left braces

One way to classify left braces is to split this problem in two steps. First, to classify the simple left braces, and second, to develop a general theory of extensions of braces. In Section 5, we have seen what is known about simple left braces. In this section, we will see what is known about the theory of extensions of left braces.

Definition 6.1 *Let I and H be two left braces. An extension of I by H is a short exact sequence of left braces*

$$0 \longrightarrow I \longrightarrow B \longrightarrow H \longrightarrow 0. \tag{6.1}$$

A general theory of extensions has not been developed yet. The first result of extensions appears in [11], Corollary D, an it was translated to the language of left braces in [3], Theorem 2.1. This result characterizes the extensions (6.1) of left braces such that the image of I in B is an ideal of B contained in Soc(B). Note that in this case I should be a trivial brace.

Another approach using linear cycle sets is given in [43]. In [46] Rump introduced cycle sets and linear cycle sets. Recall that a cycle set is a set X equipped with a binary operation $\cdot$ such that

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

for all $x, y, z \in X$, and for every $x \in X$, the map $y \mapsto x \cdot y$ is a bijection from X to X. A linear cycle set is an abelian group $(A, +)$ with another operation $\cdot$ such that $(A, \cdot)$ is a cycle set and:

(1) $(a + b) \cdot c = (a \cdot b) \cdot (a \cdot c)$,

(2) $a \cdot (b + c) = a \cdot b + a \cdot c$,

for all $a, b, c \in A$. In [48], Proposition 5, Rump showed that there is a bijective correspondence between left braces and linear cycle sets. In fact, note that in a linear cycle set A we can define an operation $\circ$ by the rule $a \circ b = {}^{a}b + a$, where $a \cdot ({}^{a}b) = b$. Then $(A, +, \circ)$ is a left brace. Conversely, if B is a left brace then we can define an operation $\diamond$ by the rule $a \diamond b = \lambda_a^{-1}(b)$. Then $(B, +, \diamond)$ is a linear cycle set. The central extensions defined in [43] (Definition 5.5) corresponds to extensions of left braces (6.1) such that the image of I in B is an ideal of B contained in $\mathrm{Soc}(B) \cap Z(B)$, where $Z(B)$ is the center of the multiplicative group of B. Thus this is a particular case of the extensions of left braces of [11],[3]. The advantage of [43] is its interpretation as 2-cohomological classes of a certain cohomology.

In [5] (Theorem 3.3) Bachiller characterizes the extensions (6.1) such that I is a trivial brace. This generalizes [3], Theorem 2.1. It would be interesting to know whether a cohomology theory can be constructed to characterize this type of extensions.

7 Multiplicative group of finite left braces

By Theorem 5.2, the multiplicative group of every finite left brace is solvable. Implicitly in [29] and explicitly in [24] it is asked: is every finite solvable group isomorphic to the multiplicative group of a finite left brace? In [4] Bachiller answered this question in the negative by showing that for infinitely many primes p there exists a group of order p^{10} of nilpotency class 9 which is not isomorphic to the multiplicative group of any left brace. His proof uses Lazard's correspondence between nilpotent Lie algebras over $\mathbb{F}_p$ and finite p-groups and the generalization of some results in the theory of Hopf-Galois extensions, and it also is based on the proof of Burde [14] of the existence of nilpotent Lie algebras over $\mathbb{C}$ of dimension 10 with no faithful representation of dimension 11.

On the other hand, there are some positive results on the structure of the multiplicative group of a finite left brace.

The following result is a particular case of Lemma 8.1 in [23].

Lemma 7.1 *Let p be a prime. Let G be a finite non-trivial p-group. Then G is isomorphic to a subgroup of the multiplicative group of a two-sided brace of order a power of p.*

PROOF — Let $\mathbb{F}_p$ be the field of p elements. Then it is known that the augmentation ideal $R = \omega(\mathbb{F}_p[G])$ of the group algebra $\mathbb{F}_p[G]$ is its Jacobson radical. In fact, R is a nilpotent ring. Thus $(R, +, \circ)$, where

$$a \circ b = ab + a + b,$$

is a two-sided brace. Let

$$f \colon G \longrightarrow R$$

be the map defined by $f(g) = g - 1$, for all $g \in G$. Note that

$$\begin{aligned} f(g_1 g_2) = g_1 g_2 - 1 &= (g_1 - 1)(g_2 - 1) + g_1 - 1 + g_2 - 1 \\ &= (g_1 - 1) \circ (g_2 - 1) = f(g_1) \circ f(g_2), \end{aligned}$$

for all $g_1, g_2 \in G$. The result follows. □

The following result generalizes [24], Corollary 3.8.

Corollary 7.2 *Every finite nilpotent group G is isomorphic to a subgroup of the multiplicative group of a finite two-sided brace B, which is the direct product of two-sided braces*

$$B_1, \dots, B_n$$

of orders $p_1^{m_1}, \dots, p_n^{m_n}$, where $p_1, \dots, p_n$ are the distinct prime divisors of the order of G.

Proof — Suppose that G is a finite nilpotent group of order

$$p_1^{s_1} \dots p_n^{s_n},$$

where $p_1, \dots, p_n$ are distinct primes and $s_1, \dots, s_n$ are positive integers. Since G is nilpotent, its Sylow subgroups are normal. Let S_i be the Sylow p_i-subgroup of G. Then G is the direct product of its Sylow subgroups

$$G = \prod_{i=1}^{n} S_i.$$

By Lemma 7.1, there exists a finite two-sided brace B_i of order $p_i^{m_i}$ such that S_i is isomorphic to a subgroup of the multiplicative group of B_i. Let $B = B_1 \times \dots \times B_n$. It is clear that G is isomorphic to a subgroup of the multiplicative group of the two-sided brace B. Thus the result follows. □

Another result in this line is the following theorem.

Theorem 7.3 (see [24], Corollary 3.6) *Every finite solvable group is isomorphic to a subgroup of the multiplicative group of a finite left brace.*

It is clear that every abelian group is isomorphic to the multiplicative group of a trivial brace. It is also clear that if G_1, G_2 are groups isomorphic to multiplicative groups of left braces, then its direct product also is. We summarize other positive results in the following theorem.

Theorem 7.4 *Let* G *be a finite group. If one of the following conditions holds, then* G *is isomorphic to the multiplicative group of a left brace.*

(1) G *is nilpotent of nilpotency class two ([1]).*

(2) G *is abelian-by-cyclic (see [24], Corollary 3.10).*

(3) $G = A \rtimes H$, *where* A *is abelian and* H *is the multiplicative group of a left brace (see [24], Theorem 3.3)*

(4) $G = G_1 \wr G_2$, *where* G_1, G_2 *are isomorphic to multiplicative groups of left braces (see [24], Corollary 3.5).*

(5) G *is solvable of* A*-type, i.e. with all its Sylow subgroups abelian (see [13], Corollary 4.3).*

8 Left braces and the Yang-Baxter equation

The Yang-Baxter equation is an important equation in theoretical physics that has become, since its origin in a paper of Yang [58], a key ingredient in quantum groups and Hopf algebras [41]. It was suggested by Drinfeld in [27] to find all the set-theoretic solutions of the Yang-Baxter equation. In [29] and [33] the study of non-degenerate involutive set-theoretic solution of the Yang-Baxter equation was initiated introducing interesting related algebraic structures. The last years several papers on this type of solutions have appeared [7],[8], [9],[10],[17],[20],[21],[22],[24],[25],[26],[30],[31],[32],[46],[48],[51],[55]. We recall its definition.

Let X be a non-empty set. Let

$$r\colon X^2 \longrightarrow X^2$$

be a bijective map and write

$$r(x,y) = (\sigma_x(y), \gamma_y(x)).$$

We say that (X,r) is involutive if $r^2 = \mathrm{id}_{X^2}$. We say that (X,r) is non-degenerate if $\sigma_x, \gamma_x \in \mathrm{Sym}_X$, for all $x \in X$. We say that (X,r) is a set-theoretic solution of the Yang-Baxter equation if $r_1 r_2 r_1 = r_2 r_1 r_2$, where

$$r_1 = r \times \mathrm{id}_X\colon X^3 \longrightarrow X^3$$

and

$$r_2 = \mathrm{id}_X \times r\colon X^3 \longrightarrow X^3.$$

Example 8.1 Let X be a non-empty set. Let $r\colon X^2 \longrightarrow X^2$ by the mapping defined by $r(x,y) = (y,x)$, for all $x,y \in X$. It is easy to check that (X,r) is a non-degenerate involutive set-theoretic solution of the Yang-Baxter equation. It is called the trivial solution on X.

Let X, Y be non-empty sets and let

$$r\colon X^2 \longrightarrow X^2 \quad \text{and} \quad r'\colon Y^2 \longrightarrow Y^2$$

be maps. Write

$$r(x,x') = (\sigma_x(x'), \gamma_{x'}(x)) \quad \text{and} \quad r'(y,y') = (\sigma'_y(y'), \gamma'_{y'}(y)).$$

A homomorphism from (X, r) to (Y, r') is a map $f\colon X \longrightarrow Y$ such that

$$(f(\sigma_x(x')), f(\gamma_{x'}(x))) = r'(f(x), f(x')),$$

for all $x, x' \in X$. Note that if (X, r) is a non-degenerate involutive set-theoretic solution of the Yang-Baxter equation then so is

$$(f(X), r'_{|f(X)^2}).$$

If f is bijective then we say that (X, r) and (Y, r') are isomorphic.

Convention. By a solution of the YBE we mean a non-degenerate involutive set-theoretic solution of the Yang-Baxter equation.

The next result is an easy generalization of [19], Theorem 4.1.

Proposition 8.2 (see [21], Proposition 2) *Let X be a non-empty set. Let*

$$r\colon X^2 \longrightarrow X^2$$

be a bijective map such that

$$r(x, y) = (\sigma_x(y), \gamma_y(x)).$$

Then (X, r) is a solution of the YBE if and only if

(i) $r^2 = id_{X^2}$,

(ii) $\sigma_x \in \mathrm{Sym}_X$, *for all* $x \in X$,

(iii) $\sigma_x \circ \sigma_{\sigma_x^{-1}(y)} = \sigma_y \circ \sigma_{\sigma_y^{-1}(x)}$, *for all* $x, y \in X$.

Proof — It is straightforward (see the proof of Theorem 9.3.10 in [40]). □

Let (X, r) be a solution of the YBE and write $r(x, y) = (\sigma_x(y), \gamma_y(x))$. The structure group of (X, r) is the group $G(X, r)$ with the presentation

$$G(X, r) = \langle X \mid xy = \sigma_x(y)\gamma_y(x),\ \forall x, y \in X\rangle.$$

Let $\mathbb{Z}^X$ denote the additive free abelian group with basis X. Consider the natural action of Sym_X on $\mathbb{Z}^X$ and the associated semidirect product

$$M(X) = \mathbb{Z}^X \rtimes \mathrm{Sym}_X\,.$$

In [29] (Proposition 2.4 and 2.5) it is proven that $G(X,r)$ is isomorphic to a subgroup B of $M(X)$ of the form

$$B = \{(a, \phi(a)) \mid a \in \mathbb{Z}^X\},$$

for some function

$$\phi\colon \mathbb{Z}^X \longrightarrow \operatorname{Sym}_X .$$

In fact, $\phi(x) = \sigma_x$ for all $x \in X$, and the map $x \mapsto (x, \sigma_x)$ from X to $\mathbb{Z}^X \rtimes \operatorname{Sym}_X$ induces an isomorphism

$$\widetilde{\phi}\colon G(X,r) \longrightarrow B.$$

Note that

$$(a, \phi(a))(b, \phi(b)) = (a + \phi(a)(b), \phi(a)\phi(b)),$$

Thus $\phi(a + \phi(a)(b)) = \phi(a)\phi(b)$.

Note that one can define a sum $+$ on B by the rule

$$(a, \phi(a)) + (b, \phi(b)) = (a + b, \phi(a + b)),$$

for all $a, b \in \mathbb{Z}^X$. Note also that

$$\begin{aligned}
&(a, \phi(a))((b, \phi(b)) + (c, \phi(c))) + (a, \phi(a))\\
&= (a, \phi(a))(b + c, \phi(b + c)) + (a, \phi(a))\\
&= (a + \phi(a)(b + c), \phi(a + \phi(a)(b + c))) + (a, \phi(a))\\
&= (a + \phi(a)(b + c) + a, \phi(a + \phi(a)(b + c) + a))\\
&= (a + \phi(a)(b) + \phi(a)(c) + a, \phi(a + \phi(a)(b) + \phi(a)(c) + a))\\
&= (a + \phi(a)(b), \phi(a + \phi(a)(b))) + (a + \phi(a)(c), \phi(a + \phi(a)(c)))\\
&= (a, \phi(a))(b, \phi(b)) + (a, \phi(a))(c, \phi(c)).
\end{aligned}$$

Hence $(B, +, \cdot)$ is a left brace.

We can define a sum $+$ in $G(X,r)$ by

$$g + h = \widetilde{\phi}^{-1}(\widetilde{\phi}(g) + \widetilde{\phi}(h)),$$

for all $g, h \in G(X,r)$. Then $(G(X,r), +, \cdot)$ is a left brace and the additive group is $\mathbb{Z}^X$, the additive free abelian group with basis X. We say that this is the natural structure of left brace on the structure group $G(X,r)$. Note that

$$\begin{aligned}\lambda_a(b) = ab - a = \widetilde{\phi}^{-1}(\widetilde{\phi}(ab) - \widetilde{\phi}(a))\\ = \widetilde{\phi}^{-1}((a,\phi(a))(b,\phi(b)) - (a,\phi(a)))\\ = \widetilde{\phi}^{-1}((a+\phi(a)(b),\phi(a+\phi(a)(b))) - (a,\phi(a)))\\ = \widetilde{\phi}^{-1}((\phi(a)(b),\phi(\phi(a)(b))))\\ = \phi(a)(b),\end{aligned}$$

for all $a,b \in G(X,r)$. In particular, $\lambda_x(y) = \sigma_x(y)$, for all $x,y \in X$.

The subgroup of Sym_X generated by $\{\sigma_x \mid x \in X\}$ is denoted by $\mathcal{G}(X,r)$ (see [31]) and it is called the permutation group of the solution (X,r). Note that $\mathcal{G}(X,r) = \phi(G(X,r))$. The map

$$\phi\colon G(X,r) \longrightarrow \mathcal{G}(X,r)$$

is a homomorphism of groups. Then $\mathcal{G}(X,r)$ has a unique structure of left brace such that ϕ is a homomorphism of left braces. This is the natural structure of left brace on the permutation group of (X,r). Note that $\mathrm{Ker}(\phi) = \mathrm{Soc}(G(X,r))$. Thus

$$\mathcal{G}(X,r) \simeq G(X,r)/\mathrm{Soc}(G(X,r)).$$

In [33], Theorem 1.6, it is proven that the structure group $G(X,r)$ of a finite solution (X,r) of the YBE is a Bieberbach group, i.e. a finitely generated torsion-free abelian-by-finite group.

In order to study the structure group $G(X,r)$ of a solution of the YBE and to classify such solutions, Etingof, Shedler and Soloviev in [29] proposed an interesting operator as a tool. We recall its definition.

Definition 8.3 *Let (X,r) be a solution of the YBE. Suppose that*

$$r(x,y) = (\sigma_x(y),\gamma_y(x)).$$

The retract relation $\sim$ on the set X with respect to r is defined by $x \sim y$ if $\sigma_x = \sigma_y$.

There is a natural induced solution $\mathrm{Ret}(X,r) = ([X],[r])$*, called the re-*

traction of (X, r)*, where* $[X] = X/\sim$ *and*

$$[r]([x], [y]) = ([\sigma_x(y)], [\gamma_y(x)]),$$

where $[x]$ *denotes the* $\sim$ *equivalence class of* $x \in X$.

Definition 8.4 *A solution* (X, r) *of the YBE is called a multipermutation solution of level* m *if* m *is the smallest nonnegative integer such that the solution* $\mathrm{Ret}^m(X, r)$ *has cardinality* 1*; in this case we write* $\mathrm{mpl}(X, r) = m$*. Here we define*

$$\mathrm{Ret}^k(X, r) = \mathrm{Ret}(\mathrm{Ret}^{k-1}(X, r))$$

for $k \geqslant 1$*, and* $\mathrm{Ret}^0(X, r) = (X, r)$.

We say that the solution (X, r) *is irretractable if* $\mathrm{Ret}(X, r) = (X, r)$.

We now discuss a strong connection between braces and solutions of the YBE. We begin with the following lemma which is implicit in [48] and at page 132 of [47].

Lemma 8.5 (see [21], Lemma 2) *Let* B *be a left brace. The following properties hold.*

(i) $a\lambda_a^{-1}(b) = b\lambda_b^{-1}(a)$.

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

(iii) *The map*

$$r_B \colon B \times B \longrightarrow B \times B$$

defined by $r_B(x, y) = (\lambda_x(y), \lambda^{-1}_{\lambda_x(y)}(x))$ *is a solution of the YBE.*

Proof — **(i)** Let $a, b \in B$. Then

$$a\lambda_a^{-1}(b) = a(a^{-1}(b + a)) = b + a = b\lambda_b^{-1}(a).$$

(ii) is a consequence of (i) and Lemma 2.6.
(iii) It is easy to check that $r_B^2 = \mathrm{id}_{B^2}$. Let $g_y(x) = \lambda^{-1}_{\lambda_x(y)}(x)$. To show that (B, r_B) is non-degenerate we prove that g_y is bijective. For this we note that

$$\begin{aligned} g_y(x) = \lambda^{-1}_{\lambda_x(y)}(x) = \lambda^{-1}_{xy-x}(x) = (xy - x)^{-1}(x + xy - x) \\ = (xy - x)^{-1}xy = ((xy)^{-1}(xy - x))^{-1} = (1 - y^{-1} + (xy)^{-1})^{-1} \\ = (-y^{-1} + (xy)^{-1})^{-1}. \end{aligned}$$

Now, by (ii) and Proposition 8.2, the assertion follows. □

Let B be a left brace. The solution of the YBE equation (B, r_B) defined in Lemma 8.5 is called the solution of the YBE associated to the left brace B.

Recall that a left brace B is right nilpotent if $B^{(n)} = \{0\}$ for some positive integer n. The following result is a characterization of this class of left braces.

Proposition 8.6 (see [17], Proposition 6) *Let B be a nonzero left brace and let (B, r_B) be its associated solution of the YBE. Then*

$$\mathrm{mpl}(B, r_B) = m < +\infty$$

if and only if $B^{(m+1)} = \{0\}$ and $B^{(m)} \neq \{0\}$.

Let (X, r) be a finite multipermutation solution of the YBE. Then it is easy to see that the group $G(X, r)$ is poly-(infinite cyclic) (Proposition 4.2 in [39]). Recently the converse has been proven.

Theorem 8.7 (see [10], Theorem 2.1) *Let (X, r) be a finite solution of the YBE. Then the following statements are equivalent:*

(1) *(X, r) is a multipermutation solution.*

(2) *$G(X, r)$ is left orderable.*

(3) *$G(X, r)$ is poly-(infinite cyclic).*

We now give an equivalent condition for a group to be a multiplicative group of a left brace. This is an easy generalization of a part of [24], Theorem 2.1 (see the definition of IYB morphism at page 2546 of [24]).

Proposition 8.8 (see [23], Proposition 4.2) *A group G is the multiplicative group of a left brace if and only if there exists a group homomorphism*

$$\mu : G \longrightarrow \mathrm{Sym}_G$$

such that $x\mu(x)^{-1}(y) = y\mu(y)^{-1}(x)$ for all $x, y \in G$.

Proof — Suppose that such a homomorphism μ is given. Define an operation $+$ on G by

$$x + y = x\mu(x)^{-1}(y)$$

for $x, y \in G$. Clearly $x + y = y + x$. Further, for $x, y, z \in G$,

$$\begin{aligned}(x+y)+z &= y\mu(y)^{-1}(x)+z = y\mu(y)^{-1}(x)\,\mu(y\mu(y)^{-1}(x))^{-1}(z)\\ &= y\mu(y)^{-1}(x)\ \mu(\mu(y)^{-1}(x))^{-1}\ (\mu(y)^{-1}(z))\\ &= y\mu(y)^{-1}(z)\ \mu(\mu(y)^{-1}(z))^{-1}\ (\mu(y)^{-1}(x))\\ &= y\mu(y)^{-1}(z)\mu(y\mu(y)^{-1}(z))^{-1}(x)\\ &= (y+z)+x = x+(y+z).\end{aligned}$$

It is easy to check that 1 is the neutral element for this addition and $\mu(x)(x^{-1})$ is the opposite of x. Hence $(G, +)$ is an abelian group.

For $x, y, z \in G$ we also get that $x^{-1}\mu(x^{-1})^{-1}(y+z) = x^{-1}+y+z$ and hence

$$\begin{aligned}\mu(x)(y+z) &= x\ (x^{-1}+y+z) = x\ (x^{-1}\mu(x)(y)+z)\\ &= xx^{-1}\mu(x)(y)\ \mu(x^{-1}\mu(x)(y))^{-1}(z)\\ &= \mu(x)(y)\ \mu(\mu(x)(y))^{-1}\ (\mu(x)(z))\\ &= \mu(x)(y)+\mu(x)(z)\end{aligned}$$

and therefore

$$\begin{aligned}x(y+z)+x =& x\mu(x)^{-1}(\mu(x)(y+z))+x = x+\mu(x)(y+z)+x\\ =& x+\mu(x)(y)+x+\mu(x)(z) = xy+xz.\end{aligned}$$

Hence $(G, +, \cdot)$ is a left brace. Note that in this brace $\lambda_x = \mu(x)$ for every $x \in G$.

The converse follows by Lemmas 2.6 and 8.5. □

The following result gives a strong link between left braces and solutions of the YBE.

Theorem 8.9 (see [21], Theorem 2) *If B is a left brace then there exists a solution (X, r') of the YBE such that the solution $\mathrm{Ret}(X, r')$ is isomorphic to the solution (B, r_B) associated to the left brace B and, moreover, $\mathcal{G}(X, r')$ is isomorphic to B as left braces. Furthermore, if B is finite then X can be taken a finite set.*

Given a left brace B, in [7] there is a method to construct explicitly all the solutions (X, r) of the YBE such that $\mathcal{G}(X, r)$ is isomorphic to B as left braces. In some sense in [7], the classification of all finite solutions of the YBE is reduced to the classification of all finite left braces.

9 Left braces and related algebraic structures

In this section we give some connections between left braces an other algebraic structures.

Definition 9.1 *Let* G *be a group. The holomorph of* G *is the group*

$$\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G).$$

Definition 9.2 *Let* G *be a group. A regular subgroup of* $\mathrm{Hol}(G)$ *is a subgroup* H *of* $\mathrm{Hol}(G)$ *of the form* $H = \{(a, \phi(a)) \in \mathrm{Hol}(G) \mid a \in G\}$ *for some function* $\phi \colon G \longrightarrow \mathrm{Aut}(G)$.

Theorem 9.3 (see [23], Theorem 5.1) *Let* $(A, +)$ *be an abelian group. Let*

$$\mathcal{B}(A) = \{(A, +, \cdot) \mid (A, +, \cdot) \text{ is a left brace}\}$$

and

$$\mathcal{S}(A) = \{G \mid G \text{ is a regular subgroup of } \mathrm{Hol}(A)\}.$$

Then the map $f : \mathcal{B}(A) \to \mathcal{S}(A)$ *defined by*

$$f(A, +, \cdot) = \{(a, \lambda_a) \mid a \in A\}$$

is bijective.

Proof — Let $a, b \in A$. Then

$$(a, \lambda_a)(b, \lambda_b) = (a + \lambda_a(b), \lambda_a\lambda_b) = (a + ab - a, \lambda_{ab}) = (ab, \lambda_{ab})$$

and

$$\begin{aligned}(a, \lambda_a)^{-1} &= (\lambda_a^{-1}(-a), \lambda_a^{-1}) = (-\lambda_{a^{-1}}(a), \lambda_{a^{-1}})\\ &= (-a^{-1}a + a^{-1}, \lambda_{a^{-1}}) = (a^{-1}, \lambda_{a^{-1}}).\end{aligned}$$

Hence $\{(a, \lambda_a) \mid a \in A\} \in \mathcal{S}(A)$ and thus f is well defined.

Consider $G = \{(a, \phi(a)) \mid a \in A\} \in \mathcal{S}(A)$. We define an operation $\cdot$ on A by

$$a \cdot b = a + \phi(a)(b),$$

for $a, b \in A$. We prove that $(A, +, \cdot)$ is a left brace. For this we first show that $(A, \cdot)$ is a group. Let $a, b, c \in A$. Since

$$(a, \phi(a))\,(b, \phi(b)) = (a + \phi(a)(b), \phi(a)\,\phi(b)) \in G$$

we have that

$$\phi(a + \phi(a)(b)) = \phi(a)\,\phi(b).$$

Thus

$$(a \cdot b) \cdot c = (a + \phi(a)(b)) \cdot c =$$

$$a + \phi(a)(b) + \phi(a + \phi(a)(b))(c) = a + \phi(a)(b) + \phi(a)\,\phi(b)(c)$$

and

$$a \cdot (b \cdot c) = a \cdot (b + \phi(b)(c)) =$$

$$a + \phi(a)(b + \phi(b)(c)) = a + \phi(a)(b) + \phi(a)\,\phi(b)(c).$$

So

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Notice that

$$a \cdot 0 = a + \phi(a)(0) = a$$

and

$$a \cdot \phi(a)^{-1}(-a) = a - a = 0.$$

Hence, $(A, \cdot)$ is a group. We also have

$$a \cdot (b + c) + a = a + \phi(a)(b + c) + a$$

$$= a + \phi(a)(b) + a + \phi(a)(c) = a \cdot b + a \cdot c.$$

Hence $(A, +, \cdot)$ is a left brace.

So, we have constructed a map $\mathcal{S}(A) \to \mathcal{B}(A)$ and it is easy to verify that this is the inverse of the map f. □

A connection of this type in the context of regular permutation subgroups of the affine group $AGL(V)$ on a vector space V was given by Catino and Rizzo [16].

Note that if $G = \{(a, \phi(a)) \mid a \in A\} \in \mathcal{S}(A)$ then from the proof it follows that the bijective map $G \to A : (a, \phi(a)) \mapsto a$ is a multiplicative homomorphism of the group G to the multiplicative group of the left brace $f^{-1}(G)$. We can now define a sum on G using this bijection, that is

$$(a, \phi(a)) + (b, \phi(b)) = (a + b, \phi(a + b))$$

for $a, b \in A$, making this bijection an isomorphism of left braces.

In case the group $\phi(A)$ is finite then the group G has been investigated in [34] and it was called a group of IG-type. Thus every group of IG-type is isomorphic to the multiplicative group of a left brace.

We now recall the definition of a monoid of I-type introduced by Gateva-Ivanova and Van den Bergh in [33]. For this, let FaM_n denote the multiplicative free abelian monoid of rank n with basis

$$\{u_1, \dots, u_n\}.$$

Definition 9.4 *A monoid S generated by a set $X = \{x_1, \dots, x_n\}$ is said to be of left I-type if there exists a bijection (called a left I-structure)*

$$v\colon \mathrm{FaM}_n \longrightarrow S$$

such that, for all $a \in \mathrm{FaM}_n$,

$$v(1) = 1 \quad \textit{and} \quad \{v(u_1 a), \dots, v(u_n a)\} = \{x_1 v(a), \dots, x_n v(a)\}.$$

Similarly, one defines monoids of right I-type. In [39] Jespers and Okniński proved that a monoid S is of left I-type if and only if S is of right I-type. The monoid S is simply called a monoid of I-type and its group of fractions SS^{-1} is said to be a group of I-type.

Gateva-Ivanova and Van den Bergh in [33] proved that a group G is of I-type if and only if it is isomorphic to the structure group of a finite solution of the YBE. Thus, groups of I-type are also of IG-type.

We can now characterize groups of I-type as follows.

Proposition 9.5 (see [23], Proposition 5.2) *A group G is of I-type if and only if it is isomorphic to the multiplicative group of a left brace B such that the additive group of B is a free abelian group with a finite basis X such that $\lambda_x(y) \in X$ for all $x, y \in X$.*

Proof — Suppose G is a group of I-type. We may assume that G is a subgroup of $\mathbb{Z}^Y \rtimes \mathrm{Sym}_Y$, for some finite set Y, of the form

$$G = \{(u, \phi(u)) \mid u \in \mathbb{Z}^Y\},$$

and for some mapping $\phi\colon \mathbb{Z}^Y \longrightarrow \mathrm{Sym}_Y$. By the comment given before the proposition, we know that G is a left brace for the addition

$$(a, \phi(a)) + (b, \phi(b)) = (a + b, \phi(a + b)),$$

with $a, b \in \mathbb{Z}^Y$. Its additive group is a free abelian group with basis

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

and

$$\begin{aligned}\lambda_{(x,\phi(x))}(y, \phi(y)) &= (x, \phi(x))(y, \phi(y)) - (x, \phi(x))\\ &= (x + \phi(x)(y), \phi(x + \phi(x)(y))) - (x, \phi(x))\\ &= (\phi(x)(y), \phi(\phi(x)(y))) \in X.\end{aligned}$$

Conversely, suppose that B is a left brace such that its additive group is a free abelian group with a finite basis X such that $\lambda_x(y) \in X$ for all $x, y \in X$. Hence $\lambda_x^{-1}(y) \in X$, for all $x, y \in X$. By Lemma 2.6,

$$\lambda_x^{-1} = \lambda_{x^{-1}}.$$

In particular,

$$\lambda_{x^{-1}}(x) = 1 - x^{-1} = -x^{-1} \in X$$

for all $x \in X$. Since X is finite, the map $x \mapsto -x^{-1}$ is a permutation of X. It follows that $(-x)^{-1} \in X$ (the inverse image of x) for all $x \in X$. Therefore,

$$\lambda_{-x}(y) = \lambda^{-1}_{(-x)^{-1}}(y) \in X$$

for all $x, y \in X$. Let $a \in B$. We know from Lemma 2.6 that λ_a is an automorphism of the additive group of the brace B.

Suppose that

$$a = \sum_{x \in X} z_x x$$

for some integers z_x. We shall prove that $\lambda_a(x) \in X$, for all $x \in X$, by induction on

$$m_a = \sum_{x \in X} |z_x|.$$

If $m_a = 1$, then the result is clear. Suppose that $m_a > 1$ and that $\lambda_b(x) \in X$, for all $x \in X$ and all $b \in B$ such that $m_b < m_a$. Clearly there exists $x \in X$ such that either

$$m_{a+x} < m_a \quad \text{or} \quad m_{a-x} < m_a.$$

Note that, for all $c, d \in B$,

$$c+d = c+d-1 = c+cc^{-1}d - cc^{-1} = c(c^{-1}d - c^{-1}) = c\lambda_{c^{-1}}(d). \quad (9.1)$$

Suppose that $m_{a+x} < m_a$. Because of (9.1) we get that

$$\lambda_a = \lambda_{a+x-x} = \lambda_{(-x)\lambda^{-1}_{-x}(a+x)} = \lambda_{-x}\lambda_{\lambda^{-1}_{-x}(a+x)}.$$

Since $\lambda_{-x}(y) \in X$ and λ_{-x} is an automorphism of the additive group of B, we have that

$$m_{\lambda^{-1}_{-x}(a+x)} = m_{a+x} < m_a.$$

Hence by the induction hypothesis, $\lambda_{\lambda^{-1}_{-x}(a+x)}(y) \in X$, and therefore $\lambda_a(y) \in X$, in this case.

Suppose that $m_{a-x} < m_a$. Again by (9.1) we have

$$\lambda_a = \lambda_{a-x+x} = \lambda_{x\lambda_x^{-1}(a-x)} = \lambda_x\lambda_{\lambda_x^{-1}(a-x)}.$$

Since $\lambda_x(y) \in X$ and λ_x is an automorphism of the additive group of B, we have that

$$m_{\lambda_x^{-1}(a-x)} = m_{a-x} < m_a.$$

Hence by the induction hypothesis,

$$\lambda_{\lambda_x^{-1}(a-x)}(y) \in X,$$

and therefore $\lambda_a(y) \in X$, in this case.

Thus every automorphism λ_a of the additive group of B is induced by a permutation of the finite set X. Note that for all $a, b \in B$

$$(ab, \lambda_{ab}) = (a + \lambda_a(b), \lambda_a\lambda_b) = (a, \lambda_a)(b, \lambda_b).$$

Therefore the map

$$f : B \longrightarrow \{(a, \lambda_a) \mid a \in B\}$$

defined by $f(a) = (a, \lambda_a)$ is an isomorphism of the multiplicative group of B and the subgroup

$$\{(a, \lambda_a) \mid a \in B\}$$

of the semidirect product $B \rtimes \mathrm{Aut}(B, +)$. Hence the multiplicative group of B is of I-type. □

Note also that if G is a left brace, then the identity map

$$\mathrm{id}\colon G \longrightarrow G$$

is a bijective 1-cocycle of the group G with coefficients in the left G-module $(G, +)$ with respect the action given by

$$\lambda\colon G \longrightarrow \mathrm{Aut}(G, +).$$

This is because for all $a, b \in G$ we have $ab = a + \lambda_a(b)$. Furthermore, if H is a group, A is a left H-module and

$$\pi\colon H \longrightarrow A$$

is a bijective 1-cocycle, then we can define a sum $+$ in H by

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

for all $a, b \in H$; and the group H with this sum is a left brace. This is because for all $a, b, c \in H$ we have that

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

This gives us a bijective correspondence between left braces and groups with a bijective 1-cocycle with respect to a left action (see [24],[29]). The latter class of groups gives rise to groups of central type which play an important role in the theory of finite dimensional central simple algebras (see [12],[28]). This class of groups with a bijective 1-cocycle also appeared in the context of left-invariant affine structures on Lie groups [14].

Definition 9.6 *A Garside monoid is a pair* (M, Δ) *where* M *is a cancellative monoid such that:*

(1) *there exists* $d : M \longrightarrow \mathbb{N}$ *satisfying* $d(ab) \geqslant d(a) + d(b)$ *and* $a \neq 1$ *implies* $d(a) \neq 0$,

(2) *any two elements of* M *have a left- and a right-lcm and a left- and a right-gcd,*

(3) Δ *is a Garside element of M, this meaning that the left- and right-divisors of* Δ *coincide and generate* M,

(4) *the family of all divisors of* Δ *in* M *is finite.*

Recall that a non-invertible element of a monoid is an atom if it is not a product of two non-invertible elements. A monoid S is atomic if every non-invertible element of S is a product of atoms.

Note that if (M, Δ) is a Garside monoid, then condition (1) in the definition implies that $d(1) = 0$ and M is conical, that is $ab = 1$ implies $a = b = 1$. Furthermore, M is atomic and the set of atoms of M is finite by (4). Moreover, for every $a \in M$, the supremum of the number of atoms in the factorization of a as a product of atoms is finite. Note that if $a \in M$ is a divisor of Δ, then there exist $a', a'' \in M$ such that $aa' = a'a'' = \Delta$ and $a\Delta = \Delta a''$. Now it is easy to see that M satisfies the left and right Ore conditions. Thus it has left and right group of fractions $G = M^{-1}M = MM^{-1}$.

Definition 9.7 *A group* G *is said to be a Garside group if it is the (left) group of fractions of a submonoid* M *and there exists* $\Delta \in M$ *such that* (M, Δ) *is a Garside monoid.*

In [25] (Theorem 3.3), Chouraqui proved that the structure group of a finite solution of the YBE is a Garside group. We shall prove this result using the natural structure of left brace of the structure group of a solution of the YBE.

Lemma 9.8 *Let* (X, r) *be a finite solution of the YBE. Let*

$$n = [G(X, r) : \mathrm{Soc}(G(X, r))].$$

Let z be an integer. Let

$$\Delta_z = \sum_{x \in X} zx.$$

Then $g\Delta_z = g + \Delta_z$*, for all* $g \in G(X,r)$*. In particular,* $\Delta_z^m = m\Delta_z$*, for all integer* m*, and* $n\Delta_z$ *is a central element of the structure group* $G(X,r)$*.*

Proof — Let $g \in G(X,r)$. We have

$$g\Delta_z = \lambda_g(\Delta_z) + g = \lambda_g\big(\sum_{x\in X} zx\big)+g = \sum_{x\in X} z\lambda_g(x) + g = \Delta_z + g.$$

The second part is a consequence of the first and the fact that $n\Delta_z$ is contained in $\operatorname{Soc}(G(X,r))$. □

Let (X,r) be a finite solution of the YBE. Let $M(X,r)$ be the submonoid of $G(X,r)$ generated by X.

Lemma 9.9 *We have*

$$M(X,r) = \big\{\sum_{x\in X} z_x x \mid z_x \in \mathbb{N}\big\} \quad \textit{and} \quad M(X,r)^{-1} = -M(X,r).$$

Proof — Let

$$M = \big\{\sum_{x\in X} z_x x \mid z_x \in \mathbb{N}\big\}.$$

Note that $\lambda_g(a) \in M$, for all $g \in G(X,r)$ and all $a \in M$.

Every element of $M(X,r)$ is of the form

$$x_1 \dots x_m,$$

with $x_1,\dots,x_m \in X$. We shall prove that $x_1\dots x_m \in M$ by induction on m. For $m = 1$ it is clear. Suppose that $m > 1$ and that

$$y_1 \cdots y_{m-1} \in M$$

for all $y_1,\dots,y_{m-1} \in X$. By the induction hypothesis, $x_2 \dots x_m \in M$, and thus

$$x_1 \dots x_m = x_1 + \lambda_{x_1}(x_2 \dots x_m) \in M.$$

Hence $M(X,r) \subseteq M$. Let

$$\sum_{x\in X} z_x x \in M.$$

We shall prove that

$$\sum_{x\in X} z_x x \in M(X,r)$$

by induction on

$$t = \sum_{x \in X} z_x.$$

For $t = 1$ it is clear. Suppose that $t > 1$ and that

$$\sum_{x \in X} a_x x \in M(X, r)$$

for all

$$\sum_{x \in X} a_x x \in M$$

with

$$\sum_{x \in X} a_x < t.$$

Since $t > 1$ there exists $x_0 \in X$ such that $z_{x_0} > 0$. Let

$$a = -\lambda_{x_0}^{-1}(x_0) + \sum_{x \in X} z_x \lambda_{x_0}^{-1}(x).$$

Now we have that $a \in M$ and, by the induction hypothesis, $a \in M(X, r)$. Thus

$$\sum_{x \in X} z_x x = x_0 - x_0 + \sum_{x \in X} z'_x x = x_0 \lambda_{x_0}^{-1}(-x_0 + \sum_{x \in X} z'_x x) = x_0 a \in M(X, r).$$

Hence $M = M(X, r)$.

Note that

$$g^{-1} = -\lambda_{g^{-1}}(g)$$

and

$$-g = \lambda_{(-g)^{-1}}(g)^{-1}$$

for all $g \in G(X, r)$. Therefore

$$M^{-1} = -M,$$

and the result follows. □

Note that $M(X, r)$ has a degree function

$$\deg \colon M(X, r) \longrightarrow \mathbb{N}$$

defined by $\deg(x_1 \dots x_m) = m$, for all $x_1, \dots, x_m \in X$.

Lemma 9.10 *Let* $a \in M(X, r)$*. By Lemma 9.9,*

$$a = \sum_{x \in X} a_x x,$$

for some $a_x \in \mathbb{N}$*. Then* $\deg(a) = \sum_{x \in X} a_x$.

Proof — We will prove the result by induction on $\deg(a)$. If $\deg(a) = 1$, then $a = x$ for some $x \in X$, and the result is clear. Suppose that

$$\deg(a) = m > 1$$

and that the result is true for all $b \in M(X, r)$ with $\deg(b) < m$. We have that $a = x_1 \dots x_m$, for some $x_1, \dots, x_m \in X$. By the induction hypothesis,

$$x_2 \dots x_m = \sum_{x \in X} b_x x,$$

for some $b_x \in \mathbb{N}$ such that $\sum_{x \in X} b_x = m - 1$. We have

$$\begin{aligned} a &= x_1 + \lambda_{x_1}(x_2 \dots x_m) \\ &= x_1 + \lambda_{x_1}(\textstyle\sum_{x \in X} b_x x) = x_1 + \sum_{x \in X} b_x \lambda_{x_1}(x). \end{aligned}$$

Since $\lambda_{x_1}(x) \in X$, for all $x_1, x \in X$, the result follows. □

Lemma 9.11 *Let* $a, b \in M(X, r)$ *and* $c, d \in M(X, r)^{-1}$*. By Lemma 9.9,*

$$a = \sum_{x \in X} a_x x, \; b = \sum_{x \in X} b_x x, \; c = \sum_{x \in X} c_x x \quad \textit{and} \quad d = \sum_{x \in X} d_x x,$$

for some $a_x, b_x, -c_x, -d_x \in \mathbb{N}$*. Then*

(i) $b^{-1} a \in M(X, r)$ *if and only if* $b_x \leqslant a_x$ *for all* $x \in X$.

(ii) $c^{-1} d \in M(X, r)^{-1}$ *if and only if* $c_x \geqslant d_x$ *for all* $x \in X$.

Proof — **(i)** Note that

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

Therefore $b^{-1} a \in M(X, r)$ if and only if $a - b \in M(X, r)$ and the result follows easily by Lemma 9.9.

(ii) As above

$$c^{-1}d = \lambda_{c^{-1}}(d - c).$$

Therefore $c^{-1}d \in M(X,r)^{-1}$ if and only if $d - c \in M(X,r)^{-1}$ and the result follows easily by Lemma 9.9. □

Lemma 9.12 *Any two elements of* $M(X,r)$ *have a left- and a right-lcm and a left- and a right-gcd.*

Proof — Let $a, b \in M(X,r)$. By Lemma 9.9

$$a = \sum_{x \in X} a_x x \quad \text{and} \quad b = \sum_{x \in X} b_x x,$$

for some $a_x, b_x \in \mathbb{N}$. By Lemma 9.11 it is clear that the left-gcd of a and b is

$$\text{l-gcd}(a,b) = \sum_{x \in X} \min(a_x, b_x)x,$$

and that its right-lcm is

$$\text{r-lcm}(a,b) = \sum_{x \in X} \max(a_x, b_x)x.$$

Now consider the monoid $M(X,r)^{-1}$. Since $a^{-1}, b^{-1} \in M(X,r)^{-1}$, by Lemma 9.9

$$a^{-1} = \sum_{x \in X} a'_x x \quad \text{and} \quad b^{-1} = \sum_{x \in X} b'_x x,$$

for some non-positive integers a'_x, b'_x. By Lemma 9.11 it is clear that the left-gcd of a^{-1} and b^{-1} in $M(X,r)^{-1}$ is

$$\text{l-gcd}(a^{-1}, b^{-1}) = \sum_{x \in X} \max(a'_x, b'_x)x,$$

and that its right-lcm is

$$\text{r-lcm}(a^{-1}, b^{-1}) = \sum_{x \in X} \min(a'_x, b'_x)x.$$

Note that if $d^{-1} = \text{l-gcd}(a^{-1}, b^{-1})$, then d is the right-gcd of a and b in $M(X,r)$, and if $m^{-1} = \text{r-lcm}(a^{-1}, b^{-1})$, then m is the left-lcm of a

and b in $M(X,r)$. Thus the result follows. □

Theorem 9.13 (see [25], Theorem 3.3) *Let (X,r) be a finite solution of the YBE. Let m be a positive integer. Then $(M(X,r),\Delta_m)$ is a Garside monoid and thus $G(X,r)$ is a Garside group.*

Proof — It is clear that the submonoid $M(X,r)$ of $G(X,r)$ is cancellative. We have seen that $M(X,r)$ has a degree function deg. In particular condition (1) in the definition of Garside monoid is satisfied.

By Lemma 9.12, condition (2) in the definition of Garside monoid is satisfied by $M(X,r)$.

By Lemma 9.9, $\Delta_m \in M(X,r)$ and, by Lemma 9.8, $\Delta_m^{-1} = -\Delta_m$. By Lemma 9.11, the set of left-divisors of Δ_m in $M(X,r)$ is

$$D_1 = \Big\{\sum_{x\in X} z_x x \mid z_x \in \mathbb{Z},\ 0 \leqslant z_x \leqslant m,\ \text{for all } x \in X\Big\},$$

and the set of left-divisors of Δ_m^{-1} in the monoid $M(X,r)^{-1}$ is

$$D_2 = \Big\{-\sum_{x\in X} z_x x \mid z_x \in \mathbb{Z},\ 0 \leqslant z_x \leqslant m,\ \text{for all } x \in X\Big\}.$$

Note that

$$\Big(\sum_{x\in X} z_x x\Big)^{-1} = -\lambda_{(\sum_{x\in X} z_x x)^{-1}}\Big(\sum_{x\in X} z_x x\Big) = -\sum_{x\in X} z_x \lambda_{(\sum_{x\in X} z_x x)^{-1}}(x),$$

for all $z_x \in \mathbb{Z}$. Hence $D_2^{-1} = D_1$. Thus the set of right-divisors of Δ_m in $M(X,r)$ also is D_1, which is finite and contains X. Therefore Δ_m is a Garside element of $M(X,r)$. Hence

$$(M(X,r),\Delta_m)$$

is a Garside monoid, and clearly $G(X,r)$ is its group of left (right) group of fractions. □

In [26] Dehornoy develops a sort of right-cyclic calculus to give another proof of Theorem 9.13. He also describes finite quotients of $G(X,r)$ that play a role similar to the role that Coxeter groups play for Artin-Tits groups. We shall see this using the left brace structure of $G(X,r)$.

Definition 9.14 (see [26], Definition 5.1) *If (M, Δ) is a Garside monoid and G is its group of fractions, a surjective homomorphism*

$$\pi\colon G \longrightarrow \overline{G}$$

is said to provide a Garside germ for (G, M, Δ) if there exists a map

$$\sigma\colon \overline{G} \longrightarrow M$$

such that $\pi \circ \sigma$ is the identity, the image of σ is the family of all divisors of Δ in M, and M admits a presentation

$$\langle \sigma(\overline{G}) \mid \{\sigma(f)\sigma(g) = \sigma(fg) \mid f, g \in \overline{G} \textit{ and } \|f\|_{\overline{S}} + \|g\|_{\overline{S}} = \|fg\|_{\overline{S}}\}\rangle,$$

where $\overline{S}$ is the image under π of the atom set of M, and $\|f\|_{\overline{S}}$ is the length of a shortest decomposition of f as a product of elements of $\overline{S}$.

Proposition 9.15 (see [26], Proposition 5.2) *Let (X, r) be a finite solution of the YBE. Let*

$$|X| = n,\ G = G(X, r),\ M = M(X, r) \ \textit{and}\ \ d = [G : \mathrm{Soc}(G)].$$

Let k be a positive integer such that

$$kd - 1 \geqslant 1 \quad \textit{and} \quad \Delta = \Delta_{kd-1}.$$

Then

$$N = \{kdg \mid g \in G\}$$

is a normal subgroup of G and the natural map

$$\pi\colon G \longrightarrow G/N$$

provides a Garside germ for (G, M, Δ). The group G/N has order $(kd)^n$ and the kernel of π is isomorphic to $\mathbb{Z}^n$.

Proof — By Theorem 9.13, (M, Δ) is a Garside monoid. We also know that the set of left-divisors of Δ is

$$D_1 = \Big\{ \sum_{x \in X} z_x x \mid z_x \in \mathbb{Z},\ 0 \leqslant z_x \leqslant kd - 1 \Big\}.$$

It is easy to see that N is a left ideal of the left brace G. Let $g, h \in G$.

Then, since $d = [G : \mathrm{Soc}(G)]$, $dg \in \mathrm{Soc}(G)$ and

$$\begin{aligned} h^{-1}(kdg)h &= h^{-1}(kdg + h) = \lambda_{h^{-1}}(kdg + h) + h^{-1} \\ &= kd\lambda_{h^{-1}}(g) + \lambda_{h^{-1}}(h) + h^{-1} = kd\lambda_{h^{-1}}(g) \in N. \end{aligned}$$

Hence N is an ideal of the left brace G. In particular, the multiplicative group of N is a normal subgroup of the structure group G. The natural homomorphism $\pi\colon G \longrightarrow G/N$ is in fact a homomorphism of left braces. Since the additive group of the left brace G is free abelian with basis X, the restriction of π to D_1 is a bijection

$$\pi|_{D_1} : D_1 \longrightarrow G/N.$$

Let

$$\sigma = (\pi|_{D_1})^{-1}.$$

We have that $\pi(\sigma(f)) = f$, for all $f \in G/N$. We know by [33] that M admits a presentation as a monoid

$$\langle X \mid xy = zt \text{ whenever } r(x, y) = (z, t)\rangle.$$

The set of atoms of M is X. Let $\overline{X} = \pi(X)$. Let $\|a\|_{\overline{X}}$ denote the length of a shortest decomposition of $a \in G/N$ as a product of elements of $\overline{X}$. Let $a \in G/N$ and

$$\sigma(a) = \sum_{x \in X} a_x x,$$

for some $a_x \in \mathbb{N}$. By Lemma 9.10,

$$\|a\|_{\overline{X}} = \sum_{x \in X} a_x.$$

Hence, for $f, g \in G/N$,

$$\|f\|_{\overline{X}} + \|g\|_{\overline{X}} = \|fg\|_{\overline{X}}$$

if and only if

$$\sigma(f)\sigma(g) = \sigma(fg).$$

Since $kd > 1$, for $x, y \in X$, $xy \notin D_1$ if and only if

$$kd = 2 \quad \text{and} \quad xy = x + \lambda_x(y) = 2x,$$

that is if and only if $kd = 2$ and $\lambda_x(y) = x$. In this case,

$$r(x,y) = (\lambda_x(y), \lambda^{-1}_{\lambda_x(y)}(x)) = (x,y).$$

Now it is easy to see that M admits a presentation

$$\langle \sigma(G/N) \mid \{\sigma(f)\sigma(g) = \sigma(fg) \mid f,g \in G/N \text{ and } \|f\|_{\overline{X}} + \|g\|_{\overline{X}} = \|fg\|_{\overline{X}}\}\rangle.$$

Therefore the result follows. □

Now give an intriguing connection between multiplicative groups of left braces and fundamental problems on integral group rings.

Proposition 9.16 (Sysak, [56],[57]) *Let G be a group. Then G is the multiplicative group of a left brace if and only if there exists a left ideal L of $\mathbb{Z}[G]$ such that*

(i) *the augmentation ideal* $\omega(\mathbb{Z}[G]) = G - 1 + L$ *and*

(ii) $G \cap (1 + L) = \{1\}$.

Proof — Suppose that there exists a left ideal L of $\mathbb{Z}[G]$ satisfying (i) and (ii). Let $a, b \in G$. Then by (i) there exist $c \in G$ and $\alpha \in L$ such that $a - 1 + b - 1 = c - 1 + \alpha$. Furthermore, if

$$a - 1 + b - 1 = d - 1 + \beta,$$

for $d \in G$ and $\beta \in L$, then $c - d \in L$. Hence $d^{-1}c - 1 \in L$ and, by (ii), $d^{-1}c = 1$. Thus there is a unique $c \in G$ such that

$$a - 1 + b - 1 - c + 1 \in L.$$

We define a sum $\oplus$ on G by

$$(a \oplus b) - a - b + 1 \in L,$$

for $a, b \in G$.

Clearly

$$a \oplus b = b \oplus a.$$

Let $a, b, c \in G$. Then

$$((a \oplus b) \oplus c) - (a \oplus b) - c + 1 \in L.$$

Since

$$(a \oplus b) - a - b + 1 \in L,$$

we have that

$$((a \oplus b) \oplus c) - a - b - c + 2 \in L.$$

Since

$$(b \oplus c) - b - c + 1 \in L,$$

we have

$$((a \oplus b) \oplus c) - a - (b \oplus c) + 1 \in L.$$

Therefore

$$(a \oplus b) \oplus c = a \oplus (b \oplus c).$$

Note that

$$(a \oplus 1) - a - 1 + 1 \in L.$$

Therefore

$$a^{-1}(a \oplus 1) \in 1 + L,$$

and by (ii), $a \oplus 1 = a$. Furthermore, for $a \in G$, there exists a unique $\ominus a \in G$ such that

$$1 - a - (\ominus a) + 1 \in L.$$

Then

$$a \oplus (\ominus a) = 1.$$

Hence $(G, \oplus)$ is an abelian group. Let $a, b, c \in G$. Then

$$\begin{aligned} &(c(a \oplus b) \oplus c) - ca - cb + 1 \\ &= (c(a \oplus b) \oplus c) - c(a \oplus b) - c + 1 + c(a \oplus b) + c - 1 - ca - cb + 1 \\ &= (c(a \oplus b) \oplus c) - c(a \oplus b) - c + 1 + c((a \oplus b) - a - b + 1) \in L. \end{aligned}$$

Therefore

$$c(a \oplus b) \oplus c = ca \oplus cb.$$

Thus G is the multiplicative group of a left brace.

Suppose now that G is the multiplicative group of a left brace. Denote by $\oplus$ the sum of the left brace G. Let I be the additive subgroup of $\omega(\mathbb{Z}[G])$ generated by all the elements of the form

$$(a \oplus b) - a - b + 1,$$

for $a, b \in G$. We shall see that I is a left ideal of $\mathbb{Z}[G]$. To prove this, it is sufficient to show that $c((a \oplus b) - a - b + 1) \in I$, for all $a, b, c \in G$. Note that

$$\begin{aligned} c((a \oplus b) - a - b + 1) &= c(a \oplus b) - ca - cb + c \\ &= (c(a \oplus b) \oplus c) - (c(a \oplus b) \oplus c) \\ &\quad + c(a \oplus b) - ca - cb + c \\ &= (ca \oplus cb) - (c(a \oplus b) \oplus c) + c(a \oplus b) - ca - cb + c \\ &= (ca \oplus cb) - ca - cb + 1 \\ &\quad - (c(a \oplus b) \oplus c) + c(a \oplus b) + c - 1 \in I. \end{aligned}$$

Therefore I is a left ideal.

Let

$$\alpha = \sum_{x \in G} \alpha_x x \in \omega(\mathbb{Z}[G]).$$

We shall prove that $\alpha \in G - 1 + I$ by induction on

$$\sum_{x \in G} |\alpha_x|.$$

If

$$\sum_{x \in G} |\alpha_x| = 0,$$

then $\alpha = 0 = 1 - 1 \in G - 1 + I$. If

$$\sum_{x \in G} |\alpha_x| = 2,$$

then $\alpha = x - y$, for some $x, y \in G$ with $x \neq y$. In this case, let $z \in G$ such that $y \oplus z = 1$. Then

$$\begin{aligned} \alpha &= x - 1 + (y \oplus z) - y - z + 1 + z - 1 \\ &= (x \oplus z) - 1 - (x \oplus z) + x + z - 1 + (y \oplus z) - y - z + 1 \in G - 1 + I. \end{aligned}$$

Suppose that

$$\sum_{x \in G} |\alpha_x| = n > 2$$

and that

$$\beta \in G - 1 + I,$$

for all

$$\beta = \sum_{x \in G} \beta_x x \in \omega(\mathbb{Z}[G])$$

such that

$$\sum_{x \in G} |\beta_x| < n.$$

Because

$$\alpha \in \omega(\mathbb{Z}G)$$

there exist $x, y \in G$ such that $\alpha_x \alpha_y < 0$. By symmetry we may assume that $\alpha_x < 0$. Then,

$$\beta = \alpha + x - y \in G - 1 + I,$$

by the induction hypothesis, and therefore

$$\alpha = y - x + g - 1 + \gamma,$$

for some $g \in G$ and some $\gamma \in I$. Since

$$y - x = h - 1 + \delta$$

for some $h \in G$ and some $\delta \in I$, we have that

$$\alpha = h + g - 2 + \gamma + \delta = (h \oplus g) - 1 - (h \oplus g) + h + g - 1 + \gamma + \delta \in G - 1 + I.$$

Hence

$$\omega(\mathbb{Z}[G]) = G - 1 + I.$$

Note that $\omega(\mathbb{Z}[G])$ is the free abelian group

$$\bigoplus_{g \in G} \mathbb{Z}(g - 1).$$

Let

$$\psi \colon \omega(\mathbb{Z}[G]) \longrightarrow (G, \oplus)$$

be the morphism of abelian groups such that

$$\psi(g - 1) = g.$$

It is easy to see that $I \subseteq \ker(\psi)$. Therefore

$$G \cap (1 + I) = \{1\}.$$

The proof is complete. $\square$

In a similar way we can prove the following result.

Proposition 9.17 *Let* G *be a group. Then* G *is the multiplicative group of a two-sided brace if and only if there exists an ideal* L *of* $\mathbb{Z}[G]$ *such that*

(i) *the augmentation ideal* $\omega(\mathbb{Z}[G]) = G - 1 + L$ *and*

(ii) $G \cap (1 + L) = \{1\}$.

Proposition 9.17 for finite groups essentially was proven by Sandling (see [53], Theorem 1.5). It is a crucial property to prove the following positive solution to the isomorphism problem of integral group rings of adjoint groups of finite radical rings (see also [44], Section 9.4, for a proof of this result).

Theorem 9.18 (see Sandling [53], Theorem 3.1) *Let* G *be a finite group isomorphic to the adjoint group of a radical ring. If* H *is a group such that*

$$\mathbb{Z}[G] \simeq \mathbb{Z}[H],$$

then $G \simeq H$.

Roggenkamp and Scott gave in [45] an affirmative answer to the isomorphism problem for finite nilpotent groups, thus generalizing the result of Sandling.

Remark 9.19 Suppose that for a group G, there exists a left ideal L of $\mathbb{Z}[G]$ such that

$$\omega(\mathbb{Z}[G]) = G - 1 + L$$

and

$$G \cap (1 + L) = \{1\}.$$

Let α be a unit in $\mathbb{Z}[G]$ of augmentation 1. Then there exist $g \in G$ and $\beta \in L$ such that

$$\alpha - 1 = g - 1 + \beta.$$

Thus $\alpha = g(1 + g^{-1}\beta)$. Thus the group of units of $\mathbb{Z}[G]$ is

$$\mathcal{U}(\mathbb{Z}[G]) = (\pm G)H,$$

where

$$H = (1 + L) \cap \mathcal{U}(\mathbb{Z}[G]).$$

Furthermore, since $G \cap (1 + L) = \{1\}$, we have that

$$(\pm G) \cap H = \{1\}.$$

If L is a two-sided ideal, then H is a normal subgroup of $\mathcal{U}(\mathbb{Z}[G])$. Such normal subgroups H are called normal complements in the group of units of the group ring. The existence of normal complements is related with the isomorphism problem. For finite nilpotent groups, an affirmative answer to the existence of normal complements implies an affirmative answer to the isomorphism problem [54], Proposition (30.4). The existence of normal complements is known for finite nilpotent groups of class 2. But for general finite nilpotent groups it remains an open question (see [54], Section 34 and Problem 30).

10 Open problems

Problem 10.1 (see [18], Question 2.1(2)) *Let B be a left brace. Assume that the operation $*$, defined by $a * b = ab - a - b$, for all $a, b \in B$, is associative. Is B a two-sided brace?*

With the additional hypothesis that the additive group of B has no elements of order 2, the answer is positive (see [18], Proposition 2.2).

Note that a left brace B is a two-sided brace if and only if

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

for all $a, b, c \in B$. In fact, for $a, b, c \in B$,

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

and

$$a * c + b * c = ac - a - c + bc - b - c,$$

thus $(a + b) * c = a * c + b * c$ if and only if $(a + b)c + c = ac + bc$.

Problem 10.2 (see [8], Problem 5.1) *Describe the structure of all left braces of order p^n, for a prime p. And describe the group $\mathrm{Aut}(B, +, \cdot)$ of automorphisms for all such left braces.*

We know that all finite non-trivial simple left braces are special matched products of left braces $B_1, \dots, B_n$ of orders $p_1^{m_1}, \dots, p_n^{m_n}$, for $n > 1$, distinct primes $p_1, \dots, p_n$ and positive integers $m_1, \dots, m_n$. Thus in order to classify all finite simple left braces, to solve this problem seems crucial.

Also for the classification of the finite simple left braces the following two problems are interesting.

Problem 10.3 (see [8], Problem 5.2) *Determine for which prime numbers* p, q *and positive integers* α, β, *there exists a simple left brace of cardinality* $p^\alpha q^\beta$.

Problem 10.4 *Classify all the finite simple left braces such that every simple homomorphic image of each proper subbrace is trivial.*

Problem 10.5 *Let* G *be a nilpotent group of nilpotency class 2. Is* G *isomorphic to the multiplicative group of a two-sided brace? Is* G *isomorphic to the multiplicative group of a left brace?*

In [1] Ault and Watters conjectured that every nilpotent group of class 2 is the adjoint group of a nilpotent ring of nilpotency index 3. They show that this is true for nilpotent groups G of class 2 that satisfies one of the following properties:

(i) $G/Z(G)$ is a weak direct product of cyclic groups.

(ii) $G/Z(G)$ is a torsion group.

(iii) Every element of $[G, G]$ has a unique square root.

In [36] Hales and Passi gave a counterexample to the conjecture of Ault and Watters. They also showed that a nilpotent group G of class 2 is the adjoint group of a nilpotent ring of nilpotency index 3 if it satisfies any of the following properties:

(iv) $G/Z(G)$ is a uniquely 2-divisible group.

(v) G/N is a torsion-free group and completely decomposable (i. e. a weak direct product of rank one groups) for some normal subgroup N such that $[G, G] \subseteq N \subseteq Z(G)$.

Proposition 10.6 (see [21], Proposition 4) *Let* G *be a nilpotent group of class 2. Let* H *be the subgroup* $H = \{g^2 z \mid g \in G,\ z \in Z(G)\}$ *of* G. *Then the operation* $+$ *defined on* H *by*

$$h_1^2 z_1 + h_2^2 z_2 = (h_1 h_2)^2 z_1 z_2 [h_2, h_1]$$

for $h_1, h_2 \in G$ *and* $z_1, z_2 \in Z(G)$*, is well defined and* $(H, +, \cdot)$ *is a two-sided brace. The radical ring associated to the two-sided brace* H *is nilpotent of nilpotency index at most* 3*. Furthermore, the solution of the Yang-Baxter equation associated to the brace* H *is square free.*

Problem 10.7 *Let* G *be a finite nilpotent group of nilpotency class* 3*. Is* G *isomorphic to the multiplicative group of a left brace.*

Note if p is an odd prime, then the group

$$\langle a, b \mid a^p = b^p = [a,b]^p = [[a,b],a]^p = [[a,b],b]^p = 1$$
$$\text{and } \ [[a,b],a], [[a,b],b] \text{ are central}\rangle$$

is not isomorphic to the multiplicative group of a two-sided brace (see [42]). But, by [22] (Theorem 2.1), it is isomorphic to the multiplicative group of a left brace.

Problem 10.8 *Let* G *be a finite nilpotent group of nilpotency class* $c < 9$*. Is* G *isomorphic to the multiplicative group of a left brace.*

By [4], there is a finite nilpotent group (in fact, a p-group for some prime p) of nilpotency class 9 which is not isomorphic to the multiplicative group of any left brace.

Problem 10.9 *Characterize the finite nilpotent groups that are multiplicative groups of a left brace.*

Problem 10.10 *Characterize the finite nilpotent groups that are multiplicative groups of a two-sided brace.*

This is equivalent to characterize the finite nilpotent groups that are isomorphic to the circle group of a finite nilpotent ring. In [42] one can find an obstruction to this.

Acknowledgment

I would like to thank David Bachiller, Eric Jespers and Jan Okniński to share with me many ideas and friendship. I would also like to thank Tatiana Gateva-Ivanova, Ángel del Río, Agata Smoktunowicz and Leandro Vendramin for their pleasant collaboration.

REFERENCES

[1] J. C. Ault – J. F. Watters: "Circle groups of nilpotent rings", *Amer. Math. Monthly* 80 (1973), 48–52.

[2] D. Bachiller: "Study of the Algebraic Structure of Left Braces and the Yang-Baxter Equation", Ph.D. thesis, *Universitat Autònoma de Barcelona* (2016).

[3] D. Bachiller: "Classification of braces of order p^3", *J. Pure Appl. Algebra* 219 (2015), 3568–3603.

[4] D. Bachiller: "Counterexample to a conjecture about braces", *J. Algebra* 453 (2016), 160–176.

[5] D. Bachiller: "Extensions, matched products and simple braces", *J. Pure Appl. Algebra* 222 (2018), 1670–1691.

[6] D. Bachiller: "Solutions of the Yang-Baxter equation associated to skew left braces, with applications to racks", *J. Knot Theory Ramifications*; arXiv:1611.08138v1[math.QA].

[7] D. Bachiller – F. Cedó – E. Jespers: "Solutions of the Yang-Baxter equation associated with a left brace", *J. Algebra* 463 (2016), 80–102.

[8] D. Bachiller – F. Cedó – E. Jespers – J. Okniński: "Iterated matched products of finite braces and simplicity; new solutions of the Yang-Baxter equation", *Trans. Amer. Math. Soc* 370 (2018), 4881–4907.

[9] D. Bachiller – F. Cedó – E. Jespers – J. Okniński: "Asymmetric product of left braces and simplicity; new solutions of the Yang-Baxter equation"; arXiv:1705.08493v1[math.QA].

[10] D. Bachiller – F. Cedó – L. Vendramin: "A characterization of finite multipermutation solutions of the Yang-Baxter equation", *Publ. Mat.*, to appear; arXiv:1701.09109v3[math.GR].

[11] N. Ben David: "On Groups of Central Type and Involutive Yang-Baxter Groups: a Cohomological Approach", Ph.D. thesis, *Technion*, Haifa (2012).

[12] N. Ben David – Y. Ginosar: "On groups of central type, non-degenerate and bijective cohomology classes", *Israel J. Math.* 172 (2009), 317–335.

[13] N. Ben David – Y. Ginosar: "On groups of I-type and involutive Yang-Baxter groups", *J. Algebra* 458 (2016), 197–206

[14] D. Burde: "Affine structures on nilmanifolds", *Int. J. Math.* 7 (1996), 599–616.

[15] F. Catino – I. Colazzo – P. Stefanelli: "Regular subgroups of the afine group and asymmetric product of braces", *J. Algebra* 455 (2016), 164–182.

[16] F. Catino – R. Rizzo: "Regular subgroups of the affine group and radical circle algebras", *Bull. Austral Math. Soc.* 79 (2009), 103–107.

[17] F. Cedó – T. Gateva-Ivanova – A. Smoktunowicz: "On the Yang-Baxter equation and left nilpotent left braces", *J. Pure Appl. Algebra* 221 (2017), 751–756.

[18] F. Cedó – T. Gateva-Ivanova – A. Smoktunowicz: "Braces and symmetric groups with special conditions", *J. Pure Appl. Algebra*, to appear; doi:10.1016/j.jpaa.2018.02.012.

[19] F. Cedó – E. Jespers – J. Okniński: "The Gelfand-Kirillov dimension of quadratic algebras satisfying the cyclic condition", *Proc. Amer. Math. Soc.* 134 (2006), 643–663.

[20] F. Cedó – E. Jespers – J. Okniński: "Retractability of the set theoretic solutions of the Yang-Baxter equation", *Adv. Math.* 224 (2010), 2472–2484.

[21] F. Cedó – E. Jespers – J. Okniński: "Braces and the Yang-Baxter equation", *Comm. Math. Phys.* 327 (2014), 101–116.

[22] F. Cedó – E. Jespers – J. Okniński: "Nilpotent groups of class three and braces", *Publ. Mat.* 60 (2016), 55–79.

[23] F. Cedó – E. Jespers – J. Okniński: "Braces and the Yang-Baxter equation"; arXiv:1205.3587v1[math.RA].

[24] F. Cedó – E. Jespers – Á. del Río: "Involutive Yang-Baxter groups", *Trans. Amer. Math. Soc.* 362 (2010), 2541–2558.

[25] F. Chouraqui: "Garside groups and the Yang-Baxter Equation", *Comm. Algebra* 38 (2010), 4441–4460.

[26] P. Dehornoy: "Set-theoretic solutions of the Yang-Baxter equation, RC-calculus, and Garside germs", *Adv. Math.* 282 (2015), 93–127.

[27] V.G. Drinfeld: "On unsolved problems in quantum group theory. Quantum Groups", Lecture Notes Math. 1510, *Springer*, Berlin (1992), 1–8.

[28] P. Etingof – S. Gelaki: "A method of construction of finite-dimensional triangular semisimple Hopf algebras", *Math. Res. Let.* 5 (1998), 551–561.

[29] P. Etingof – T. Schedler – A. Soloviev: "Set-theoretical solutions to the quantum Yang-Baxter equation", *Duke Math. J.* 100 (1999), 169–209.

[30] T. Gateva-Ivanova: "A combinatorial approach to the set-theoretic solutions of the Yang-Baxter equation", *J. Math. Phys.* 45 (2004), 3828–3858.

[31] T. Gateva-Ivanova – P. Cameron: "Multipermutation solutions of the Yang-Baxter equation", *Comm. Math. Phys.* 309 (2012), 583–621.

[32] T. Gateva-Ivanova – S. Majid: "Matched pairs approach to set theoretic solutions of the Yang-Baxter equation", *J. Algebra* 319 (2008), no. 4, 1462–1529.

[33] T. Gateva-Ivanova – M. Van den Bergh: "Semigroups of I-type", *J. Algebra* 206 (1998), 97–112.

[34] I. Goffa – E. Jespers: "Monoids of IG-type and maximal orders", *J. Algebra* 308 (2007), 44–62.

[35] L. Guarnieri – L. Vendramin: "Skew braces and the Yang-Baxter equation", *Math. Comp.*, to appear; arXiv:1511.03171.

[36] A. W. Hales – I. B. S. Passi: "The second augmentation quotient of an integral group ring", *Arch. Math. (Basel)* 31 (1978), 259–265.

[37] P. Hegedűs: "Regular subgroups of the affine group", *J. Algebra* 225 (2000), 740–742.

[38] B. Huppert: "Endliche Gruppen I", *Springer*, Berlin (1967).

[39] E. Jespers – J. Okniński: "Monoids and Group of I-Type", *Algebr. Represent. Theory* 8 (2005), 709–729.

[40] E. Jespers – J. Okniński: "Noetherian Semigroup Rings", *Springer*, Dordrecht (2007).

[41] C. Kassel: "Quantum Groups", *Springer*, New York (1995).

[42] R.L. Kruse: "On the circle group of a nilpotent ring", *Amer. Math. Monthly* 77 (1970),168–170.

[43] V. Lebed – L. Vendramin: "Cohomology and extensions of braces", *Pacific J. Math.* 284 (2016), 191–212.

[44] C. Polcino Milies – S.K. Sehgal: "An Introduction to Group Rings", *Kluwer*, Dordrecht (2002).

[45] K.W. Roggenkamp – L.L. Scott: "Isomorphisms of p-adic group rings", *Ann. Math.* 126 (1987), 593–647.

[46] W. Rump: "A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation", *Adv. Math.* 193 (2005), 40–55.

[47] W. Rump: "Modules over braces", *Algebra Discrete Math.* (2006), 127–137.

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

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

[50] W. Rump: "Generalized radical rings, unknotted biquandles, and quantum groups", *Colloq. Math.* 109 (2007), 85–100.

[51] W. Rump: "Semidirect products in algebraic logic and solutions of the quantum Yang-Baxter equation", *J. Algebra Appl.* 7 (2008), 471–490.

[52] W. Rump: "Addendum to "Generalized radical rings, unknotted biquandles, and quantum groups" (Colloq. Math. 109 (2007), 85–100)", *Colloq. Math.* 117 (2009), 295–298.

[53] R. Sandling: "Group rings of circle and unit groups", *Math. Z.* 140 (1974), 195–202.

[54] S.K. Sehgal: "Units in Integral Group Rings", *Pitman*, Essex (1993).

[55] A. Smoktunowicz: "On Engel groups, nilpotent groups, rings, braces and the Yang-Baxter equation", *Trans. Amer. Math. Soc*, to appear; doi:10.1090/tran/7179; arXiv:1509.00420v4[math.RA].

[56] Y.P. Sysak: "Product of groups and the quantum Yang-Baxter equation", notes of a talk in Advances in Group Theory and Applications, Porto Cesareo (2011).

[57] Y.P. Sysak: "The adjoint group of radical rings and related questions" in: Ischia Group Theory 2010 (proceedings of the conference: Ischia, Naples, Italy, 14-17 April 2010), 344–365, *World Scientific*, Singapore (2011).

[58] 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.

Ferran Cedó
Departament de Matemàtiques
Universitat Autònoma de Barcelona
08193 Bellaterra, Barcelona (Spain)
e-mail: cedo@mat.uab.cat