Module braces: relations between the additive and the multiplicative groups

Ilaria Del Corso

Received: 9 October 2022 / Accepted: 14 June 2023 / Published online: 12 July 2023
© The Author(s) 2023

Abstract
In this paper, we define a class of braces that we call module braces or \( R \)-braces, which are braces for which the additive group has also a module structure over a ring \( R \), and for which the values of the gamma functions are automorphisms of \( R \)-modules. This class of braces has already been considered in the literature in the case where the ring \( R \) is a field; we generalise the definition to any ring \( R \), reinterpreting it in terms of the so-called gamma function associated with the brace, and prove that this class of braces enjoys all the natural properties one can require. We exhibit explicit example of \( R \)-braces, and we study the splitting of a module braces in relation to the splitting of the ring \( R \), generalising thereby Byott’s result on the splitting of a brace with nilpotent multiplicative group as a sum of its Sylow subgroups. The core of the paper is in the last two sections, in which, using methods from commutative algebra and number theory, we study the relations between the additive and the multiplicative groups of an \( R \)-brace showing that if a certain decomposition of the additive group is small (in some sense which depends on \( R \)), then the additive and the multiplicative groups have the same number of elements of each order. In some cases, this result considerably broadens the range of applications of the results already known on this issue.

Keywords Skew braces · Brace · Radical rings · Modules

Mathematics Subject Classification 16XX

1 Introduction

A brace is an algebraic structure introduced by Rump in [37] as a generalisation of a radical ring. On a radical ring \( N \), besides the usual additive group structure, one can define another
group operation, called the adjoint operation, giving on \( N \) an additional group structure; the two operations on \( N \) are linked by the “compatibility relation”

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

for \( x, y, z \in N \).

A (left) brace is an abelian group \((N, +)\), together with an additional group structure \((N, \circ)\) such that the two operations are linked by the same compatibility relation as that of the radical rings.

In the paper [30], the authors further generalised this concept by defining a skew (left) brace as a brace without the requirement on the first group to be abelian. For the skew brace \((N, +, \circ)\), the notation of braces is kept: \((N, +)\) is called the additive group, and \((N, \circ)\) the multiplicative group.

With the paper [30], a systematic study was begun of the properties of these structures, which turn out to be very interesting since they naturally appear in many mathematical contexts.

First of all, we recall that skew braces can be described in terms of regular subgroups of the holomorph. In fact, for a fixed group \((N, +)\), the skew braces with additive group \((N, +)\) correspond to the regular subgroups of \(\text{Hol}(N)\). As shown in [30, Theorem 4.2] (see also [15–17]), the regular subgroup of the holomorph are in turn in one-to-one correspondence with the functions

\[
\gamma : N \to \text{Aut}(N)
\]

classified by the functional equation

\[
\gamma(x + \gamma_x(y)) = \gamma_x \gamma_y.
\]

We call these functions gamma functions; in the literature, they are usually referred to as \(\lambda\)-functions.

The study of the Yang–Baxter equation has been the motivation for the definition and for the study of skew braces. In fact, braces were introduced by Rump to study non-degenerate involutive set-theoretic solutions of the Yang–Baxter equation, and in [30], skew braces are introduced to include the non-involutive case.

The study of skew braces is strictly related also to that of the Hopf–Galois structures on a finite Galois extension \(L/K\). The work of Greither and Pareigis in [29] and that of Childs [18] and Byott [5] showed that if \(\Gamma = \text{Gal}(L/K)\), to each Hopf–Galois structure on \(L/K\), one can associate a group \((G, +)\) with the same cardinality as \(\Gamma\) and such that the holomorph \(\text{Hol}(G)\) of \((G, +)\) contains a regular subgroup isomorphic to \(\Gamma\). Since classifying the regular subgroups of \(\text{Hol}(G)\) is equivalent to determining the operations “\(\circ\)” on \(G\) such that \((G, +, \circ)\) is a (left) skew brace, the Hopf–Galois structures on an extension with Galois group isomorphic to a group \(\Gamma\) correspond bijectively to the skew braces \((G, +, \circ)\) with \((G, \circ) \cong \Gamma\). This connection was first observed by Bachiller in [4, §2], and it is described in detail in the appendix to [43] by Byott and Vendramin (see also [42] for a slightly different point of view).

In recent years, these different approaches concurred to construct a rich theory. A number of papers are devoted to the enumeration of the skew braces (or, equivalently, the Hopf–Galois structures) whose cardinality has a particular form, and their isomorphism classes [1–3, 5, 6, 10, 11, 19, 32, 35].

Part of the literature is devoted to understanding how properties of \((G, +)\) influence those of \((G, \circ)\) and vice versa, when \((G, +, \circ)\) is a skew brace [4, 7, 8, 14, 27, 34, 44, 45]. Another
part concerns the study of skew braces of a particular type, e.g., nilpotent skew braces (see [23, 40]), bi-skew braces (see [9, 20, 41]).

In this paper, we address the latter two aspects. We define a class of braces, that we call module braces or $R$-braces, which are braces for which the additive group has also a module structure over a ring $R$ and for which the values of the gamma function are automorphisms of $R$-modules (see Definition 2). The class of $\mathbb{Z}$-braces is the class of braces defined by Rump.

$R$-brace has already been considered in the literature in the case where the ring $R$ is a field (see [12, 13, 39, 40], where also some applications of this structure are provided). We generalise the definition given there to any ring $R$, reinterpreting it in terms of the gamma function associated with the brace. This class turns out to be very natural; in fact, it enjoys many of the natural properties one can expect, and their properties can be handily described via gamma functions.

In some cases, this more general context ($R$-brace instead of $\mathbb{Z}$-brace) allows a more conceptual view of classical results on braces, and formulations more suitable for generalisations.

This is the case of Proposition 3.7 in which we study the splitting of a module braces in relation to the splitting of the ring $R$, generalising the splitting of a brace with nilpotent multiplicative group as a sum of its Sylow subgroups (see Remark 3.9), which is the central point of [7, Theorem 1] (see also [23, Corollary 4.3] and [10, Subs. 2.4]).

We also study the relations between the additive and the multiplicative groups of an $R$-brace, in the case when the additive group is small, in the sense of [27, Theorem 1] and [4, Theorem 2.5]. By introducing tools from commutative algebra and number theory, we are able to obtain, in Theorem 4.1 and its corollaries, a complete generalisation of that results.

The paper is organised as follows.

In Sect. 2, we introduce all the notation and main results on skew braces we will need, restating the definitions and some basic results in terms of the gamma function associated with a skew braces. Although we will apply the machinery in the more specific context of braces, we develop it in full generality, as it could have an independent interest. Moreover, the general treatment requires hardly more effort and helps to place our results within the general theory.

In Sect. 3, we define module braces and prove that substructures can be naturally defined and have a good behaviour with respect to the usual operations. We also construct explicit example of $R$-braces and show that the brace associated with any radical ring with an $R$-algebra structure, over a commutative ring $R$, is always an $R$-brace.

As we already mentioned, in Proposition 3.7, we study the splitting of an $R$-brace in relation to the splitting of the (commutative) ring $R$, showing that, in some cases, to this decomposition corresponds a splitting of an $R$-brace. The condition we have on $R$-braces when specified for $R = \mathbb{Z}$ corresponds to the nilpotence of the multiplicative group of the brace and its splitting to that given in [7, Theorem 1] as a sum of the Sylow subgroups.

Section 4 is the core of the paper. At the beginning of the section, we state, in Theorem 4.1, the following generalisation of [27, Theorem 1] and [4, Theorem 2.5], which is proved in Sect. 5.

**Theorem** Let $p$ be a prime number, and let $D$ be a PID such that $p$ is a prime in $D$. Let $(N, +, \circ)$ be a $D$-brace of order a power of $p$.

Assume that the number of cyclic factors of the decomposition of $N$ as a sum of cyclic $D$-module is $< p - 1$.

Then, $(N, +)$ and $(N, \circ)$ have the same number of elements of each order. In particular, if $(N, \circ)$ is abelian, then $(N, +) \cong (N, \circ)$. 
For $D = \mathbb{Z}$, the previous theorem is [4, Theorem 2.5]. A family of rings $D$ fulfilling the assumption of the previous theorem is given by the rings of integers of unramified extensions of $\mathbb{Q}_p$, the field of $p$-adic numbers. In Sect. 4, after introducing the necessary tools of number theory and commutative algebra, we show that these rings of integers play a fundamental role in this context, since every $R$-brace of order a power of $p$ is also naturally a module over one of such rings (see Proposition 4.10), showing that the assumption on the ring $D$ in the theorem is less restrictive than it might appear. This section also contains some corollaries that apply the theorem to specific cases.

The advantage of appealing to Theorem 4.1, instead of to [4, Theorem 2.5], when dealing with $D$-braces, is that the condition of having few cyclic factors in the $D$-module decomposition can be much weaker than the condition of having few cyclic factors in the $\mathbb{Z}$-module decomposition (see Lemma 4.5). Therefore, in some cases, the use of Theorem 4.1, instead of its classic form, considerably broadens the range of application.

In a forthcoming paper, we will show how Theorem 4.1 and its corollaries can be used to make some progress in the study of Fuchs’ question on the group of units of a ring (see Remark 4.14).

2 Skew braces and the nilpotency series

In this section, we briefly recall the basic of the skew braces language introduced in [30] with a particular emphasis on gamma functions (see [10, 15]). We also introduce the right series of a skew left brace, following the notation given in [31].

2.1 Skew braces and ideals

Let $N$ be a set, and let “$+$” and “$\circ$” be two group operations on $N$.

$(N, +, \circ)$ is a skew left brace if the following brace axiom holds for $x, y, z \in N$

$$x \circ (y + z) = (x \circ y) - x + (x \circ z). \quad (1)$$

Analogously, we say that $(N, +, \circ)$, is skew right brace if, for $x, y, z \in N$,

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

In the following, we will simply call skew brace a skew left brace, and we refer to $(N, +)$ as the additive group and to $(N, \circ)$ as the multiplicative group of the skew brace.

From the brace axiom, it follows that the two group structures of a skew brace have the same unit element, which we will denote by 0.

Starting from any group $(N, +)$ and doubling the operation, we get a (left and right) skew brace $(N, +, +)$ called the trivial skew brace.

For a skew brace $(N, +, \circ)$, Eq. (1) can be rewritten as

$$-x + x \circ (y + z) = -x + (x \circ y) - x + (x \circ z). \quad (3)$$

If $(N, +, \circ)$ is a skew brace, then (3) and the fact that $(N, \circ)$ is a group yield that for all $x \in N$ the maps $N \to N$ given by

$$\gamma_x : y \mapsto -x + x \circ y$$
are automorphisms of \((N, +)\), and that \(\gamma : (N, \circ) \to \text{Aut}(N, +)\) defined by \(\gamma(x) = \gamma_x\) is a homomorphism, namely
\[
\gamma(x \circ y) = \gamma(x)\gamma(y)
\]
for all \(x, y \in N\).

Conversely, given a group \((N, +)\), we say that a map \(\gamma : N \to \text{Aut}(N, +)\) is a \textit{gamma function} if it verifies the following gamma functional equation
\[
\gamma(x + \gamma_x(y)) = \gamma(x)\gamma(y)
\]
(4)
for each \(x, y \in N\).

For a given gamma function on \((N, +)\), we can define an operation on \(N\) by
\[
x \circ y = x + \gamma(y),
\]
(5)
for \(x, y \in N\).

It is easy to check that given the gamma function \(\gamma\) the operation \(\circ\) as in (5) gives a group structure on \(N\) and that (1) holds, so and \((N, +, \circ)\) is a skew brace. (See [10, after Theorem 2.2] for the explicit correspondence between the properties of \(\gamma\) and those of \(\circ\). Notice that there the case is considered of right skew braces.)

We also recall that a skew brace structure can be defined also starting from a group \((N, +)\) with an additional binary operation usually, denoted by \(\star\) such that
\[
x \star (y + z) = x \star y + y + x \star z - y
\]
(6)
for all \(x, y, z \in N\), with the additional condition that the operation \(\circ\) defined by
\[
x \circ y = x + x \star y + y
\]
(7)
defines on \(N\) a group structure (see [23, Theorem 1.4]).

In terms of the gamma function associated with the skew brace, we have
\[
x \star y = \gamma_x(y) - y.
\]
(8)
Vice versa, given a (left) skew brace \((N, +, \circ)\), then
\[
x \star y = -x + x \circ y - y
\]
verifies (6). The construction of a skew brace via the \(\star\) operation generalises that made by Rump for braces.

A left (right) \textit{brace} is a skew left (right) brace with abelian additive group and was introduced in [37] as a generalisation of radical rings. In fact, if \((N, +, \cdot)\) is a radical ring, taking \(\star\) to be the product of the ring, and the operation \(\circ\) as in (7), we get that \((N, +, \circ)\) is two-sided brace, namely a brace for which both (1) and (2) hold. In this case, we will refer to the operation \(\circ\) as the adjoint operation, and to \((N, \circ)\) as to the adjoint group of the radical ring.

On the contrary, if \((N, +, \circ)\) is a two-sided brace, then defining
\[
x \cdot y = -x + x \circ y - y,
\]
we have that \((N, +, \cdot)\) is a radical ring (see [36] or [21, Prop. 1]). In this case, \((1 + N, \cdot)\) and \((N, \circ)\) are isomorphic groups via the map \(1 + x \to x\).

As for the gamma function associated with the brace \((N, +, \circ)\) arising from a radical ring, we have
\[
\gamma_x(y) = -x + x \circ y = (x + 1)y.
\]
Definition 1 A subset $A$ of a skew brace $(N, +, \circ)$ is called
- a subskew brace if it is a subgroup both of $(N, +)$ and $(N, \circ)$;
- a left ideal if it is $\gamma(N)$ invariant, namely $\gamma_x(A) \subseteq A$ for each $x \in N$, and it is a subgroup for any (and hence for both) group structures;
- an ideal if it is $\gamma(N)$ invariant and it is a normal subgroup of both $(N, +)$ and $(N, \circ)$.

Clearly any ideal is a left ideal, and any left ideal is a subskew brace. The converse does not hold in general.

Notice that the gamma function of a subskew brace is the restriction of the gamma function of the skew brace.

We also recall that if $I$ is an ideal of the skew brace $N$, then $N/I$ has a structure of quotient group for both the operations, so it is a skew brace.

Two skew braces $N$ and $M$ are called isomorphic if there exists a map $f : N \rightarrow M$ which is an isomorphism for both the additive and the multiplicative structures.

Lemma 2.1 Let $(M, +, \circ)$ and $(N, +', \circ')$ be isomorphic skew braces. Let $\gamma$ and $\gamma'$ be the gamma functions attached to $M$ and $N$, respectively. Then, for each skew brace isomorphism $f : M \rightarrow N$, and for each $x \in M$, the following holds:

$$f \gamma_x = \gamma'_{f(x)} f.$$  \hfill (9)

Proof Let $x, y \in M$. Then,

$$f \gamma_x(y) = f(-x + x \circ y) = -' f(x) +' f(x) \circ' f(y) = \gamma_{f(x)}(f(y)).$$

The following corollary is an obvious consequence of the analogue result for groups and the previous lemma.

Corollary 2.2 An isomorphism between two skew braces $M$ and $N$ induces a one-to-one correspondence between the subskew braces, the left ideals and the ideals of $M$ and $N$.

2.2 Splitting of skew braces

The direct product of two skew braces $L$ and $M$ is the skew brace on the set $L \times M$ with additive (resp. multiplicative) group given by the direct product of the additive (resp. multiplicative) groups of $L$ and $M$.

If $\gamma_L$ and $\gamma_M$ are the gamma function associated with $L$ and $M$, respectively, then the gamma function associated with $L \times M$ is the map which associates with $(l, m) \in L \times M$ the automorphism $((\gamma_L)_l, (\gamma_M)_m)$.

If a skew brace $N$ is isomorphic to $L \times M$, then $L$ and $M$ are (isomorphic to) ideals of $N$.

[7, Theorem 1] is proven that if both groups of a finite skew brace $N$ are nilpotent, then $N$ is the direct product of skew braces of prime power order. The same has been also reobtained in [10, Theorem 2.6] using the gamma functions. The argument given there can be generalised to obtain the following.

Proposition 2.3 Let $N$ be a skew brace with associated gamma function $\gamma$. Assume that the additive group of $N$ is a direct sum of subgroups $N = \bigoplus_{j=1}^t I_j$, and for all $n \in N$, use the notation $n = \sum_{j=1}^t n_j$ with $n_j \in I_j$.

The following facts are equivalent.
(i) The map \( f : N \to I_1 \times \cdots \times I_t \) defined by \( f(\sum_{j=1}^t x_j) = (x_1, \ldots, x_t) \) is a skew brace isomorphism.

(ii) \( I_1, \ldots, I_t \) are ideals of \( N \).

(iii) For all \( x, y \in N \)

\[ \gamma_x(y) = \sum_{j=1}^t \gamma_{x_j}(y_j). \]

(iv) For all \( x, y \in N \)

\[ x \star y = \sum_{j=1}^t x_j \star y_j. \]

Proof (i) \( \Rightarrow \) (ii) is clear, and (ii) \( \Rightarrow \) (i) is [23, Theorem 4.2].

(i) \( \Rightarrow \) (iii) follows by recalling that the gamma functions associated to the ideals \( I_j \) are the restrictions of \( \gamma \), so, denoting by \( \gamma' \) the gamma function associated with their direct product, we have

\[ \gamma'_{(x_1, \ldots, x_t)} = (\gamma_{x_1}, \ldots, \gamma_{x_t}). \]

Therefore, using (9), we compute

\[ \gamma_x(y) = f^{-1}\gamma'_f(y) = f^{-1}\gamma'_{(x_1, \ldots, x_t)}(y_1, \ldots, y_t) = \sum_{j=1}^t \gamma_{x_j}(y_j). \]

As for the converse, we have to prove that the map \( f \), which is known to be an isomorphism of additive groups, is also a morphism of multiplicative groups, namely

\[ f(x \circ y) = f(x) \circ' f(y) \]

where \( \circ' \) denotes the product in \( I_1 \times \cdots \times I_t \). Now,

\[ f(x \circ y) = f(x + \gamma_x(y)) = f\left(\sum_{j=1}^t x_j + \sum_{j=1}^t \gamma_{x_j}(y_j)\right) = \sum_{j=1}^t (x_1 + \gamma_{x_1}(y_1), \ldots, x_t + \gamma_{x_t}(y_t)) = (x_1 \circ y_1, \ldots, x_t \circ y_t) = f(x) \circ' f(y). \]

Finally, the equivalence from (iii) and (iv) easily follows from (8).

\[ \square \]

2.3 Nilpotency and solubility of a skew brace

The operation \( \star \) associated with a skew brace \((N, +, \circ)\) is a commutator in \( \text{Hol}(N) = \text{Aut}(N) \rtimes N \), namely

\[ x \star y = \gamma_x(y) - y = [\gamma_x, y], \tag{10} \]

and it is a measure of the difference between the two operations.

For \( X, Y \) non-empty subsets of a skew brace \( N \), we let \( X \star Y \) be the additive subgroup of \((N, +)\) generated by the elements \( x \star y \) for \( x \in X \) and \( y \in Y \). Again, we can describe this set in terms of commutators in \( \text{Hol}(N) \), namely

\[ X \star Y = [\gamma(X), Y]. \]
We define \( N^{(1)} = N^1 = N_{(1)} = N \) and inductively
\[
N^{(k)} = N^{(k-1)} \ast N, \quad N^k = N \ast N^{k-1}, \quad N_{(k)} = N_{(k-1)} \ast N_{(k-1)}
\] (11)
for all \( k \geq 2 \). Also for \( k = 2 \), we have the equalities \( N^{(2)} = N^2 = N_{(2)} \).

2.3.1 The right series

All the elements of the series \( N^{(k)} \) are ideals of the skew brace (see [23, Proposition 2.1]), and therefore, the chain
\[
N = N^{(1)} \supseteq N^{(2)} \supseteq N^{(3)} \supseteq \cdots ,
\] (12)
is a filtration for the skew brace \( N \), and is called the right series of the skew brace.

The filtration of the right series is particularly interesting since it is has the property that the skew brace structure induced on the quotients of the filtration is the trivial one. So, this series makes it clear that there are important links between the additive and the multiplicative structure of a skew brace.

A skew brace \( N \) is called right nilpotent of class \( m \) if \( N^{(m)} \supseteq N^{(m+1)} = 0 \) for some \( m \geq 1 \).

The following lemma is [23, Proposition 2.3].

Lemma 2.4 \( N^{(2)} \) is the smallest ideal of \( N \) such that \( N/N^{(2)} \) is a trivial skew brace.

Remark 2.5 In the case, when \( N^{(2)} \) is a trivial brace, Lemma 2.4 says that both \((N, +)\) and \((N, \circ)\) are extensions of \( N/N^{(2)} \) by \( N^{(2)} \).

2.3.2 The left series

All the elements of the series \( N^k \) are left ideals of the skew brace (see [23, Proposition 2.2]), and therefore, the chain
\[
N = N^1 \supseteq N^2 \supseteq N^3 \supseteq \cdots ,
\] (13)
is a filtration for both the additive and the multiplicative group of the skew brace \( N \). This series is called the left series of the skew brace. As we noticed before, \( x \ast y \) is the commutator in \( \text{Hol}(N) \) of \( \gamma_x \) and \( y \), therefore
\[
N^k = [\underbrace{\gamma(N), \ldots, \gamma(N)}_{k-1}, N]
\]
is an iterated commutator.

A skew brace \( N \) is called left nilpotent of class \( m \) if \( N^m \supseteq N^{m+1} = 0 \) for some \( m \geq 1 \).

The characterisation of \( N^k \) as an iterated commutator immediately gives the following (see also [23, proposition 4.4])

Proposition 2.6 Let \( p \) be a prime and \( N \) be a skew brace of cardinality \( p^m \). Then, \( N \) is left nilpotent of class \( \leq m \).

3 Module braces

In this section, we restrict our study to braces, namely to skew braces with an abelian additive group, whose additive groups have an additional structure of modules over a ring \( R \).
**Definition 2** Let \((N, +, \circ)\) be a brace with gamma function \(\gamma : N \to \text{Aut}(N)\). Assume that \((N, +)\) has a structure of left (right) module over some ring \(R\).

We say that \((N, +, \circ)\) is a \((\text{left/right}) R\)-module brace (an \(R\)-brace for short) if \(\gamma_x\) is a \(R\)-module automorphism of \(N\), for each \(x \in N\), namely if \(\gamma(N) \subseteq \text{Aut}_R(N)\).

This notion clearly generalises the classic notion of braces, which we are now calling \(\mathbb{Z}\)-braces. This also extend the notion of \(F\)-brace, where \(F\) is a field, given in [13, Definition 2]. In fact, following the definition given there, a brace \(N\) is an \(R\)-brace if

\[-rx + r(x \circ y) = -x + x \circ (ry),\]

for all \(x, y \in N\) and \(r \in R\), which in terms of the gamma function is

\[r\gamma_x(y) = \gamma(x)(ry),\]

namely it is equivalent to \(\gamma \in \text{Aut}_R(N)\). The same condition, in terms of the \(\star\) operation, becomes

\[r(xy) = x\star ry.\]

(See also [39, 40] where the case when \(R\) is a field is considered.)

We recall that when \(R\) is commutative, each left \(R\)-module is also a right \(R\)-module and vice versa.

**Example 1** An \(R\)-module \(N\) with the trivial brace structure is always an \(R\)-brace, since in this case, the corresponding gamma function is the trivial map \(x \mapsto \gamma_x = \text{id}\) for all \(x \in N\).

**Example 2** Let \(N = (N, +, \cdot)\) be a radical ring and let \(\circ\) the adjoint operation on \(N\). If \((N, +)\) has a right \(R\)-module structure, we have that \((N, +, \circ)\) is an \(R\)-module brace. In fact the gamma function associated with this brace is given by \(\gamma_x(y) = -x + x + y + xy = (1 + x)y\), for all \(x, y \in N\), so \(\gamma_x \in \text{Aut}_R(N)\) for all \(x\).

**Example 3** Let \(R = \mathbb{Z}[i]\) be the ring of Gaussian integers, and let \(N\) be the additive group \(\mathbb{Z}[i] \times \mathbb{Z}[i]\). Consider on \(N\) the operation \(\circ\) defined by

\[(\alpha_1, \beta_1) \circ (\alpha_2, \beta_2) = (\alpha_1 + (-1)^{\Re(\alpha_1)}\alpha_2, \beta_1 + (-1)^{\Re(\alpha_1)}\beta_2)\]

(14)

for all \((\alpha_1, \beta_1), (\alpha_2, \beta_2) \in \mathbb{Z}[i] \times \mathbb{Z}[i]\) (here \(\Re(\alpha_1)\) denotes the real part of \(\alpha_1\)). We claim that \((N, +, \circ)\) is an \(R\)-brace. An easy way to prove this is to show that the map

\[\gamma : N \to \text{Aut}_R(N)\]

defined by \((\alpha, \beta) \mapsto \gamma(\alpha, \beta) = (-1)^{\Re(\alpha)}\text{id}\) is well-defined and verifies the gamma functional equation (4). Clearly, \(\gamma(\alpha, \beta) = \pm id \in \text{Aut}_R(N)\); moreover,

\[
\gamma((\alpha_1, \beta_1) + \gamma(\alpha_1, \beta_1)(\alpha_2, \beta_2)) = \gamma((\alpha_1, \beta_1) + (-1)^{\Re(\alpha_1)}(\alpha_2, \beta_2))
\]

\[
= \gamma((\alpha_1 + (-1)^{\Re(\alpha_1)}\alpha_2, \beta_1 + (-1)^{\Re(\alpha_1)}\beta_2))
\]

\[
= (-1)^{\Re(\alpha_1)} + (-1)^{\Re(\alpha_1)}\Re(\alpha_2)
\]

\[
= (-1)^{\Re(\alpha_1)}(-1)^{\Re(\alpha_2)}
\]

\[
= \gamma((\alpha_1, \beta_1))\gamma((\alpha_2, \beta_2)).
\]

Finally, it is immediate to see that the \(\circ\) operation associated with \(\gamma\) is (14).

This example has been constructed by using the general result of [10, Proposition 2.14].
Lemma 3.1 Let M and N be R-braces; then, their direct product $M \times N$, with the R-module structure given by the direct product of R-modules, is an R-brace.

Proof The lemma follows by noticing that if $\gamma$ and $\gamma'$ are the gamma functions associated with $M$ and $N$, respectively, then the $\gamma$-function associated with $M \times N$ is the map

$$\gamma \times \gamma' : M \times N \to \text{Aut}_R(M) \times \text{Aut}_R(N) \subseteq \text{Aut}_R(M \times N).$$

⊓⊔

The following example shows that not all braces $N$ for which the additive group has also an $R$-module structure are $R$-braces.

Example 4 Let $N = \mathbb{Z}[i]$ considered as a $\mathbb{Z}[i]$-module, and let $\gamma : \mathbb{Z}[i] \to \text{Aut}(\mathbb{Z}[i])$ be the map defined by

$$\gamma(a+ib)(x+iy) = ((-1)^a x + iy).$$

It is easy to verify that $\gamma$ is a gamma function, so $(N, +, \circ)$ is a brace. However, $N$ is not a $\mathbb{Z}[i]$-brace, since $\gamma(a+ib) \notin \text{Aut}_{\mathbb{Z}[i]}(\mathbb{Z}[i])$ for $a$ odd.

The next easy lemma (which will be useful in the following) shows that the restriction of scalars preserves the module brace structure.

Lemma 3.2 Let S and T be rings and let $f : T \to S$ be a ring homomorphism. Then, each $S$-brace $M$ has a natural $T$-brace structure via $f$.

Proof It is well-known that $M$ is a $T$-module via $f$. On the other hand, if $\varphi \in \text{Aut}_S(M)$, then $t \cdot \varphi(m) = f(t)\varphi(m) = \varphi(f(t)m) = \varphi(t \cdot m)$ for all $t \in T$ and $m \in M$, so $\varphi \in \text{Aut}_T(M)$ and $M$ is a $T$-brace. □

In the notation of the previous lemma, we say that $M$ is a $T$-brace by restriction of scalars (via $f$).

Most of the definitions one can give for braces have an analog for $R$-braces. Two $R$-braces $N$ and $M$ are isomorphic if there exists a braces isomorphism $\varphi : N \to M$ such that $\varphi$ is also an $R$-module isomorphism.

An $R$-subbrace of an $R$-brace $N$ is a subbrace which is also an $R$-submodule, this definition is justified by the following lemma.

Lemma 3.3 Let $N$ be an $R$-brace and let $M$ be a subbrace and an $R$-submodule of $N$. Then, $M$ with the induced operations is an $R$-brace.

Proof A subbrace is a brace with the induced operations. So, if $\gamma : N \to \text{Aut}_R(N)$ is the gamma function associated with the $R$-brace $N$, then the gamma function associated with the brace $M$ is the restriction of $\gamma$ to $M$, more precisely the map

$$\gamma_M : M \to \text{Aut}(M)$$

sending $m \mapsto \gamma_M (m) : (\gamma_M (m))_M : (this map is well-defined since $M$ is a subbrace of $N$, so $\gamma_M (m') = -m + m \circ m' \in M$ for all $m, m' \in M$). On the other hand, since $\gamma_M$ is an $R$-module automorphism for all $m$, then also its restriction to the $R$-submodule $M$ is such, so $(\gamma_M)_M \in \text{Aut}_R(M)$.

□ Springer
A left ideal $I$ of an $R$-brace $N$ is called left $R$-ideal if $I$ is also an $R$-submodule of $N$. Equivalently, a left $R$-ideal of $N$ is an $R$-subbrace of $N$ which is $\gamma(N)$-invariant. (In [12], an analogous definition is given for the case when $R$ is a field.) In the same way, an $R$-ideal of an $R$-brace $N$ is an ideal of $N$ which is also an $R$-submodule of $N$.

**Lemma 3.4** Let $(N, +, \circ)$ be an $R$-brace, and let $I$ be an $R$-ideal of $N$. Then, the quotient brace $N/I$ is an $R$-brace.

**Proof** We already know that $N/I$ is a brace and an $R$-module. Now, if $\gamma$ is the gamma function associated with $N$, then the gamma function $\overline{\gamma}$ associated with the quotient structure on $N/I$ is the map defined by $\overline{\gamma}_x + I = \pi \gamma_x$, where $\pi : N \to N/I$ denotes the projection, whose values are in $Aut_R(N/I)$.

**Lemma 3.5** Let $(N, +, \circ)$ be an $R$-brace. Then for each $k \geq 1$, the following hold.

(i) $N^{(k)}$ is an $R$-ideal of $N$;
(ii) $N^k$ is a left $R$-ideal of $N$;
(iii) $N(k)$ is an $R$-ideal of $N(k-1)$ and an $R$-subbrace of $N$.

**Proof** (i) By [23, Proposition 2.1], $N^{(k)}$ is an ideal of the brace $N$; moreover, $N^{(k)}$ is closed under multiplication by elements of $R$ since, for $x \in N^{(k-1)}$, $y \in N$ and $r \in R$,

$$r(x \star y) = r(\gamma_x(y) - y) = r\gamma_x(y) - ry = \gamma_x(ry) - ry = x \star ry \in N^{(k)}$$

being $\gamma_x$ an $R$-module morphism.

(ii) By [23, Proposition 2.1], $N^k$ a left ideal of the brace $N$ and the equality $r(x \star y) = x \star ry$ together with an inductive argument shows that $N^k$ is an $R$-module.

(iii) $N(k) = N(k-1) \star N(k-1)$, so it is an $R$-ideal of $N(k-1)$ by part (i), and therefore it is an $R$-subbrace of $N$. 

### 3.1 Splitting of module braces

The following easy lemma is well-known (see [22, §6A]).

**Lemma 3.6** Let $R$ be a commutative ring with 1, and let

$$R = \bigoplus_{i=1}^t R_i$$

be a direct sum decomposition of $R$ into ideals.

Set $1 = e_1 + \cdots + e_t$ with $e_i \in R_i$. Then, $e_1, \ldots, e_t$ are pairwise orthogonal idempotents, and $R_i = e_i R$, for each $i$.

The elements $e_1, \ldots, e_t$ of the previous lemma are called the orthogonal idempotents of the decomposition (15).

The following proposition can be seen as a generalisation of [7, Theorem 1].

**Proposition 3.7** Let $R$ be a commutative ring with 1, with a decomposition as in (15), and orthogonal idempotents $e_1, \ldots, e_t$.

Let $(N, +)$ be an abelian group which is also an $R$-module. Then, $N$ can be written in the form

$$N = \bigoplus_{i=1}^t N_i,$$
where each $N_i = e_i N$ is an $R$-module, which is annihilated by $R_j$ for all $j \neq i$.

If, in addition, $(N, +)$ has also a structure $(N, +, \circ)$ of $R$-brace, then, $N_i$ is a left $R$-ideal of $N$, for each $i$.

Moreover, all the $N_i$’s are normal in $(N, \circ)$, or, equivalently, are ideals of $N$, if and only if the decomposition in (16) is an $R$-braces decomposition.

**Proof** Each element $x \in N$ can be written as $x = 1x = e_1 x + \cdots + e_t x$. Further, the decomposition of $x$ into a sum of elements of the $N_i$’s is unique since if $x = e_1 y_1 + \cdots + e_t y_t$, by multiplying by $e_i$, we get $e_i x = e_i (e_1 y_1 + \cdots + e_t y_t) = e_i y_i$. This proves the equality in (16).

Moreover, let $j \neq i$; for all $r_j \in R_j$ and $x \in N$, we have $r_j e_i x = r_j e_j e_i x = 0$, so $N_i$ is annihilated by $R_j$.

We also notice that $N_i = e_i N$ is invariant under the action of $\text{Aut}_R(N)$, for all $i$. Therefore, if $(N, +)$ has also a structure $(N, +, \circ)$ of $R$-brace, then all $N_i$’s are left ideals of $N$, and the last part of the statement follows from Proposition 2.3.

In view of Example 2, as a particular case of the previous proposition, we get the following.

**Corollary 3.8** Let $R$ be a commutative ring with unit $1$, with a decomposition as in (15), and orthogonal idempotents $e_1, \ldots, e_t$.

Let $(N, +, \cdot)$ be a radical ring, and assume that it has also an $R$-algebra structure, then

$$N = \bigoplus_{i=1}^{t} e_i N$$

(17)

as $R$-braces, namely

$$1 + N = \bigoplus_{i=1}^{t} (1 + e_i N).$$

**Proof** In Example 2, we showed that in this case, the brace associated with the radical ring $N$ is an $R$-brace, so, by Proposition 3.7, the equality in (17) is a brace decomposition if and only if the left ideals $e_1 N, \ldots, e_t N$ are ideals of $N$.

In view of Proposition 2.3, this is equivalent to showing that

$$x \cdot y = \sum_{i=1}^{t} e_i x \cdot e_i y,$$

for all $x, y \in N$ (recall that the $\star$ operation of a radical ring is just the product of the ring), and this easily follows from the orthogonality of the $e_i$’s.

**Remark 3.9** If $R = \mathbb{Z}$ and $(N, +, \circ)$ is a finite brace, then the action of $\mathbb{Z}$ on $N$ cannot be faithful, so $N$ is a $\mathbb{Z}/d\mathbb{Z}$-module for some $d$.

Let $d = p_1^{a_1} \cdots p_t^{a_t}$, where the $p_i$’s are pairwise distinct primes, then

$$\mathbb{Z}/d\mathbb{Z} \cong \bigoplus_{i=1}^{t} \mathbb{Z}/p_i^{a_i} \mathbb{Z}$$

and, with the notation of Proposition 3.7, $N_i$ is the Sylow $p_i$-subgroup of $(N, +)$, and it is also a Sylow $p_i$-subgroup of $(N, \circ)$. Therefore, if $(N, \circ)$ is nilpotent, we recover the core of [7, Theorem 1] (see also [23, Corollary 4.3] and [10, Subs. 2.4]).
4 R-braces of small rank

In this section, we present our result on the relations between the additive and the multiplicative groups of a $R$-brace. In [27, Theorem 1] and its generalisation in [4, Theorem 2.5], these relations are studied for $(\mathbb{Z})$-braces. Building upon these results, in Theorem 4.1, we prove that in the case $D$-braces, where $D$ is a principal ideal domain with some additional assumptions, the connections between the additive and the multiplicative groups can be much tighter, depending on $D$.

(In a different direction, [4, Theorem 2.5] has been recently generalised in [14].)

Theorem 4.1 gives results for module braces on rings of a particular type. In the remainder of the section, after introducing some basic on $p$-adic fields, we show that this theorem can be applied to module braces on certain $p$-adic rings; then, in Lemma 4.5 and Corollary 4.6, we quantify the advantage that in this case, one can obtain by applying Theorem 4.1 instead of [4, Theorem 2.5]. Next, we show, with an argument traceable to Hensel’s Lemma, how Theorem 4.1 can be applied to modules on local rings (see Lemma 4.8). Finally, we show how to apply the results obtained in these cases to get information on $R$-braces, with $R$ any commutative ring.

Let $D$ be a principal ideal domain (PID), and let $M$ be a torsion $D$-module. $M$ has a unique decomposition as a sum of indecomposable cyclic $D$-modules. We call $D$-rank of $M$ the number of cyclic factors of this decomposition and denote it as rank$_D M$.

**Theorem 4.1** Let $p$ be a prime number, and let $D$ be a PID such that $p$ is a prime in $D$. Let $(N, +, \circ)$ be a $D$-brace of order a power of $p$.

Assume that $r = \text{rank}_D N < p - 1$.

Then, $(N, +)$ and $(N, \circ)$ have the same number of elements of each order. In particular, if $(N, \circ)$ is abelian, then $(N, +) \cong (N, \circ)$.

Sometimes we will say generically that a $D$-brace $N$ as in the theorem has “small” $D$-rank.

**Remark 4.2** [4, Theorem 2.5] gives the same result of Theorem 4.1 for $D = \mathbb{Z}$. Further examples of rings $D$ as in the theorem are given by the ring of integers of unramified extensions of the field of the $p$-adic numbers $\mathbb{Q}_p$.

Theorem 4.1 will be proved in Sect. 5. The next corollary makes it explicit for radical rings with a $D$-algebra structure.

**Corollary 4.3** Let $(N, +, \cdot)$ be a nilpotent commutative ring of order a power of a prime $p$. Let $D$ be a PID in which $p$ is prime. If $N$ is a $D$-module of $\text{rank}_D N < p - 1$, then $1 + N \cong N$.

**Proof** The brace associated with $N$ is a $D$-brace (see Example 2); therefore, since for a nilpotent ring $(1 + N, \cdot) \cong (N, \circ)$, Theorem 4.1 applies. $\square$

In the following, we show that the assumption on the ring $D$ in Theorem 4.1 is not so restrictive, since in many cases it can be satisfied with $D \neq \mathbb{Z}$.

### 4.1 Module braces over $p$-adic rings

As we noted above, the rings of integers of unramified extensions of the field $\mathbb{Q}_p$ enjoy the properties prescribed for the ring $D$ in Theorem 4.1. We now recall the definition and some of their properties, which can be found for example in [33, Ch. II, §4], [38, Ch. III, §5].
Let \( p \) be a prime. A finite extension \( K/\mathbb{Q}_p \) is called \textit{unramified} if the ideal generated by \( p \) is prime in the ring of integer \( \mathcal{O}_K \) of \( K \). Since \( \mathcal{O}_K \) is a discrete valuation ring, the only ideals of \( \mathcal{O}_K \) are the powers of the maximal ideal that in this case is \( p\mathcal{O}_K \).

**Proposition 4.4** Let \( \overline{\mathbb{Q}}_p \) be a fixed algebraic closure of \( \mathbb{Q}_p \). For each \( \lambda \geq 1 \), there exists a unique unramified extension of \( \mathbb{Q}_p \) of degree \( \lambda \) contained in \( \overline{\mathbb{Q}}_p \). This extension is a Galois extension of \( \mathbb{Q}_p \). Its ring of integers is a discrete valuation ring with maximal ideal \( (p) \), and it is generated over \( \mathbb{Z}_p \) by any root of any monic polynomial of \( \mathbb{Z}_p[x] \) of degree \( \lambda \), whose reduction modulo \( p \) is irreducible.

For each prime \( p \) and for each positive integer \( \lambda \), we will denote by \( \mathbb{Q}_p(\lambda) \) the unique unramified extension of \( \mathbb{Q}_p \) of degree \( \lambda \) contained in \( \overline{\mathbb{Q}}_p \), and by \( \mathbb{Z}_p(\lambda) \) its ring of integers.

The following lemma and the next corollary quantify the gain we have by appealing to Theorem 4.1 instead of [4, Theorem 1] when dealing with a \( \mathbb{Z}_p(\lambda) \)-brace.

**Lemma 4.5** Let \( M \) be a finite \( \mathbb{Z}_p(\lambda) \)-module. Then,

\[
\text{rank}_\mathbb{Z}(M) = \lambda \cdot \text{rank}_{\mathbb{Z}_p(\lambda)}(M).
\]

**Proof** Consider the decomposition of \( M \) as a sum of cyclic \( \mathbb{Z}_p(\lambda) \)-modules

\[
M \cong \bigoplus_{i=1}^{r} \frac{\mathbb{Z}_p(\lambda)}{p^i \mathbb{Z}_p(\lambda)}.
\]

Recalling that \( \mathbb{Z}_p(\lambda) \) is a free \( \mathbb{Z}_p \)-module of rank \( \lambda \), we get the following chain of isomorphisms of \( \mathbb{Z} \)-modules

\[
M \cong \bigoplus_{i=1}^{r} \frac{\mathbb{Z}_p(\lambda)}{p^i \mathbb{Z}_p(\lambda)} \cong \bigoplus_{i=1}^{r} \left( \frac{\mathbb{Z}_p}{p^i \mathbb{Z}_p} \right)^{\lambda} \cong \bigoplus_{i=1}^{r} \left( \frac{\mathbb{Z}}{p^i \mathbb{Z}} \right)^{\lambda},
\]

namely, if \( \text{rank}_{\mathbb{Z}_p(\lambda)}(M) = r \), then \( \text{rank}_\mathbb{Z}(M) = \lambda \cdot r \).

Theorem 4.1 and the previous lemma immediately give the following.

**Corollary 4.6** Let \( (N, +, \circ) \) be a \( \mathbb{Z}_p(\lambda) \)-brace of order a power of \( p \), and assume that \( \text{rank}_\mathbb{Z}N < \lambda(p - 1) \). Then, \( (N, +) \) and \( (N, \circ) \) have the same number of elements of each order. In particular, if \( (N, \circ) \) is abelian, then \( (N, +) \cong (N, \circ) \).

**Remark 4.7** Let \( K \) be a finite extension of \( \mathbb{Q}_p \). Denote by \( \mathcal{O}_K \) its ring of integers and let \( P_K \) be its maximal ideal. If \( [\mathcal{O}_K/P_K : \mathbb{F}_p] = \lambda \), then \( \mathbb{Z}_p(\lambda) \subseteq \mathcal{O}_K \) (this is a classical fact and an easy consequence of [33, Proposition 10]), so every \( \mathcal{O}_K \)-brace is also a \( \mathbb{Z}_p(\lambda) \)-brace by restriction of the action (see Lemma 3.2); therefore, we can apply the previous corollary to those having a “small” \( \mathbb{Z}_p(\lambda) \)-rank.

In the next subsection, we will discuss a generalisation of this argument to module braces over a general local ring.

### 4.2 Module braces over local rings

In the following, for a local ring \( S \), with finite residue field, we will use the notation \( (S, m, \mathbb{F}_{p^r}) \) to encode the information on the ring \( S \), namely to intend that \( m \) is its maximal ideal and that its residue field \( S/m \) is isomorphic to \( \mathbb{F}_{p^r} \). In this case, if \( S \) is finite its characteristic is a power of \( p \).
Lemma 4.8 Let $(S, m, \mathbb{F}_p^\times)$ be a finite local ring. Then, every $S$-brace is also a $\mathbb{Z}_p(\lambda)$-braces, by restriction of scalars.

Proof By Lemma 3.2, we are reduced to show that there exists a ring homomorphism $\mathbb{Z}_p(\lambda) \to S$.

Let $\text{char}(S) = p^\ell$. The residue field $S/m$ is of the form $\mathbb{F}_p(\xi)$, for some $\xi \in S^*$, with $\xi$ of degree $\lambda$ over $\mathbb{F}_p$. (Here, $\xi$ denotes the class of $\xi$ modulo $m$).

Let $\tilde{g}(x) \in \mathbb{F}_p[x]$ be the minimal polynomial of $\xi$ over $\mathbb{F}_p$, and let $g(x) \in \frac{\mathbb{Z}}{p\mathbb{Z}}[x]$ be a monic lifting of $\tilde{g}(x)$.

Up to changing $\xi$ with another element in the same class modulo $m$, we can assume that $g(\xi) = 0$. This can be easily shown by arguing as in the classical proof of the Hensel’s Lemma (see for example [38, Section 2.2]). In fact, $g(\xi) = 0$ means that $g(\xi) \in m$. On the other hand, $g'(\xi) \notin m$ since $\tilde{g}(x) \in \mathbb{F}_p[x]$ is irreducible and $\mathbb{F}_p$ is a perfect field, so its derivative $g'(x)$ is not zero, hence it does not vanish in $\xi$. Therefore, $g'(\xi)$ is invertible in $S$, and, denoting by $u$ its inverse, we have that $\xi_1 = \xi - g(\xi)u \in S$ and is in the same class of $\xi$ modulo $m$. Now,

$$g(\xi_1) = g(\xi - g(\xi)u) \equiv g(\xi) - g(\xi)ug'(\xi) \equiv 0 \pmod{g(\xi)^2},$$

so $g(\xi_1) \equiv m^2$. Since $m$ is nilpotent, by iterating this construction, in a finite number of steps, we get what claimed.

Consider the composition map

$$\psi: \mathbb{Z}_p[x] \to \frac{\mathbb{Z}}{p^\ell \mathbb{Z}}[x] \to S$$

where the first map is the reduction modulo $p^\ell$ and the second is the evaluation homomorphism $x \mapsto \xi$. Let $\tilde{g}(x)\mathbb{Z}_p[x]$ be any monic lifting of $g(x)$. Clearly, $\psi(\tilde{g}(x)) = g(\xi) = 0$, so $\psi$ induces a homomorphism $\psi': \mathbb{Z}_p[x]/(\tilde{g}(x)) \to S$. Finally, by Proposition 4.4, $\mathbb{Z}_p[x]/(\tilde{g}(x)) \cong \mathbb{Z}_p(\lambda)$ and this concludes the proof. □

Corollary 4.6 and the previous lemma immediately give the following.

Corollary 4.9 Let $(S, m, \mathbb{F}_p^\times)$ be a local ring, and let $(N, +, \circ)$ be a $S$-brace of order a power of $p$. If rank$_\mathbb{Z}N < \lambda(p - 1)$, then $(N, +)$ and $(N, \circ)$ have the same number of elements of each order. In particular, if $(N, \circ)$ is abelian, then $(N, +) \cong (N, \circ)$.

Proof First of all, we notice that, being $N$ finite, up to changing $S$ with its quotient by the annihilator of $N$, we can assume that $N$ is a faithful module and therefore also that $S$ is finite. Clearly this does not change its property of being local or its residue field. Therefore, by Lemma 4.8, $N$ has naturally a $\mathbb{Z}_p(\lambda)$-structure, and we can apply Corollary 4.6. □

4.3 Finite module brace over a general ring

We now show that the results obtained for module braces over a local ring can be applied to finite any $R$-brace $N$, where $R$ is any commutative ring.

Let $\text{Ann}_R(N)$ be the annihilator of $N$ in $R$, and put $A = R/\text{Ann}_R(N)$. Then, $N$ is a faithful $A$-module with the induced structure, and being $N$ finite, the ring $A$ is finite, and therefore artinian. By the structure theorem of artinian rings, we have

$$A = \bigoplus_{i=1}^t A_i \quad (18)$$

□ Springer
where the \( A_i \)'s are local artinian (in this case finite) rings, of characteristic a power of a prime \( p_i \), say. We fix the notation \( (A_i, m_i, \mathbb{F}_{p_i}^\lambda_i) \).

Let \( e_1, \ldots, e_t \) be the orthogonal idempotents of \( A \) such that \( e_1 + \cdots + e_t = 1 \) and \( A_i = e_i A \). By Proposition 3.7, letting \( N_i = e_i N \), we have

\[
N = \bigoplus_{i=1}^{t} N_i, \tag{19}
\]

where this equality holds for \( (N, +) \), and for \( N \) as an \( A \)-module brace in the case when \( N_1, \ldots, N_t \) are ideals of \( N \). In any case, since \( N_1, \ldots, N_t \) are always left ideals, some information on the \( A \)-brace \((R\text{-brace}) \) \( N \) can be derived from the study of its subbraces \( N_1, \ldots, N_t \), which are module braces over finite local rings.

We can then apply the results obtained above to this general case, getting the following.

**Proposition 4.10** Let \( R \) be a commutative ring and let \((N, +, \circ)\) be a finite \( R \)-brace.

Let \( A = R/\text{Ann}_R(N) \), and consider the decomposition of \( A \) into a sum of finite local rings \((A_i, m_i, \mathbb{F}_{p_i}^\lambda_i)\) as in (18), and the decomposition of \( N \) given in (19). The followings hold.

1. For each \( i = 1, \ldots, t \), the subbrace \( N_i \) has cardinality a power of \( p_i \) and is a \( \mathbb{Z}_{p_i}(\lambda_i) \)-brace.
2. If \( N \) has order a power of a prime \( p \), then \( p_i = p \) for all \( i \), and \( N \) is a \( \mathbb{Z}_p(\lambda) \)-brace where \( \lambda = \gcd(\lambda_i \mid i = 1, \ldots, t) \).

**Proof** By Lemma 4.8, the \( A_i \)-brace \( N_i \) is a \( \mathbb{Z}_{p_i}(\lambda_i) \)-brace. Therefore, \( N_i \) is a direct sum of cyclic and finite \( \mathbb{Z}_{p_i}(\lambda_i) \)-modules, so it is a \( p_i \)-group, proving (1).

As for (2), we notice that since \( N \) is a \( p \)-group and a faithful \( A \)-module, then the characteristic of \( A \) is a power of \( p \). Therefore, the same is true for \( A_1, \ldots, A_t \), and part (1) ensures that \( N_i \) is a \( \mathbb{Z}_p(\lambda_i) \)-brace. Now, since \( \lambda_i \mid \lambda_i \) for all \( i \), then \( \mathbb{Z}_p(\lambda) \subseteq \mathbb{Z}_p(\lambda_i) \), and \( N_i \) is a \( \mathbb{Z}_p(\lambda) \)-brace by restriction of the action, and so, by Lemma 3.1 also \( N = \bigoplus_{i=1}^{t} N_i \) is a \( \mathbb{Z}_p(\lambda) \)-brace.

**Corollary 4.11** In the notation of Proposition 4.10, assume that \( N \) has order the power of a prime \( p \) and that the \( \mathbb{Z} \)-rank of \((N, +)\) is \( < \lambda(p - 1) \). Then, \((N, +)\) and \((N, \circ)\) have the same number of elements of each order, and if \((N, \circ)\) is abelian, then \((N, +) \cong (N, \circ)\).

**Proof** By Proposition 4.10, \( N \) is a \( \mathbb{Z}_p(\lambda) \)-module, so we can apply Corollary 4.6.

**Corollary 4.12** In the notation of Proposition 4.10, assume that for some \( i \in \{1, \ldots, t\} \)

\[
\text{rank}_\mathbb{Z}(N_i) < \lambda_i(p_i - 1). \tag{20}
\]

Then, \((N_i, +)\) and \((N_i, \circ)\) have the same number of elements of each order, and if \((N_i, \circ)\) is abelian, then \((N_i, +) \cong (N_i, \circ)\).

If, in addition, \( N_1, \ldots, N_t \) are ideals of the brace \( N \), and (20) holds for all \( i \), then \((N, +)\) and \((N, \circ)\) have the same number of elements of each order, and if \((N, \circ)\) is abelian, then \((N, +) \cong (N, \circ)\).

**Proof** By Proposition 4.10, \( N_i \) has cardinality a power of \( p_i \), so the first part follows from Corollary 4.9.

For the last part, we recall that if \( N_1, \ldots, N_t \) are ideals then, by Proposition 3.7, \( N = \bigoplus_{i=1}^{t} N_i \) as a brace, and since \((N_i, +)\) and \((N_i, \circ)\) have the same number of elements of each order, for each \( i \), the same is true for their direct products. Finally, if also \((N, \circ)\) is abelian, then necessarily \((N, \circ) \cong (N, +)\).
Remark 4.13 As we saw in the previous corollaries, interesting information on an $R$-brace can also be obtained with the application of Theorem 4.1, or its corollaries, to its subbraces, even in the case when it can not be applied to the whole brace.

Consider the case of an $R$-brace $N$, with an $R$-ideal $I$: we have the following exact sequence of $R$-braces

$$0 \to I \to N \to N/I \to 0.$$  

The exactness of this sequence of $R$-braces means that both the additive group of $(N, +)$ is an extension of $(N/I, +)$ by $(I, +)$, and the multiplicative group $(N, \circ)$ is an extension of $(N/I, \circ)$ by $(I, \circ)$. If we can somehow control the differences between the additive and the multiplicative structure of $I$ and $N/I$ (for example by applying to them Theorem 4.1, or its corollaries), we can deduce information on the relation between the additive and the multiplicative group of the brace $N$.

In particular, when $I$ and $N/I$ are trivial braces, then both the additive and the multiplicative group of $N$ are extension of $N/I$ by $I$ (see also Lemma 2.4 and Remark 2.5).

Remark 4.14 The result of this section can be fruitfully applied for example in the study of Fuchs’ question on the classification of the abelian groups that can be realised as group of units of a commutative ring. This is an old question that originally appears in [28, Problem 72], which is far from being completely solved.

In [24, 25], R.Dvornicich and the author considered the case of finite abelian group, and in [26], the author studied the case of finitely generated abelian groups. From [24, Proposition 2.2], we know that a lot of information on the group of units of a ring $R$ is contained into the group $1 + \mathfrak{N}$, where $\mathfrak{N}$ is the nilradical of $R$, (see also [24, Theorem 3.1] and [25, Subsection 5.3]). Therefore, the results of this section can be be applied to the nilpotent commutative ring $\mathfrak{N}$ and to the $R$-brace associated with it, whenever $\mathfrak{N}$ has “small” $R$-rank.

In a forthcoming paper, we will study Fuchs’ question further, by introducing the current point of view of module braces, and applying the results of this section. This will prove fruitful and allow us to make progress.

5 Proof of Theorem 4.1

The proof of Theorem 4.1 is inspired from that of [27, Theorem 1]. We first establish the preliminary results.

Remark 5.1 We notice that under the assumption of the theorem $D/pD$ is a finite field. In fact, if $N$ is a non-trivial $D$-module of cardinality a power of $p$, then the annihilator $I$ of $N$ in $D$ is contained in $pD$. Now, $N$ is finite and is faithful over $D/I$, so that $D/I$, and therefore also $D/pD$, must be finite.

The following lemma refines Proposition 2.6.

Lemma 5.2 Let $K$ be a finite field of characteristic $p$ and let $(M, +, \circ)$ be a $K$-module brace of dimension $r$. Then, $M^{r+1} = 0$.

Proof $M$ is a $p$-group, so, by Proposition 2.6, $M$ is left nilpotent, namely $M^k = 0$ for some $k > 0$. This implies that the left series of $M$ is strictly decreasing to 0

$$M \supseteq M^2 \supseteq \cdots \supseteq \{0\}. \tag{21}$$
Now, in (21), we have a strictly decreasing chain of $K$-vector spaces (see Lemma 3.5), so $\dim_K M^{(i)} \leq r - i + 1$, and therefore, $M^{r+1} = 0$.  

We use the notation $m_\circ a = a \circ a \circ \cdots \circ a (m \text{ factors})$. We can easily obtain the following formula (see also [14, (3.2)])

$$p_\circ a = (\gamma_a^{p-1} + \cdots + \gamma_a + 1)(a) = (p + \binom{p}{2})\delta_a + \cdots + \left(\frac{p}{p-1}\right)\gamma_a^{p-2}\delta_a^{p-2} + \delta_a^{p-1}(a)$$  \hfill (22)

where we are using the notation $\delta_a = \gamma_a - \text{id}$.

The following proposition is the analogue of [27, Proposition 4].

**Proposition 5.3** Let $K$ be a finite field of characteristic $p$. Let $(M, +, \circ)$ be a $K$-brace of dimension $r < p - 1$. Then, all the nonzero elements of $(M, \circ)$ have order $p$.

In particular, if $(M, \circ)$ is abelian $(M, \circ)$ and $(M, +)$ are isomorphic groups.

**Proof** Let $K = \mathbb{F}_{p^n}$, then $K$ as a group is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\lambda$, so that $M$, which is isomorphic to $K'$ as a $K$-vector space, is an elementary abelian $p$-group.

Our goal is to prove that all non-trivial elements of $(M, \circ)$ have order $p$.

Now, $\delta_a^{p-1}(a) \in M^p$ and by Lemma 5.2 $M^p = 0$, so Equation (22) reduces to

$$p_\circ a = (p + \binom{p}{2})\delta_a + \cdots + \left(\frac{p}{p-1}\right)\gamma_a^{p-2}\delta_a^{p-2} + \delta_a^{p-1}(a),$$

which gives $p_\circ a = 0$ for all $a \in M$.  \hfill \Box

The next easy lemma is a generalisation of [4, Lemma 2.7].

**Lemma 5.4** Let $p$ be a prime number and let $D$ be a PID in which $pD$ is prime. Let $N$ be a $D$-module of cardinality a power of $p$ and $D$-rank $r$. Then, for each $f \in \text{Aut}_D(N)$ of order a power of $p$, $(f - \text{id})^r(N) \subseteq pN$.

**Proof** $pN$ is a characteristic subgroup (and a $D$-submodule) of $N$, so, $f$ induces an automorphism $\tilde{f}$ of $N/pN$. Since $N/pN$ is a vector space over $K = D/pD$ of dimension $d$, with $d \leq r$, then the automorphism $\tilde{f}$ can be identified with a matrix $F \in \text{GL}_d(K)$. As $F$ has order a power of $p$ and the characteristic of $K$ is $p$, then $F$ is conjugated to an upper triangular matrix $d \times d$ whose diagonal entries are $1$. Therefore, $(F - \text{Id})^d = 0$, so $(f - \text{id})^r(N) \subseteq pN$.  \hfill \Box

For a finite abelian $p$-group $(G, \times)$, and $i \geq 0$, we will denote by $\Omega_i(G, \times)$ the set of elements of $(G, \times)$ of order dividing $p^i$. Clearly, if $(G, \times)$ is abelian, then $\Omega_i(G, \times)$ a subgroup of $(G, \times)$.

The key point for proving the theorem is the following lemma.

**Lemma 5.5** Let everything be as in the statement of Theorem 4.1. Then,

$$\Omega_{i+1}(N, +) \setminus \Omega_i(N, +) \subseteq \Omega_{i+1}(N, \circ) \setminus \Omega_i(N, \circ),$$ \hfill (23)

for each $i \geq 0$.  \hfill \Box
Proof First of all, we notice that for each $i$, $\Omega_i(N, +)$ is a characteristic subgroup of $(N, +)$, and therefore, it is also a left $D$-ideal of the $D$-brace $(N, +, \circ)$; in particular, $\Omega_i(N, +)$ is a $D$-brace.

We start by proving that for each $i > 0$

$$\Omega_i(N, +) \subseteq \Omega_i(N, o). \tag{24}$$

We first consider the case $i = 1$.

As a $D$-module, $\Omega_1(N, +)$ is annihilated by $pD$, therefore it is a $K$-vector space of dimension $< p - 1$, where $K = D/pD$ is a finite field (see Remark 5.1). Proposition 5.3 applies, giving $\Omega_1(N, +) \subseteq \Omega_1(N, o)$.

Let $i > 0$ and assume by induction that

$$\Omega_i(N, +) \subseteq \Omega_i(N, o).$$

Let $a \in \Omega_{i+1}(N, +)$. Then, $pa^j \in \Omega_i(N, +)$ for all $j \geq 1$, so from Eq. (22), we get that $p_a(a) = (\gamma_a - id)^{p-1}(a)$ (mod $\Omega_i(N, +)$). Since the rank of $\Omega_{i+1}(N, +)$ is $< p - 1$, by Lemma 5.4, we get $\delta_{\Omega_{i+1}}^p(a) \in p\Omega_{i+1}(N, +) \subseteq \Omega_i(N, +)$, so $p_a(a) \in \Omega_i(N, +) \subseteq \Omega_i(N, o)$. Therefore, $a \in \Omega_{i+1}(N, o)$, proving the first statement.

We turn now to proving (23). Let $i > 0$ and assume by induction that

$$\Omega_i(N, +) \setminus \Omega_{i-1}(N, +) \subseteq \Omega_i(N, o) \setminus \Omega_{i-1}(N, o).$$

We have to show that

$$\Omega_{i+1}(N, +) \setminus \Omega_i(N, +) \subseteq \Omega_{i+1}(N, o) \setminus \Omega_i(N, o).$$

Let $a \in \Omega_{i+1}(N, +) \setminus \Omega_i(N, +)$. We have already seen that $a \in \Omega_{i+1}(N, o)$, so we are left to prove that $a$ is not in $\Omega_i(N, o)$. This can be reduced to showing that $p_a(a) \notin \Omega_{i-1}(N, +)$. In fact, this implies $p_a(a) \in \Omega_i(N, +) \setminus \Omega_{i-1}(N, +) \subseteq \Omega_i(N, o) \setminus \Omega_{i-1}(N, o)$, and this ensures that $a$ is not in $\Omega_i(N, o)$.

To show that $p_a(a)$ is not in $\Omega_{i-1}(N, +)$, we will prove that its class is not $0$ in the quotient $\Omega_{i+1}(N, +)/\Omega_{i-1}(N, +)$.

Denote by $\delta_{\Omega}(a)$ the class of $\delta_{\Omega}(a)$ in the $D$-module $\Omega_{i+1}(N, +)/\Omega_{i-1}(N, +)$. Define $S$ to be the $D$-submodule of $\Omega_{i+1}(N, +)/\Omega_{i-1}(N, +)$ generated by $\{\delta_{\Omega}(a)\}_{j \geq 0}$, and, for each $i \geq 1$,

$$S_i = \langle \delta_{\Omega}(a) \mid j \geq i - 1 \rangle_D.$$ 

We get the strictly decreasing chain

$$S = S_1 \supseteq S_2 \supseteq \cdots \supseteq S_t \supseteq \{0\}$$

for some $t$. In fact, clearly $\delta_{\Omega}(S_1) = S_{i+1} \subseteq S_i$; moreover, $S_n \equiv 0$ for $n$ sufficiently large, since using Lemma 5.4, we get that if $p^t N = 0$, then $\delta_{\Omega}^p(a) \in p^t N = 0$, so $S_{i+1} = 0$.

Finally, if $S_{i+1} = S_i$, then $S_{i+k} = S_i$ for all $k \geq 0$; therefore, this can only happen if $S_i = 0$.

By Eq. (22),

$$p_a(a) = (p + \left(\frac{p}{2}\right) \delta_{\Omega} + \cdots + \left(\frac{p}{p-1}\right) \delta_{\Omega}^{p-2}(a)) + \delta_{\Omega}^{p-1}(a).$$

If $p_a(a)$ is not in $S_2$, then $p_a(a) = p_a(a) + s_2$, with $s_2 \in S_2$, is not $0$, so $p_a(a) \notin \Omega_{i-1}(N, +)$.

Let $p_a(a) \in S_2$. Since $a$ has order $p^2$, then $p_a(a)$ is nonzero, and it belongs to $S_k \setminus S_{k+1}$ for some $k \geq 2$. This implies that the $D$-module $S/S_k$ is annihilated by $p$ so it is a $K$-module and its dimension is $< p - 1$.
On the other hand, using the notation $[s]$ for the class of $s$ in the quotient $S/S_k$, we claim
that $[\bar{a}], [\delta_{\alpha}(a)], \ldots, [\delta_{\alpha}^{k-2}(a)]$ is a $K$-basis of $S/S_k$. In fact, it is clear that they are a set of
generators; if they were linearly dependent, then we would have $\sum_{i=0}^{k-2} \lambda_i [\delta_{\alpha}^i(a)] = 0$ for
some $\lambda_i \in K$ and $\lambda_{i_0} \neq 0$, so, by applying $\delta_{\alpha}^{-1}(a)$ to the previous equality, we would get
$[\delta_{\alpha}^{k-2}(a)] = 0$, and therefore, $S_k = S_{k-1}$, a contradiction.

This proves that the dimension over $K$ of $S/S_k$ is $k-1$, so $k-1 < p-1$, hence $p-1 \geq k$ and
$\delta_{\alpha}^{k-1}(a) \in S_{k+1}$.

Finally, taking into account that $p\bar{a} \in S_k$ implies $p\delta_{\alpha}^i(\bar{a}) \in S_{k+1}$ for all $i \geq 1$, from
the previous equation, we get $p_o a \equiv pa \neq 0 \pmod{S_{k+1}}$; therefore, it is not zero in the
quotient $\Omega_{i+1}(N, +)/\Omega_{i-1}(N, +)$. This proves that $p_o a \notin \Omega_{i-1}(N, +)$.

**Proof of Theorem 4.1** Consider the two partitions of $N$

$$N = \bigcup_{i \geq 0} \Omega_{i+1}(N, +) \setminus \Omega_i(N, +) = \bigcup_{i \geq 0} \Omega_{i+1}(N, o) \setminus \Omega_i(N, o).$$

The last equality together with (23) gives, for each $i \geq 0$,

$$\Omega_{i+1}(N, +) \setminus \Omega_i(N, +) = \Omega_{i+1}(N, o) \setminus \Omega_i(N, o),$$

showing that in this case the order of each element is the same in $(N, +)$ and $(N, o)$.

In particular, if $(N, +)$ and $(N, o)$ are both abelian, they must be isomorphic.

**Funding** Open access funding provided by Università di Pisa within the CRUI-CARE Agreement.

**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which
permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give
appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence,
and indicate if changes were made. The images or other third party material in this article are included in the
article’s Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is
not included in the article’s Creative Commons licence and your intended use is not permitted by statutory
regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.
To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

**References**

1. Acri, E., Bonatto, M.: Skew braces of size $pq$. Commun. Algebra 48(5), 1872–1881 (2020)
2. Alabdali, A.A., Byott, N.P.: Hopf-Galois structures of squarefree degree. J. Algebra 559, 58–86 (2020)
3. Acri, E., Bonatto, M.: Skew braces of size $p^2q$ i: Abelian type. Algebra Colloq. 29(02), 297–320 (2022)
4. Bachiller, D.: Counterexample to a conjecture about braces. J. Algebra 453, 160–176 (2016)
5. Byott, N.P.: Uniqueness of Hopf Galois structure for separable field extensions. Commun. Algebra 24(10),
3217–3228 (1996)
6. Byott, N.P.: Hopf-Galois structures on Galois field extensions of degree $pq$. J. Pure Appl. Algebra 188(1–
3), 45–57 (2004)
7. Byott, N.P.: Nilpotent and abelian Hopf-Galois structures on field extensions. J. Algebra 381, 131–139
(2013)
8. Byott, N.P.: Solubility criteria for Hopf-Galois structures. N.Y. J. Math. 21, 883–903 (2015)
9. Caranti, A.: Bi-skew braces and regular subgroups of the holomorph. J. Algebra 562, 647–665 (2020)
10. Campedel, E., Caranti, A., Del Corso, I.: Hopf-Galois structures on extensions of degree $p^2q$ and skew
braces of order $p^2q$: the cyclic Sylow $p$-subgroup case. J. Algebra 556, 1165–1210 (2020)
11. Campedel, E., Caranti, A., Del Corso, I.: Hopf-Galois structures on extensions of degree $p^2q$ and skew
braces of order $p^2q$: the elementary abelian Sylow $p$-subgroup case. arXiv:2303.13387
12. Catino, F., Colazzo, I., Stefanelli, P.: On regular subgroups of the affine group. Bull. Aust. Math. Soc.
91(1), 76–85 (2015)
13. Catino, F., Colazzo, I., Stefanelli, P.: Skew left braces with non-trivial annihilator. J. Algebra Appl. 18(02),
1950033 (2019)
14. Caranti, A., Del Corso, I.: On the ranks of the additive and the multiplicative groups of a brace. Riv. Math. Univ. Parma (N.S.) 13(1), 31–46 (2022)
15. Caranti, A., Dalla Volta, F.: The multiple holomorph of a finitely generated abelian group. J. Algebra 481, 327–347 (2017)
16. Caranti, A., Dalla Volta, F.: Groups that have the same holomorph as a finite perfect group. J. Algebra 507, 81–102 (2018)
17. Caranti, A., Dalla Volta, F., Sala, M.: Abelian regular subgroups of the affine group and radical rings. Publ. Math. Debrecen 69(3), 297–308 (2006)
18. Childs, L.N.: On the Hopf-Galois theory for separable field extensions. Commun. Algebra 17(4), 809–825 (1989)
19. Childs, L.N.: Elementary abelian Hopf Galois structures and polynomial formal groups. J. Algebra 283(1), 292–316 (2005)
20. Childs, L.N.: Bi-skew braces and Hopf-Galois structures. New York J. Math. 25, 574–588 (2019)
21. Cedó, F., Jespers, E., Okniński, J.: Braces and the Yang–Baxter equation. Commun. Math. Phys. 327, 101–116 (2014)
22. Curtis, C.W., Reiner, I.: Methods of Representation Theory, vol. I, Wiley, New York (1981). With applications to finite groups and orders. A Wiley-Interscience Publication, Pure and Applied Mathematics
23. Cedó, F., Smoktunowicz, A., Vendramin, L.: Skew left braces of nilpotent type. Proc. Lond. Math. Soc. 118(6), 1367–1392 (2019)
24. Del Corso, I., Dvornicich, R.: Finite groups of units of finite characteristic rings. Ann. Mat. 197, 66–671 (2018)
25. Del Corso, I., Dvornicich, R.: On Fuchs’ Problem about the group of units of a ring. Bull. Lond. Math. Soc. 50, 274–292 (2018)
26. Del Corso, I.: Finitely generated abelian groups of units. J. Lond. Math. Soc. (2) 101(1), 247–270 (2020)
27. Featherstonhaugh, S.C., Caranti, A., Childs, L.N.: Abelian Hopf-Galois structures on prime-power Galois field extensions. Trans. Am. Math. Soc. 364(7), 3675–3684 (2012)
28. Fuchs, L.: Abelian Groups, 3rd edn. Pergamon, Oxford (1960)
29. Greither, C., Pareigis, B.: Hopf Galois theory for separable field extensions. J. Algebra 106(1), 239–258 (1987)
30. Guarnieri, L., Vendramin, L.: Skew braces and the Yang–Baxter equation. Math. Comput. 86(307), 2519–2534 (2017)
31. Jespers, E., Kubat, L., Van Antwerpen, A., Vendramin, L.: Factorizations of skew braces. Math. Ann. 375(3), 1649–1663 (2019)
32. Kohl, T.: Classification of the Hopf Galois structures on prime power radical extensions. J. Algebra 207(2), 525–546 (1998)
33. Lang, S.: Algebraic Number Theory. Graduate Texts in Mathematics, vol. 110, 2nd edn. Springer, New York (1994)
34. Nasybullov, T.: Connections between properties of the additive and the multiplicative groups of a two-sided skew brace. J. Algebra 540, 156–167 (2019)
35. Nejabati Zenouz, K.: On Hopf–Galois Structures and Skew Braces of Order $p^3$. PhD thesis, The University of Exeter (2018). https://ore.exeter.ac.uk/repository/handle/10871/32248
36. Rump, W.: Modules over braces. Algebra Discrete Math. 2, 127–137 (2006)
37. Rump, W.: Braces, radical rings, and the quantum Yang-Baxter equation. J. Algebra 307(1), 153–170 (2007)
38. Serre, J.P.: Local Fields. Graduate Texts in Mathematics. Springer, New York (1995)
39. Smoktunowicz, A.: Algebraic approach to Rump’s results on relations between braces and pre-Lie algebras. J. Algebra Appl. 21(3), 2250054 (2022)
40. Smoktunowicz, A.: A new formula for Lazard’s correspondence for finite braces and pre-Lie algebras. J. Algebra 594, 202–229 (2022)
41. Stefanello, L., Trappeniers, S.: On bi-skew braces and brace blocks (2022)
42. Stefanello, L., Trappeniers, S.: On the connection between Hopf–Galois structures and skew braces (2022)
43. Smoktunowicz, A., Vendramin, L.: On skew braces (with an appendix by N. Byott and L. Vendramin). J. Comb. Algebra 2(1), 47–86 (2018)
44. Tsang, C., Qin, C.: On the solvability of regular subgroups in the holomorph of a finite solvable group. Int. J. Algebra Comput. 30(2), 253–265 (2020)
45. Tsang, C.: Non-existence of Hopf-Galois structures and bijective crossed homomorphisms. J. Pure Appl. Algebra 223(7), 2804–2821 (2019)