Publ. Mat. **60** (2016), 55–79
DOI: 10.5565/PUBLMAT_60116_03

# NILPOTENT GROUPS OF CLASS THREE AND BRACES

Ferran Cedó, Eric Jespers, and Jan Okniński

**Abstract:** New constructions of braces on finite nilpotent groups are given and hence this leads to new solutions of the Yang–Baxter equation. In particular, it follows that if a group $G$ of odd order is nilpotent of class three, then it is a homomorphic image of the multiplicative group of a finite left brace (i.e. an involutive Yang–Baxter group) which also is a nilpotent group of class three. We give necessary and sufficient conditions for an arbitrary group $H$ to be the multiplicative group of a left brace such that $[H,H] \subseteq \mathrm{Soc}(H)$ and $H/[H,H]$ is a standard abelian brace, where $\mathrm{Soc}(H)$ denotes the socle of the brace $H$.

**2010 Mathematics Subject Classification:** 16T25, 20F18, 20F16.

**Key words:** Yang–Baxter equation, set-theoretic solution, brace, nilpotent group, metabelian group.

## 1. Introduction

The quantum Yang–Baxter equation, that first appeared in work on mathematical physics, lies at the foundations of several areas of mathematics, in particular the theory of quantum groups. The paper of Drinfeld [**5**] on set-theoretical solutions stimulated a lot of interest and activity, especially in developing some algebraic tools in this context. Already in [**11**], Manin proposed the study of quadratic algebras related to solutions of the Yang–Baxter equation. The approach of Gateva-Ivanova and Van den Bergh [**8**] and Etingof, Schedler, and Soloviev [**6**], based on certain classes of groups associated to solutions, turned out to be very fruitful. For algebraic and combinatorial methods developed in this context, as well as for recent results and other references we refer the reader

Research partially supported by grants of DGI MINECO (Spain) MTM2011-28992-C02-01, FEDER UNAB10-4E-378 "Una manera de hacer Europa", Comissionat per Universitats i Recerca de la Generalitat de Catalunya, Onderzoeksraad of Vrije Universiteit Brussel, Fonds voor Wetenschappelijk Onderzoek (Belgium), Centre for Advanced Studies of the Royal Flemish Academy of Belgium for Science and the Arts, National Science Centre grant DEC-2013/09/B/ST1/04408 (Poland).

to [**7, 10**]. It remains a challenging and difficult problem to create new classes of solutions.

In order to investigate non-degenerate involutive set-theoretic solutions of the Yang–Baxter equation, Rump [**13**] introduced another algebraic structure, called a brace. In recent years this structure and certain related structures were used to answer some problems in this area, see for example [**3, 4, 12, 13, 14**]. Recall that a left brace is a set $G$ equipped with two operations, an addition $+$ and a multiplication $\cdot$, such that $(G,+)$ is an abelian group, $(G,\cdot)$ is a group, and

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

for all $a,b,c\in G$. A right brace is defined similarly and a two-sided brace is a left and right brace (for the same operations). For every $a$ in a left brace $G$ one defines the additive group automorphism $\lambda_a\colon G\to G$ by $\lambda_a(b)=ab-a$ for all $b\in G$ and this yields an action $\lambda\colon (G,\cdot)\to \mathrm{Aut}((G,+))$. This on its turn leads to a map $r\colon G\times G\to G\times G$, defined by $r(a,b)=(\lambda_a(b),\lambda^{-1}_{\lambda_a(b)}(a))$, that is a set-theoretic solution of the Yang–Baxter equation [**13**] (see also [**3**]), i.e. $r_{1,2}r_{2,3}r_{1,2}=r_{2,3}r_{1,2}r_{2,3}$. Here we denote by $r_{i,j}\colon G^3\to G^3$ the map obtained by applying $r$ to the $(i,j)$-component and the identity to the remaining factor. Obviously, $\lambda$-invariant subsets of $G$ also lead to set-theoretic solutions.

It is known [**13**] that every multiplicative group of a finite left brace is the permutation group associated to an involutive non-degenerate set-theoretic solution of the Yang–Baxter equation (the so called IYB group [**4**]) and, thus by a result of Etingof, Schedler, and Soloviev [**6**] such a group is solvable. Rump announced [**15**] that there exists a group of order $11^9$ that is not the multiplicative group of any left brace, but a complete proof of this claim is not yet available. So, a problem is to characterise the finite nilpotent (or solvable) groups that are the multiplicative group of a left brace (for contributions on this topic we refer to [**3, 4, 14**]).

The socle of a left brace $G$ is the set

$$\mathrm{Soc}(G)=\{a\in G\mid ab=a+b \text{ for all } b\in G\}.$$

It is an easy exercise to verify that $\mathrm{Soc}(G)$ is a normal subgroup of the multiplicative group of $G$ and also it is a subgroup of the additive structure of $G$ (i.e. $\mathrm{Soc}(G)$ is an ideal of the left brace $G$). Furthermore, every normal subgroup $N$ of $G$ with $N\subseteq \mathrm{Soc}(G)$ is an ideal of $G$ and thus $G/N$ also is a left brace for the induced natural operations. The simplest left brace is the standard abelian brace $(G,+,\cdot)$ where

$$ab=a+b,$$

for all $a, b \in G$ and $(G, +)$ is an abelian group. Note that in this case, $G$ is a two-sided brace. It is known (see [**2, 3**]) that every finitely generated (multiplicative) nilpotent group $G$ of class 2 is a two-sided brace for the following addition:

$$z_1 a_1^{r_1} \cdots a_n^{r_n} + z_2 a_1^{s_1} \cdots a_n^{s_n} = z_1 z_2 a_1^{r_1+s_1} \cdots a_n^{r_n+s_n},$$

where $z_1, z_2 \in [G, G]$ and $G/[G, G]$ is the inner direct product of the cyclic subgroups $\langle a_1[G, G]\rangle, \ldots, \langle a_n[G, G]\rangle$. We simply call this the standard nilpotent of class 2 brace.

In this paper we give new constructions of left braces $G$ such that their multiplicative groups are nilpotent of class 3 and of odd order. It turns out that for these braces $[G, [G, G]] \subseteq \mathrm{Soc}(G)$ and $G/[G, [G, G]]$ is a standard nilpotent of class 2 brace. In particular, it follows that every nilpotent group of class 3 and of odd order is a homomorphic image of the multiplicative group of one of the constructed left braces. This complements the result in [**4**] that every finite nilpotent group is a subgroup of the multiplicative group of a left brace which is also a finite nilpotent group. Further, we also give necessary and sufficient conditions for a (not necessarily finite) group $H$ to be the multiplicative group of a left brace such that $[H, H] \subseteq \mathrm{Soc}(H)$ and $H/[H, H]$ is a standard abelian brace. In this case, it turns out that the multiplicative group of $H$ is metabelian. We include examples of metabelian groups that satisfy these properties. Obviously, nilpotent groups of class 3 are metabelian. However, an example in [**4**] shows that not all finite nilpotent groups of class 3 do satisfy these properties. Finally, within the class of finitely generated nilpotent groups of class 2, we give another characterisation of braces of such type.

## 2. Nilpotent groups of class three and of odd order

Throughout this section $G$ is a nilpotent group with centre $Z(G)$ and with a presentation of the following form:

$$G = \langle x_1, \ldots, x_r \mid [x_k, [x_j, x_i]] \in Z(G),\ [x_k, [x_j, x_i]]^{n_{k,j,i}} = [x_j, x_i]^{n_{j,i}} = 1,$$
$$x_i^{n_i} = 1,\ 1 \le i, j, k \le r\rangle,$$

for some $r > 1$ and non-negative odd integers $n_{k,j,i}$, $n_{j,i}$, $n_i$. Without loss of generality, throughout this section, we will assume that $n_i$ is the order of $x_i$, the order of $[x_j, x_i]$ is $n_{j,i}$, and the order of $[x_k, [x_j, x_i]]$ is $n_{k,j,i}$. We adopt the convention that $[a, b] = a^{-1}b^{-1}ab$, for $a, b \in G$. Clearly, the defining relations of $G$ yield that $G$ is nilpotent of class at most 3.

Essential for our approach is the fact that such a group is metabelian, has odd order and each element has a unique square root. From these properties we will deduce that the elements of $G$ have a particular normal form. Since $G$ has odd order, it is clear that for every $g \in G$ there exists a unique $h \in G$ such that $h^2 = g$. In fact, $h = g^k$ for some positive integer $k$ and we simply write $h = g^{\frac{1}{2}}$.

Because $G$ is nilpotent of class at most three, we have that

(1) $[a,[b,c]][d,[b,c]] = [ad,[b,c]]$ and $[a,[b,c]][a,[d,e]] = [a,[b,c][d,e]]$,

for all $a, b, c, d, e \in G$. By (1),

$$\begin{aligned} x_j x_i &= x_i x_j [x_j, x_i] = [x_j, x_i] x_i x_j [x_i x_j, [x_j, x_i]] \\ &= [x_i x_j, [x_j, x_i]][x_j, x_i] x_i x_j = [x_i, [x_j, x_i]][x_j, [x_j, x_i]][x_j, x_i] x_i x_j \\ &= [x_j, [x_j, x_i]][x_i, [x_j, x_i]][x_j, x_i] x_i x_j. \end{aligned}$$

An induction argument then easily yields that

$$x_j x_i^n = [x_j, [x_j, x_i]]^n [x_i, [x_j, x_i]]^{\frac{n(n+1)}{2}} [x_j, x_i]^n x_i^n x_j,$$

for any non-negative integer $n$. Another induction argument on $m > 1$ then also gives that

$$(2) \qquad x_j^m x_i^n = [x_j, [x_j, x_i]]^{\frac{nm(m+1)}{2}} [x_i, [x_j, x_i]]^{\frac{mn(n+1)}{2}} [x_j, x_i]^{mn} x_i^n x_j^m.$$

One can also show that

$$(3) \qquad x_k^m [x_j, x_i]^n = [x_k, [x_j, x_i]]^{mn} [x_j, x_i]^n x_k^m.$$

Suppose $n$ is a positive integer such that $x_i^n = 1$. From (2) it follows that

$$[x_j, [x_j, x_i]]^n [x_i, [x_j, x_i]]^{\frac{n(n+1)}{2}} [x_j, x_i]^n = 1.$$

By (1), $[x_i, [x_j, x_i]]^{\frac{n(n+1)}{2}} = [x_i^n, [x_j, x_i]]^{\frac{n+1}{2}} = 1$, and thus we get

$$[x_j, [x_j, x_i]]^n [x_j, x_i]^n = 1.$$

Since $x_j = [x_j, [x_j, x_i]]^n [x_j, x_i]^n x_j = x_j [x_j, x_i]^n$, we have that $[x_j, x_i]^n = 1$ and therefore $[x_j, [x_j, x_i]]^n = 1$. Let $m$ be a positive integer such that $[x_j, x_i]^m = 1$ or $x_k^m = 1$. Then, by (1), $[x_k, [x_j, x_i]]^m = [x_k, [x_j, x_i]^m] = 1$ or $[x_k, [x_j, x_i]]^m = [x_k^m, [x_j, x_i]] = 1$. Therefore, the order of $[x_j, x_i]$ in $G$ is a divisor of $n$ and thus a divisor of the order of $x_i$ and the order of $x_j$. Moreover, the order of $[x_k, [x_j, x_i]]$ is a divisor of the order of $x_k$ and the order of $[x_j, x_i]$.

By the Basis Theorem [**9**, Theorem 11.2.4], every element of the free nilpotent group of class three on $r$ generators $y_1, \ldots, y_r$ can be written

uniquely in the form (because such a group is metabelian, the order of the commutators in the following products is irrelevant)

$$\prod_{1\le i<j\le r,\, i\le k\le r} [y_k,[y_j,y_i]]^{\beta_{k,j,i}} \prod_{1\le i<j\le r} [y_j,y_i]^{\beta_{j,i}}\ y_1^{\beta_1} y_2^{\beta_2}\cdots y_r^{\beta_r},$$

where all $\beta_{k,j,i}$, $\beta_{j,i}$, $\beta_i$ are integers. Note that formulas (2) and (3) also hold for any two elements of a nilpotent group of class three. Because of the assumed conditions on the numbers $n_{k,j,i}$, $n_{j,i}$, and $n_i$ (they are odd, $n_{k,j,i} | \gcd(n_{j,i}, n_k)$ and $n_{j,i} | \gcd(n_j, n_i)$) and because of (2), (3), one can prove that the subset of this group consisting of elements of the form

$$\prod_{1\le i<j\le r,\, i\le k\le r} [y_k,[y_j,y_i]]^{n_{k,j,i}\beta_{k,j,i}} \prod_{1\le i<j\le r} [y_j,y_i]^{n_{j,i}\beta_{j,i}}\ y_1^{n_1\beta_1} y_2^{n_2\beta_2}\cdots y_r^{n_r\beta_r}$$

is a normal subgroup. Hence, it follows that every element $g \in G$ can be written uniquely in the form

$$(4)\quad g = \prod_{1\le i<j\le r,\, i\le k\le r} [x_k,[x_j,x_i]]^{\alpha_{k,j,i}} \prod_{1\le i<j\le r} [x_j,x_i]^{\alpha_{j,i}}\ x_1^{\alpha_1} x_2^{\alpha_2}\cdots x_r^{\alpha_r},$$

where $0 \le \alpha_{k,j,i} < n_{k,j,i}$, $0 \le \alpha_{j,i} < n_{j,i}$, and $0 \le \alpha_i < n_i$. We call this the normal form of $g$.

We now define an addition $+$ on $G$ using the normal forms of the elements. So, let

$$g_1 = \prod_{1\le i<j\le r,\, i\le k\le r} [x_k,[x_j,x_i]]^{\alpha_{k,j,i}} \prod_{1\le i<j\le r} [x_j,x_i]^{\alpha_{j,i}}\ x_1^{\alpha_1} x_2^{\alpha_2}\cdots x_r^{\alpha_r}$$

and

$$g_2 = \prod_{1\le i<j\le r,\, i\le k\le r} [x_k,[x_j,x_i]]^{\beta_{k,j,i}} \prod_{1\le i<j\le r} [x_j,x_i]^{\beta_{j,i}}\ x_1^{\beta_1} x_2^{\beta_2}\cdots x_r^{\beta_r}$$

be elements in $G$ written in normal form. Define

$$g_1 + g_2 = \prod_{1\le i<j\le r,\, i\le k\le r} [x_k,[x_j,x_i]]^{\gamma_{k,j,i}} \prod_{1\le i<j\le r} [x_j,x_i]^{\gamma_{j,i}}\ x_1^{\gamma_1} x_2^{\gamma_2}\cdots x_r^{\gamma_r},$$

where $\gamma_i = \alpha_i + \beta_i$, $\gamma_{i,j} = \alpha_{i,j} + \beta_{i,j}$, and

$$\gamma_{k,j,i} = \begin{cases} \alpha_{k,j,i} + \beta_{k,j,i} & \text{if } k \ne i, \\ \alpha_{i,j,i} + \beta_{i,j,i} + \frac{\alpha_{j,i}\beta_i + \alpha_i\beta_{j,i}}{2} & \text{if } k = i. \end{cases}$$

Using the restrictions on the numbers $n_i$, $n_{j,i}$, and $n_{k,j,i}$, it is easily seen that in this definition one may replace $\alpha_i$ by $\alpha_i + v_i n_i$, $\alpha_{j,i}$ by $\alpha_{j,i} + v_{j,i} n_{j,i}$, and $\alpha_{k,j,i}$ by $\alpha_{j,k,i} + v_{k,j,i} n_{k,j,i}$, for integers $v_i$, $v_{j,i}$, and $v_{k,j,i}$, and similarly for the exponents in $g_2$. In other words, to define

the addition, one does not have to assume the bounds imposed on the exponents in the normal form of the elements.

**Theorem 2.1.** *$(G,+,\cdot)$ is a left brace such that $[G,[G,G]]$ is an ideal contained in $\mathrm{Soc}(G)$ and $G/[G,[G,G]]$ is a standard nilpotent of class 2 brace. Furthermore, if $n_{i,j,i}>1$ for some $1\le i<j\le r$, then $(G,+,\cdot)$ is not a right brace.*

*Proof:* Let $g_1,g_2,g_3\in G$. Write

$$g_1=\prod_{1\le i<j\le r,\, i\le k\le r}[x_k,[x_j,x_i]]^{\alpha_{k,j,i}}\prod_{1\le i<j\le r}[x_j,x_i]^{\alpha_{j,i}}\ x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_r^{\alpha_r},$$

$$g_2=\prod_{1\le i<j\le r,\, i\le k\le r}[x_k,[x_j,x_i]]^{\beta_{k,j,i}}\prod_{1\le i<j\le r}[x_j,x_i]^{\beta_{j,i}}\ x_1^{\beta_1}x_2^{\beta_2}\cdots x_r^{\beta_r},$$

and

$$g_3=\prod_{1\le i<j\le r,\, i\le k\le r}[x_k,[x_j,x_i]]^{\delta_{k,j,i}}\prod_{1\le i<j\le r}[x_j,x_i]^{\delta_{j,i}}\ x_1^{\delta_1}x_2^{\delta_2}\cdots x_r^{\delta_r},$$

where all exponents are integers. It is easy to see that $g_1+g_2=g_2+g_1$, $g_1+1=g_1$, and

$$\prod_{1\le i<j\le r,\, i\le k\le r}[x_k,[x_j,x_i]]^{-\alpha_{k,j,i}}\prod_{1\le i<j\le r}[x_j,x_i]^{-\alpha_{j,i}}\ x_1^{-\alpha_1}x_2^{-\alpha_2}\cdots x_r^{-\alpha_r}$$

$$\prod_{1\le i<j\le r}[x_i,[x_j,x_i]]^{\alpha_i\alpha_{j,i}}+g_1=1.$$

Furthermore, for $i<j$, the exponent of $[x_i,[x_j,x_i]]$ in the normal form of $g_1+(g_2+g_3)$ (modulo $n_{i,j,i}$) is

$$\alpha_{i,j,i}+\beta_{i,j,i}+\delta_{i,j,i}+\frac{\beta_i\delta_{j,i}+\beta_{j,i}\delta_i}{2}+\frac{\alpha_i(\beta_{j,i}+\delta_{j,i})+\alpha_{j,i}(\beta_i+\delta_i)}{2}$$

and the exponent of $[x_i,[x_j,x_i]]$ in the normal form of $(g_1+g_2)+g_3$ (modulo $n_{i,j,i}$) is

$$\alpha_{i,j,i}+\beta_{i,j,i}+\frac{\alpha_i\beta_{j,i}+\alpha_{j,i}\beta_i}{2}+\delta_{i,j,i}+\frac{(\alpha_i+\beta_i)\delta_{j,i}+(\alpha_{j,i}+\beta_{j,i})\delta_i}{2}.$$

Therefore $g_1+(g_2+g_3)=(g_1+g_2)+g_3$. Hence $(G,+)$ is an abelian group.

Next we show that $g_1(g_2+g_3)+g_1=g_1g_2+g_1g_3$ and thus it follows that $(G,+,\cdot)$ is a left brace. It is clear that the exponent of $x_i$ in the normal form of $g_1(g_2+g_3)+g_1$ (modulo $n_i$) is

$$\alpha_i+\beta_i+\delta_i+\alpha_i$$

and the exponent of $x_i$ in the normal form of $g_1g_2 + g_1g_3$ (modulo $n_i$) is

$$\alpha_i + \beta_i + \alpha_i + \delta_i.$$

So both exponents are equal (modulo $n_i$). Let $1 \leq i < j \leq r$. By (2) and (3), the exponent of $[x_j, x_i]$ in the normal form of $g_1(g_2 + g_3) + g_1$ (modulo $n_{j,i}$) is

$$\alpha_{j,i} + \beta_{j,i} + \delta_{j,i} + \alpha_j(\beta_i + \delta_i) + \alpha_{j,i}$$

and the exponent of $[x_j, x_i]$ in the normal form of $g_1g_2 + g_1g_3$ (modulo $n_{j,i}$) is

$$\alpha_{j,i} + \beta_{j,i} + \alpha_j\beta_i + \alpha_{j,i} + \delta_{j,i} + \alpha_j\delta_i.$$

So, also these exponents are equal (modulo $n_{j,i}$). Let $i \leq k \leq r$. Suppose that $k \notin \{i, j\}$. Then, by (2) and (3), the exponent of $[x_k, [x_j, x_i]]$ in the normal form of $g_1(g_2 + g_3) + g_1$ (modulo $n_{k,j,i}$) is

$$\alpha_{k,j,i} + \beta_{k,j,i} + \delta_{k,j,i} + \alpha_k(\beta_{j,i} + \delta_{j,i}) + \alpha_{k,j,i}$$

and the exponent of $[x_k, [x_j, x_i]]$ in the normal form of $g_1g_2 + g_1g_3$ (modulo $n_{k,j,i}$) is

$$\alpha_{k,j,i} + \beta_{k,j,i} + \alpha_k\beta_{j,i} + \alpha_{k,j,i} + \delta_{k,j,i} + \alpha_k\delta_{j,i}.$$

By (2) and (3), the exponent of $[x_j, [x_j, x_i]]$ in the normal form of $g_1(g_2 + g_3) + g_1$ (modulo $n_{j,j,i}$) is

$$\alpha_{j,j,i} + \beta_{j,j,i} + \delta_{j,j,i} + \frac{\alpha_j(\alpha_j + 1)(\beta_i + \delta_i)}{2} + \alpha_{j,j,i}$$

and the exponent of $[x_j, [x_j, x_i]]$ in the normal form of $g_1g_2 + g_1g_3$ (modulo $n_{j,j,i}$) is

$$\alpha_{j,j,i} + \beta_{j,j,i} + \frac{\alpha_j(\alpha_j + 1)\beta_i}{2} + \alpha_{j,j,i} + \delta_{j,j,i} + \frac{\alpha_j(\alpha_j + 1)\delta_i}{2}.$$

Finally the exponent of $[x_i, [x_j, x_i]]$ in the normal form of $g_1(g_2 + g_3) + g_1$ (modulo $n_{i,j,i}$) is

$$\alpha_{i,j,i} + \beta_{i,j,i} + \delta_{i,j,i} + \frac{\beta_i\delta_{j,i} + \beta_{j,i}\delta_i}{2} + \frac{\alpha_j(\beta_i + \delta_i)(\beta_i + \delta_i + 1)}{2} + \alpha_{i,j,i}$$
$$+ \frac{(\alpha_{j,i} + \beta_{j,i} + \delta_{j,i} + \alpha_j(\beta_i + \delta_i))\alpha_i + (\alpha_i + \beta_i + \delta_i)\alpha_{j,i}}{2}$$

and the exponent of $[x_i,[x_j,x_i]]$ in the normal form of $g_1g_2+g_1g_3$ (modulo $n_{i,j,i}$) is

$$\alpha_{i,j,i}+\beta_{i,j,i}+\frac{\alpha_j\beta_i(\beta_i+1)}{2}+\alpha_{i,j,i}+\delta_{i,j,i}+\frac{\alpha_j\delta_i(\delta_i+1)}{2}$$
$$+\frac{(\alpha_{j,i}+\beta_{j,i}+\alpha_j\beta_i)(\alpha_i+\delta_i)+(\alpha_{j,i}+\delta_{j,i}+\alpha_j\delta_i)(\alpha_i+\beta_i)}{2},$$

and it is easy to check that these exponents coincide. Hence $g_1(g_2+g_3)+g_1=g_1g_2+g_1g_3$. Therefore, $(G,+,\cdot)$ indeed is a left brace.

The definition of the addition $+$ easily implies that $[G,[G,G]]\subseteq \mathrm{Soc}(G)$, thus $[G,[G,G]]$ is an ideal of $G$, and $G/[G,[G,G]]$ is a standard nilpotent of class two brace. If $n_{i,j,i}>1$ for some $1\leq i<j\leq r$, then it is easy to check that $(x_i+x_j)x_i+x_i\neq x_i^2+x_jx_i$, and thus $(G,+,\cdot)$ is not a right brace in this case. □

An obvious consequence of Theorem 2.1 is the following result.

**Corollary 2.2.** *A finite nilpotent group of class at most* 3 *and of odd order is a homomorphic image of a nilpotent group of class* 3 *and of odd order that is the multiplicative group of a finite left brace* $G$.

The corollary can be seen as complementary to Corollary 3.8 in [**4**] that says that any finite nilpotent group is a subgroup of a nilpotent group that is the multiplicative group of a finite left brace $G$.

We finish this section with a remark. Let $G$ be a nilpotent group of class 3. From the previous results one might expect that $(G,+,\cdot)$ is a left brace for an addition on $G$ defined as follows:

$$a+b=[a,[b,a]]^x[b,[b,a]]^y[b,a]^zab, \tag{5}$$

for $a,b\in G$ and integers $x$, $y$, and $z$ (depending on $a$ and $b$). We show this is impossible. Indeed, note that if $a\in G$ then $-a=a^{-1}$ because $a+a^{-1}=aa^{-1}=1$. Hence, if $(G,+,\cdot)$ is a left brace then $aa-a=a^2+a^{-1}=a^2a^{-1}=a$. As this holds for all $a\in G$, we obtain a contradiction with Theorem 5 in [**3**], where it is shown that every left brace $A$ with the property that $a^2-a=a$ for all $a\in A$ has a multiplicative group that is nilpotent and of class at most two. Hence there are no left (right) braces $(G,+,\cdot)$ with a nilpotent multiplicative group of class 3 and an addition defined by (5).

## 3. More constructions of braces on nilpotent groups of class three

In the previous section we considered a class of nilpotent finite groups $G$ of odd order and of nilpotence class three. We showed that they are multiplicative groups of left braces. This was done via a particular construction of an additive structure such that the ideal $[G,[G,G]]$ is contained in $\operatorname{Soc}(G)$ and modulo this ideal $G$ is a standard nilpotent of class 2 brace. In this section we assume additionally that the group $G$ is 2-generated and we describe more general constructions of left braces $G$ such that $G/\operatorname{Soc}(G)$ is a left brace that is standard nilpotent of class at most 2. The idea is to check which symmetric bilinear forms (expressed in terms of the exponents used in the canonical form of elements of $G$) can be used to define the additive structure of a left brace.

So, let $G$ be a group with a presentation of the following form:

$$\begin{aligned} G = \langle x_1, x_2 \mid {} & [x_1,[x_2,x_1]], [x_2,[x_2,x_1]] \in Z(G), \\ & x_1^{n_1} = x_2^{n_2} = [x_2,x_1]^{n_3} = [x_1,[x_2,x_1]]^{n_4} = [x_2,[x_2,x_1]]^{n_5} = 1\rangle, \end{aligned}$$

where every $n_i$ is odd. As in Section 2, we assume that the order of $x_i$ is $n_i$, for $i = 1, 2$, the order of $[x_2,x_1]$ is $n_3$, the order of $[x_1,[x_2,x_1]]$ is $n_4$, and the order of $[x_2,[x_2,x_1]]$ is $n_5$. Let $a = [x_1,[x_2,x_1]]$, $b = [x_2,[x_2,x_1]]$, $c = [x_2,x_1]$, $d = x_1$, and $e = x_2$. Then every element $h \in G$ can be written uniquely in the form (its normal form)

$$h = a^{\alpha} b^{\beta} c^{\gamma} d^{\delta} e^{\varepsilon},$$

for some integers $\alpha$, $\beta$, $\gamma$, $\delta$, $\varepsilon$ such that $0 \le \alpha < n_4$, $0 \le \beta < n_5$, $0 \le \gamma < n_3$, $0 \le \delta < n_1$, and $0 \le \varepsilon < n_2$.

Consider the subring $\mathbb{Z}_2 = \{z2^r \mid r, z \in \mathbb{Z}\}$ of $\mathbb{Q}$. For $q, q' \in \mathbb{Z}_2$ and an integer $m$, we say that $q$ is congruent to $q'$ modulo $m$ if $q - q' \in m\mathbb{Z}_2$. In this case we write $q \equiv q' \pmod m$. As mentioned earlier, because $G$ has odd order the notation $g^z$ has a unique meaning for any $z \in \mathbb{Z}_2$ and $g \in G$.

Let $F, F' \in M_3(\mathbb{Z}_2)$ and let $f$, $g$ denote the induced bilinear forms on $\mathbb{Q}^3$. Thus, for $v_i = (\gamma_i, \delta_i, \varepsilon_i)$,

$$f(v_1,v_2) = (\gamma_1,\delta_1,\varepsilon_1)F \begin{pmatrix} \gamma_2 \\ \delta_2 \\ \varepsilon_2 \end{pmatrix} \text{ and } g(v_1,v_2) = (\gamma_1,\delta_1,\varepsilon_1)F' \begin{pmatrix} \gamma_2 \\ \delta_2 \\ \varepsilon_2 \end{pmatrix}.$$

We define an addition $+$ on $G$ as follows:

$$a^{\alpha_1}b^{\beta_1}c^{\gamma_1}d^{\delta_1}e^{\varepsilon_1} + a^{\alpha_2}b^{\beta_2}c^{\gamma_2}d^{\delta_2}e^{\varepsilon_2} = a^{\alpha_1+\alpha_2+f(v_1,v_2)}b^{\beta_1+\beta_2+g(v_1,v_2)}c^{\gamma_1+\gamma_2}d^{\delta_1+\delta_2}e^{\varepsilon_1+\varepsilon_2},$$

where $0 \leq \alpha_i < n_4$, $0 < \beta_i < n_5$, $0 \leq \gamma_i < n_3$, $0 \leq \delta_i < n_1$, and $0 \leq \varepsilon_i < n_2$. Because $f$ and $g$ are bilinear forms and because $n_4, n_5 \mid n_3$ and $n_3 \mid \gcd(n_1, n_2)$, it is easily seen that in the definition of the addition one does not have to assume the bounds imposed on the exponents.

**Lemma 3.1.** *If $F, F' \in M_3(\mathbb{Z}_2)$ are symmetric matrices, then $(G, +)$ is an abelian group.*

*Proof:* Since $a$, $b$ are central elements in $G$ and $f$ and $g$ are symmetric bilinear forms it is clear that the addition is commutative. The associativity of the addition is equivalent to the following equality

$$\begin{aligned} &a^{f((\gamma_1,\delta_1,\varepsilon_1),(\gamma_2,\delta_2,\varepsilon_2))+f((\gamma_1+\gamma_2,\delta_1+\delta_2,\varepsilon_1+\varepsilon_2),(\gamma_3,\delta_3,\varepsilon_3))} \\ &\quad b^{g((\gamma_1,\delta_1,\varepsilon_1),(\gamma_2,\delta_2,\varepsilon_2))+g((\gamma_1+\gamma_2,\delta_1+\delta_2,\varepsilon_1+\varepsilon_2),(\gamma_3,\delta_3,\varepsilon_3))} \\ &= a^{f((\gamma_1,\delta_1,\varepsilon_1),(\gamma_2+\gamma_3,\delta_2+\delta_3,\varepsilon_2+\varepsilon_3))+f((\gamma_2,\delta_2,\varepsilon_2),(\gamma_3,\delta_3,\varepsilon_3))} \\ &\quad b^{g((\gamma_1,\delta_1,\varepsilon_1),(\gamma_2+\gamma_3,\delta_2+\delta_3,\varepsilon_2+\varepsilon_3))+g((\gamma_2,\delta_2,\varepsilon_2),(\gamma_3,\delta_3,\varepsilon_3))}. \end{aligned}$$

Since $f$ and $g$ are symmetric bilinear forms the associativity of the addition follows. Note that $1 + h = h$ for all $h \in G$ and

$$-a^{\alpha}b^{\beta}c^{\gamma}d^{\delta}e^{\varepsilon} = a^{-\alpha+f((\gamma,\delta,\varepsilon),(\gamma,\delta,\varepsilon))}b^{-\beta+g((\gamma,\delta,\varepsilon),(\gamma,\delta,\varepsilon))}c^{-\gamma}d^{-\delta}e^{-\varepsilon}.$$

Hence $(G, +)$ is an abelian group. □

**Proposition 3.2.** *With the above notation, if $F, F' \in M_3(\mathbb{Z}_2)$ are symmetric matrices, then $(G, +, \cdot)$ is a left brace if and only if*

$$F = \begin{pmatrix} n_4q_1 & \frac{1}{2} + n_4q_2 & n_4q_3 \\ \frac{1}{2} + n_4q_2 & x & y \\ n_4q_3 & y & t \end{pmatrix} \text{ and } F' = \begin{pmatrix} n_5q_1' & n_5q_2' & n_5q_3' \\ n_5q_2' & x' & y' \\ n_5q_3' & y' & t' \end{pmatrix},$$

*for some $q_i, q_i', x, y, t, x', y', t' \in \mathbb{Z}_2$. Moreover, in this case, the ideal $\langle a, b\rangle = [G, [G, G]]$ is contained in $\mathrm{Soc}(G)$ and $G/\langle a, b\rangle$ is a standard nilpotent of class two left brace.*

*Proof:* By Lemma 3.1, $(G,+)$ is an abelian group. Let $h_i = c^{\gamma_i} d^{\delta_i} e^{\varepsilon_i}$, for $i = 1,2,3$. Let $F = (f_{ij})$ and $F' = (g_{ij})$. By the definition of $+$ and because of (2) and (3), we have

$$\begin{aligned}
h_1(h_2+h_3)+h_1 &= h_1 a^{f((\gamma_2,\delta_2,\varepsilon_2),(\gamma_3,\delta_3,\varepsilon_3))} b^{g((\gamma_2,\delta_2,\varepsilon_2),(\gamma_3,\delta_3,\varepsilon_3))} \\
&\quad c^{\gamma_2+\gamma_3} d^{\delta_2+\delta_3} e^{\varepsilon_2+\varepsilon_3} + h_1 \\
&= a^{f((\gamma_2,\delta_2,\varepsilon_2),(\gamma_3,\delta_3,\varepsilon_3))} b^{g((\gamma_2,\delta_2,\varepsilon_2),(\gamma_3,\delta_3,\varepsilon_3))} \\
&\quad c^{\gamma_1} d^{\delta_1} e^{\varepsilon_1} c^{\gamma_2+\gamma_3} d^{\delta_2+\delta_3} e^{\varepsilon_2+\varepsilon_3} + h_1 \\
&= a^{f((\gamma_2,\delta_2,\varepsilon_2),(\gamma_3,\delta_3,\varepsilon_3))+\delta_1(\gamma_2+\gamma_3)} \\
&\quad b^{g((\gamma_2,\delta_2,\varepsilon_2),(\gamma_3,\delta_3,\varepsilon_3))+\varepsilon_1(\gamma_2+\gamma_3)} \\
&\quad c^{\gamma_1+\gamma_2+\gamma_3} d^{\delta_1} e^{\varepsilon_1} d^{\delta_2+\delta_3} e^{\varepsilon_2+\varepsilon_3} + h_1 \\
&= a^{\alpha_1} b^{\beta_1} c^{\gamma_1+\gamma_2+\gamma_3} d^{\delta_1} c^{\varepsilon_1(\delta_2+\delta_3)} d^{\delta_2+\delta_3} e^{\varepsilon_1+\varepsilon_2+\varepsilon_3} + h_1 \\
&= a^{\alpha_1+\delta_1\varepsilon_1(\delta_2+\delta_3)} b^{\beta_1} c^{\gamma_1+\gamma_2+\gamma_3+\varepsilon_1(\delta_2+\delta_3)} \\
&\quad d^{\delta_1+\delta_2+\delta_3} e^{\varepsilon_1+\varepsilon_2+\varepsilon_3} + h_1,
\end{aligned}$$

where

$$\alpha_1 = f((\gamma_2,\delta_2,\varepsilon_2),(\gamma_3,\delta_3,\varepsilon_3)) + \delta_1(\gamma_2+\gamma_3) + \frac{\varepsilon_1(\delta_2+\delta_3)(\delta_2+\delta_3+1)}{2},$$

$$\beta_1 = g((\gamma_2,\delta_2,\varepsilon_2),(\gamma_3,\delta_3,\varepsilon_3)) + \varepsilon_1(\gamma_2+\gamma_3) + \frac{(\delta_2+\delta_3)\varepsilon_1(\varepsilon_1+1)}{2},$$

and

$$\begin{aligned}
h_1h_2+h_1h_3 &= c^{\gamma_1} d^{\delta_1} e^{\varepsilon_1} c^{\gamma_2} d^{\delta_2} e^{\varepsilon_2} + c^{\gamma_1} d^{\delta_1} e^{\varepsilon_1} c^{\gamma_3} d^{\delta_3} e^{\varepsilon_3} \\
&= a^{\delta_1\gamma_2} b^{\varepsilon_1\gamma_2} c^{\gamma_1+\gamma_2} d^{\delta_1} e^{\varepsilon_1} d^{\delta_2} e^{\varepsilon_2} + a^{\delta_1\gamma_3} b^{\varepsilon_1\gamma_3} c^{\gamma_1+\gamma_3} d^{\delta_1} e^{\varepsilon_1} d^{\delta_3} e^{\varepsilon_3} \\
&= a^{\delta_1\gamma_2+\frac{\varepsilon_1\delta_2(\delta_2+1)}{2}} b^{\varepsilon_1\gamma_2+\frac{\delta_2\varepsilon_1(\varepsilon_1+1)}{2}} c^{\gamma_1+\gamma_2} d^{\delta_1} c^{\varepsilon_1\delta_2} d^{\delta_2} e^{\varepsilon_1+\varepsilon_2} \\
&\quad + a^{\delta_1\gamma_3+\frac{\varepsilon_1\delta_3(\delta_3+1)}{2}} b^{\varepsilon_1\gamma_3+\frac{\delta_3\varepsilon_1(\varepsilon_1+1)}{2}} c^{\gamma_1+\gamma_3} d^{\delta_1} c^{\varepsilon_1\delta_3} d^{\delta_3} e^{\varepsilon_1+\varepsilon_3} \\
&= a^{\delta_1\gamma_2+\frac{\varepsilon_1\delta_2(\delta_2+1)}{2}+\delta_1\varepsilon_1\delta_2} b^{\varepsilon_1\gamma_2+\frac{\delta_2\varepsilon_1(\varepsilon_1+1)}{2}} c^{\gamma_1+\gamma_2+\varepsilon_1\delta_2} d^{\delta_1+\delta_2} e^{\varepsilon_1+\varepsilon_2} \\
&\quad + a^{\delta_1\gamma_3+\frac{\varepsilon_1\delta_3(\delta_3+1)}{2}+\delta_1\varepsilon_1\delta_3} b^{\varepsilon_1\gamma_3+\frac{\delta_3\varepsilon_1(\varepsilon_1+1)}{2}} \\
&\quad\quad c^{\gamma_1+\gamma_3+\varepsilon_1\delta_3} d^{\delta_1+\delta_3} e^{\varepsilon_1+\varepsilon_3}.
\end{aligned}$$

Suppose that $(G,+,\cdot)$ is a left brace. We have that $h_1(h_2+h_3)+h_1 = h_1h_2+h_1h_3$. Therefore, comparing the exponents of the elements $a$ and $b$

in $h_1(h_2+h_3)+h_1$ and $h_1h_2+h_1h_3$, we have $(\mathrm{mod}\, n_4)$

$$\alpha_1+\delta_1\varepsilon_1(\delta_2+\delta_3)$$
$$+f((\gamma_1+\gamma_2+\gamma_3+\varepsilon_1(\delta_2+\delta_3),\delta_1+\delta_2+\delta_3,\varepsilon_1+\varepsilon_2+\varepsilon_3),(\gamma_1,\delta_1,\varepsilon_1))$$
$$\equiv \delta_1\gamma_2+\frac{\varepsilon_1\delta_2(\delta_2+1)}{2}+\delta_1\varepsilon_1\delta_2+\delta_1\gamma_3+\frac{\varepsilon_1\delta_3(\delta_3+1)}{2}+\delta_1\varepsilon_1\delta_3$$
$$+f((\gamma_1+\gamma_2+\varepsilon_1\delta_2,\delta_1+\delta_2,\varepsilon_1+\varepsilon_2),(\gamma_1+\gamma_3+\varepsilon_1\delta_3,\delta_1+\delta_3,\varepsilon_1+\varepsilon_3))$$

and $(\mathrm{mod}\, n_5)$

$$\beta_1+g((\gamma_1+\gamma_2+\gamma_3+\varepsilon_1(\delta_2+\delta_3),\delta_1+\delta_2+\delta_3,\varepsilon_1+\varepsilon_2+\varepsilon_3),(\gamma_1,\delta_1,\varepsilon_1))$$
$$\equiv \varepsilon_1\gamma_2+\frac{\delta_2\varepsilon_1(\varepsilon_1+1)}{2}+\varepsilon_1\gamma_3+\frac{\delta_3\varepsilon_1(\varepsilon_1+1)}{2}$$
$$+g((\gamma_1+\gamma_2+\varepsilon_1\delta_2,\delta_1+\delta_2,\varepsilon_1+\varepsilon_2),(\gamma_1+\gamma_3+\varepsilon_1\delta_3,\delta_1+\delta_3,\varepsilon_1+\varepsilon_3)).$$

Hence

(6)
$$f((\gamma_1+\gamma_2+\varepsilon_1\delta_2,\delta_1+\delta_2,\varepsilon_1+\varepsilon_2),(\gamma_1+\gamma_3+\varepsilon_1\delta_3,\delta_1+\delta_3,\varepsilon_1+\varepsilon_3))$$
$$\equiv f((\gamma_1+\gamma_2+\gamma_3+\varepsilon_1(\delta_2+\delta_3),\delta_1+\delta_2+\delta_3,\varepsilon_1+\varepsilon_2+\varepsilon_3),(\gamma_1,\delta_1,\varepsilon_1))$$
$$+f((\gamma_2,\delta_2,\varepsilon_2),(\gamma_3,\delta_3,\varepsilon_3))+\varepsilon_1\delta_2\delta_3\ (\mathrm{mod}\, n_4)$$

and

(7)
$$g((\gamma_1+\gamma_2+\varepsilon_1\delta_2,\delta_1+\delta_2,\varepsilon_1+\varepsilon_2),(\gamma_1+\gamma_3+\varepsilon_1\delta_3,\delta_1+\delta_3,\varepsilon_1+\varepsilon_3))$$
$$\equiv g((\gamma_1+\gamma_2+\gamma_3+\varepsilon_1(\delta_2+\delta_3),\delta_1+\delta_2+\delta_3,\varepsilon_1+\varepsilon_2+\varepsilon_3),(\gamma_1,\delta_1,\varepsilon_1))$$
$$+g((\gamma_2,\delta_2,\varepsilon_2),(\gamma_3,\delta_3,\varepsilon_3))\ (\mathrm{mod}\, n_5).$$

Then, by an easy calculation we obtain

$$f_{1,1}(\gamma_2\delta_3\varepsilon_1+\gamma_3\delta_2\varepsilon_1+\delta_2\delta_3\varepsilon_1^2)+2f_{1,2}\delta_2\delta_3\varepsilon_1$$
$$+f_{1,3}(\delta_2\varepsilon_1\varepsilon_3+\delta_3\varepsilon_1\varepsilon_2)\equiv\varepsilon_1\delta_2\delta_3\ (\mathrm{mod}\, n_4)$$

and

$$g_{1,1}(\gamma_2\delta_3\varepsilon_1+\gamma_3\delta_2\varepsilon_1+\delta_2\delta_3\varepsilon_1^2)+2g_{1,2}\delta_2\delta_3\varepsilon_1$$
$$+g_{1,3}(\delta_2\varepsilon_1\varepsilon_3+\delta_3\varepsilon_1\varepsilon_2)\equiv 0\ (\mathrm{mod}\, n_5).$$

Now, taking $\gamma_2=\delta_3=\varepsilon_1=1$ and $\delta_2=\varepsilon_2=0$, we have $f_{1,1}\equiv 0\ (\mathrm{mod}\, n_4)$ and $g_{1,1}\equiv 0\ (\mathrm{mod}\, n_5)$. Taking $\delta_3=\varepsilon_1=\varepsilon_2=1$ and $\gamma_2=$

$\gamma_3 = \delta_2 = 0$, we have $f_{1,3} \equiv 0 \pmod{n_4}$ and $g_{1,3} \equiv 0 \pmod{n_5}$. Taking $\delta_2 = \delta_3 = \varepsilon_1 = 1$, we have $2f_{1,2} \equiv 1 \pmod{n_4}$ and $g_{1,2} \equiv 0 \pmod{n_5}$.

Conversely, suppose that $f_{1,1} \equiv f_{1,3} \equiv 0 \pmod{n_4}$, $f_{1,2} \equiv \frac{1}{2} \pmod{n_4}$, and $g_{1,1} \equiv g_{1,2} \equiv g_{1,3} \equiv 0 \pmod{n_5}$. It is straightforward to prove that the congruences (6) and (7) hold. Hence $h_1(h_2+h_3)+h_1 = h_1h_2+h_1h_3$ and the first part of the result follows.

That the ideal $\langle a, b\rangle$ is contained in $\mathrm{Soc}(G)$ and that the left brace $G/\langle a, b\rangle$ is standard nilpotent of class two follows at once from the definition of the addition. □

## 4. Metabelian groups

In this section we give necessary and sufficient conditions for a group $G$ to be the multiplicative group of a left brace such that $[G, G] \subseteq \mathrm{Soc}(G)$ and $G/[G, G]$ is a standard abelian brace. Clearly, in this case, the multiplicative group $G$ is metabelian. Next we present a class of examples of metabelian groups that satisfy the required conditions. In the context of the previous sections notice that nilpotent groups of class 3 are metabelian.

If $G$ is a left brace then the function $\gamma\colon G \times G \to G$ defined by $\gamma(a, b) = (a + b)b^{-1}a^{-1}$ is a measure for $G$ to be a standard abelian brace. It is this function that plays a crucial role in this section (it always satisfies property (a) and property (b), for $s \in \mathrm{Soc}(G)$, of the following theorem).

The following result generalises Theorem 1 in [**2**] on nilpotent groups of class two that are multiplicative groups of two-sided braces (or, equivalently, that are circle groups of radical rings).

**Theorem 4.1.** *The following conditions are equivalent for a group $G$.*

(1) *$G$ is the multiplicative group of a left brace $(G, +, \cdot)$ such that $[G, G] \subseteq \mathrm{Soc}(G)$ and $G/[G, G]$ is a standard abelian brace.*

(2) *$G$ is metabelian and there exists a map $\gamma\colon G \times G \to [G, G]$ that satisfies the following properties:*

   (a) $\gamma(a, b) = \gamma(b, a)[b^{-1}, a^{-1}]$, *for all* $a, b \in G$,

   (b) $\gamma(s, a) = 1$, *for all* $a \in G$ *and all* $s \in [G, G]$,

   (c) $\gamma(ab, c) = \gamma(a, c)a\gamma(b, c)a^{-1}$, *for all* $a, b, c \in G$.

*Proof:* (1) implies (2). Assume that (1) is satisfied. Let $\gamma\colon G \times G \to [G, G]$ denote the map defined by $\gamma(a, b) = (a+b)b^{-1}a^{-1}$, for all $a, b \in G$. Since $G/[G, G]$ is a standard abelian brace, $(a + b)b^{-1}a^{-1} \in [G, G]$ and

thus $\gamma$ is well-defined. Then, for all $a, b \in G$,

$$\gamma(a,b) = (a+b)b^{-1}a^{-1} = (b+a)a^{-1}b^{-1}[b^{-1},a^{-1}] = \gamma(b,a)[b^{-1},a^{-1}].$$

This proves (a). Let $s \in [G,G]$ and $a \in G$. Since $[G,G] \subseteq \mathrm{Soc}(G)$, we have that $s + a = sa$. Hence $\gamma(s,a) = (s+a)a^{-1}s^{-1} = saa^{-1}s^{-1} = 1$, and (b) follows.

Recall that in the left brace $G$ the map $\lambda\colon G \to \mathrm{Aut}(G,+)$, defined by $\lambda(a) = \lambda_a$, for all $a \in G$, is a homomorphism from the multiplicative group of the left brace $G$ to the group of automorphisms of the additive group of $G$, where $\lambda_a(b) = ab - a$, for all $a, b \in G$. In particular,

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

We shall use this formula without any mention.

Let $a, b, c \in G$. Note that $\gamma(a,b) = (a+b)b^{-1}a^{-1} = a\lambda_a^{-1}(b)b^{-1}a^{-1}$. Hence $\lambda_a^{-1}(b)b^{-1} \in [G,G]$. We get that

$$\begin{aligned}
\gamma(ab,c) &= ab\lambda_{ab}^{-1}(c)c^{-1}b^{-1}a^{-1},\\
\gamma(a,c)a\gamma(b,c)a^{-1} &= a\lambda_a^{-1}(c)c^{-1}a^{-1}ab\lambda_b^{-1}(c)c^{-1}b^{-1}a^{-1}\\
&= a\lambda_a^{-1}(c)c^{-1}b\lambda_b^{-1}(c)c^{-1}b^{-1}a^{-1},
\end{aligned}$$

and

$$\begin{aligned}
b\lambda_{ab}^{-1}(c) &= b(b^{-1}a^{-1}c - b^{-1}a^{-1}) = a^{-1}c - a^{-1} + b = \lambda_a^{-1}(c) + b,\\
\lambda_a^{-1}(c)c^{-1}b\lambda_b^{-1}(c) &= \lambda_a^{-1}(c)c^{-1}b(b^{-1}c - b^{-1}) = \lambda_a^{-1}(c)(c^{-1}b - c^{-1})\\
&= \lambda_a^{-1}(c)\lambda_c^{-1}(b) = \lambda_{\lambda_a^{-1}(c)}(\lambda_c^{-1}(b)) + \lambda_a^{-1}(c)\\
&= \lambda_{\lambda_a^{-1}(c)c^{-1}}(b) + \lambda_a^{-1}(c) = b + \lambda_a^{-1}(c),
\end{aligned}$$

the last equality holds because $\lambda_a^{-1}(c)c^{-1} \in [G,G] \subseteq \mathrm{Soc}(G)$. Therefore (c) follows.

(2) implies (1). Assume that $\gamma\colon G \times G \to [G,G]$ satisfies (a), (b), and (c). The fact that $[G,G]$ is abelian and $\gamma(G \times G) \subseteq [G,G]$ will be used without any comment in this proof. We define an addition on $G$ by $a + b = \gamma(a,b)ab$, for all $a, b \in G$. We have, for $a, b, c \in G$,

$$\begin{aligned}
b + a &= \gamma(b,a)ba = \gamma(a,b)[a^{-1},b^{-1}]ba \quad \text{(by (a))}\\
&= \gamma(a,b)ab = a + b
\end{aligned}$$

and

(8)
$$\begin{aligned}(a+b)+c&=\gamma(a,b)ab+c\\&=\gamma(\gamma(a,b)ab,c)\gamma(a,b)abc\\&=\gamma(\gamma(a,b),c)\gamma(a,b)\gamma(ab,c)\gamma(a,b)^{-1}\gamma(a,b)abc && \text{(by (c))}\\&=\gamma(a,b)\gamma(ab,c)abc && \text{(by (b)).}\end{aligned}$$

Therefore

$$\begin{aligned}a+(b+c)&=(b+c)+a\\&=\gamma(b,c)\gamma(bc,a)bca && \text{(by (8))}\\&=\gamma(b,c)\gamma(b,a)b\gamma(c,a)b^{-1}bca && \text{(by (c))}\\&=\gamma(b,c)\gamma(a,b)aba^{-1}\gamma(a,c)ac && \text{(by (a))}\\&=\gamma(b,c)\gamma(a,b)aba^{-1}b^{-1}b\gamma(a,c)b^{-1}bac\\&=\gamma(b,c)\gamma(a,b)b\gamma(a,c)b^{-1}abc\\&=\gamma(a,b)\gamma(ba,c)abc && \text{(by (c))}\\&=\gamma(a,b)\gamma(ab[b,a],c)abc\\&=\gamma(a,b)\gamma(ab,c)ab\gamma([b,a],c)b^{-1}a^{-1}abc && \text{(by (c))}\\&=\gamma(a,b)\gamma(ab,c)abc && \text{(by (b))}\\&=(a+b)+c && \text{(by (8)).}\end{aligned}$$

Hence, $(a+b)+c=\gamma(a,b)\gamma(ab,c)abc$ and thus, also using (a), $a+(b+c)=(b+c)+a=\gamma(b,c)\gamma(bc,a)bca=\gamma(b,c)\gamma(a,bc)abc$. Therefore,

$$\gamma(a,b)\gamma(ab,c)=\gamma(b,c)\gamma(a,bc), \tag{9}$$

for all $a,b,c\in G$. Note that $1+a=\gamma(1,a)a=a$ and

$$\begin{aligned}\gamma(a^{-1},a)^{-1}a^{-1}+a&=\gamma(\gamma(a^{-1},a)^{-1}a^{-1},a)\gamma(a^{-1},a)^{-1}a^{-1}a\\&=\gamma(\gamma(a^{-1},a)^{-1},a)\gamma(a^{-1},a)^{-1}\gamma(a^{-1},a)\\&\quad\gamma(a^{-1},a)\gamma(a^{-1},a)^{-1} && \text{(by (c))}\\&=1 && \text{(by (b)).}\end{aligned}$$

Hence 1 is the neutral element for the addition and $-a=\gamma(a^{-1},a)^{-1}a^{-1}$, for all $a\in G$.

Furthermore

$$\begin{aligned}
a(b+c)+a &= a\gamma(b,c)bc+a\\
&= \gamma(a\gamma(b,c)bc,a)a\gamma(b,c)bca\\
&= \gamma(abc,a)a\gamma(b,c)bca && \text{(by (c) and (b))}\\
&= \gamma(ab,ca)\gamma(c,a)\gamma(ab,c)^{-1}a\gamma(b,c)bca && \text{(by (9))}\\
&= \gamma(ab,[c^{-1},a^{-1}]ac)\gamma(c,a)\gamma(ab,c)^{-1}a\gamma(b,c)bca\\
&= \gamma([c^{-1},a^{-1}]ac,ab)[c^{-1}a^{-1}[a^{-1},c^{-1}],b^{-1}a^{-1}]\\
&\quad \gamma(c,a)\gamma(ab,c)^{-1}a\gamma(b,c)bca && \text{(by (a))}\\
&= \gamma(ac,ab)[c^{-1}a^{-1}[a^{-1},c^{-1}],b^{-1}a^{-1}]\\
&\quad \gamma(c,a)\gamma(ab,c)^{-1}a\gamma(b,c)bca && \text{(by (c) and (b))}\\
&= \gamma(ab,ac)[b^{-1}a^{-1},c^{-1}a^{-1}][c^{-1}a^{-1}[a^{-1},c^{-1}],b^{-1}a^{-1}]\\
&\quad \gamma(c,a)\gamma(ab,c)^{-1}a\gamma(b,c)bca && \text{(by (a))}\\
&= \gamma(ab,ac)[b^{-1}a^{-1},c^{-1}a^{-1}][c^{-1},a^{-1}]\\
&\quad acabc^{-1}a^{-1}[a^{-1},c^{-1}]b^{-1}a^{-1}\gamma(c,a)\gamma(ab,c)^{-1}a\gamma(b,c)bca\\
&= \gamma(ab,ac)[b^{-1}a^{-1},c^{-1}a^{-1}][c^{-1}a^{-1},b^{-1}a^{-1}][c^{-1},a^{-1}]\\
&\quad ab[a^{-1},c^{-1}]b^{-1}a^{-1}\gamma(c,a)\gamma(ab,c)^{-1}a\gamma(b,c)bca\\
&= \gamma(ab,ac)[[a^{-1},c^{-1}],b^{-1}a^{-1}]\gamma(c,a)\gamma(ab,c)^{-1}a\gamma(b,c)bca\\
&= \gamma(ab,ac)[[a^{-1},c^{-1}],b^{-1}a^{-1}]\gamma(a,c)[a^{-1},c^{-1}]\\
&\quad \gamma(ab,c)^{-1}a\gamma(b,c)bca && \text{(by (a))}\\
&= \gamma(ab,ac)[[a^{-1},c^{-1}],b^{-1}a^{-1}][a^{-1},c^{-1}]abca && \text{(by (c))}\\
&= \gamma(ab,ac)[a^{-1},c^{-1}][[a^{-1},c^{-1}],b^{-1}a^{-1}]abca\\
&= \gamma(ab,ac)[a^{-1},c^{-1}][c^{-1},a^{-1}]ab[a^{-1},c^{-1}]b^{-1}a^{-1}abca\\
&= \gamma(ab,ac)abac\\
&= ab+ac,
\end{aligned}$$

for all $a,b,c\in G$. Hence $(G,+,\cdot)$ is a left brace. Note that (b) implies that $\lambda_s(a)=sa-s=\gamma(s,a)sa-s=s+a-s=a$, for all $s\in[G,G]$ and all $a\in G$. Thus $[G,G]\subseteq \mathrm{Soc}(G)$. Therefore $[G,G]$ is an ideal of the left brace $G$ and it is easy to see that $G/[G,G]$ is a standard abelian brace. This finishes the proof. □

Since any finite metabelian group $G$ with trivial centre is a semidirect product of $[G, G]$ and an abelian subgroup (Theorem C in [**1**]), the following example applies to any such group.

**Example 4.2.** Let $G = A \rtimes B$ be the semidirect product of two abelian (multiplicative) groups $A$ and $B$. Define an addition $+$ on $G$ by

$$a_1b_1 + a_2b_2 = a_1a_2b_1b_2,$$

where $a_1, a_2 \in A$ and $b_1, b_2 \in B$. By [**3**, Section 6], $(G, +, \cdot)$ is a left brace, called the semidirect product of the two standard abelian braces $A$ and $B$. This left brace satisfies condition (1) of Theorem 4.1. The corresponding $\gamma$ of condition (2) is given by the formula

$$\gamma(a_1b_1, a_2b_2) = [a_2^{-1}, b_1^{-1}].$$

Note that the example also was obtained in [**4**, Corollary 3.10] for finite braces.

In [**4**] an example is given (Example 4.4) of a nilpotent group $G$ of class 3 such that $G$ cannot be the multiplicative group of a left brace $(G, +, \cdot)$ with $[G, G] \subseteq \mathrm{Soc}(G)$ and $G/[G, G]$ a standard abelian brace. However, this group is the multiplicative group of a left brace (Example 4.3 in [**4**]) and this is proved by making use of IYB morphisms. This group is also the multiplicative group of a left brace constructed as in Section 2.

## 5. Finitely generated nilpotent groups of class 2

In this section we characterise finitely generated nilpotent groups $G$ of class 2 that are the multiplicative group of a left brace and such that $[G, G] \subseteq \mathrm{Soc}(G)$ and $G/[G, G]$ is a standard abelian brace.

**Lemma 5.1.** *Let $G$ be a left brace such that the multiplicative group of $G$ is a nilpotent group of class 2, $[G, G] \subseteq \mathrm{Soc}(G)$ and $G/[G, G]$ is a standard abelian brace. Then $G$ is a two-sided brace.*

*Proof:* Let $a, b, c \in G$. Then, as $[G, G] \subseteq \mathrm{Soc}(G)$,

$$(b + c)a = a(b + c)[b + c, a] = [b + c, a]a(b + c) = [b + c, a] + a(b + c).$$

Because $G/[G,G]$ is standard abelian, there exists $u \in [G,G] \subseteq Z(G)$ such that

$$\begin{aligned}(b+c)a &= [bcu,a] + a(b+c)\\ &= [bc,a] + ab + ac - a\\ &= [bc,a] + ba[a,b] + ca[a,c] - a\\ &= [bc,a] + ba + [a,b] + ca + [a,c] - a \quad (\text{as } [G,G] \subseteq \mathrm{Soc}(G))\\ &= [bc,a][a,b][a,c] + ba + ca - a \quad (\text{as } [G,G] \subseteq \mathrm{Soc}(G))\\ &= 1 + ba + ca - a\\ &= ba + ca - a.\end{aligned}$$

This proves that $G$ is a right brace, and thus a two-sided brace. □

**Theorem 5.2.** *Let $G$ be a finitely generated nilpotent group of class 2. Let $a_1, a_2, \ldots, a_n \in G$ and $c_1, c_2, \ldots, c_r \in [G,G]$ be elements such that $[G,G]$ is the inner direct product of the subgroups $\langle c_1\rangle, \ldots, \langle c_r\rangle$ and $G/[G,G]$ is the inner direct product of the subgroups $\langle a_1[G,G]\rangle, \ldots, \langle a_n[G,G]\rangle$. Then the following properties are equivalent.*

(1) *For each $1 \le i \le r$, there exists a map $s_i\colon \mathbb{Z}^n \times \mathbb{Z}^n \to \mathbb{Z}$ such that*
   (i) *$s_i$ is a symmetric bilinear map modulo $n_i$, that is*

$$\begin{aligned}&s_i((\alpha_1,\ldots,\alpha_n),(\beta_1,\ldots,\beta_n))\\ &\quad\equiv s_i((\beta_1,\ldots,\beta_n),(\alpha_1,\ldots,\alpha_n)) \pmod{n_i}\end{aligned}$$

   *and*

$$\begin{aligned}&s_i((\alpha_1+\beta_1,\ldots,\alpha_n+\beta_n),(\gamma_1,\ldots,\gamma_n))\\ &\quad\equiv s_i((\alpha_1,\ldots,\alpha_n),(\gamma_1,\ldots,\gamma_n))\\ &\qquad + s_i((\beta_1,\ldots,\beta_n),(\gamma_1,\ldots,\gamma_n)) \pmod{n_i},\end{aligned}$$

   *where $n_i$ is either the order of $c_i$, if $c_i$ has finite order, or $n_i = 0$ otherwise.*
   (ii) *$c_i^{s_i((\alpha_1,\ldots,\alpha_n),(\beta_1,\ldots,\beta_n))} = 1$, whenever $a_j^{\alpha_j} \in [G,G]$, for all $j$.*

(2) *$G$ is the multiplicative group of a two-sided brace such that $[G,G] \subseteq \mathrm{Soc}(G)$ and $G/[G,G]$ is a standard abelian brace.*

*Proof:* (1) implies (2). For $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in \mathbb{Z}$ and $c, c' \in [G,G]$, we define

(10)

$$\begin{aligned}&ca_1^{\alpha_1}\cdots a_n^{\alpha_n} + c'a_1^{\beta_1}\cdots a_n^{\beta_n}\\ &\quad= cc'c_1^{s_1((\alpha_1,\ldots,\alpha_n),(\beta_1,\ldots,\beta_n))}\cdots c_r^{s_r((\alpha_1,\ldots,\alpha_n),(\beta_1,\ldots,\beta_n))}a_1^{\alpha_1+\beta_1}\cdots a_n^{\alpha_n+\beta_n}.\end{aligned}$$

First we show that this is a well-defined operation. Let $c, d, c', d' \in [G,G]$ and $\alpha_i, \alpha_i', \beta_i, \beta_i' \in \mathbb{Z}$ be such that

$$ca_1^{\alpha_1} \cdots a_n^{\alpha_n} = da_1^{\alpha_1'} \cdots a_n^{\alpha_n'}$$

and

$$c'a_1^{\beta_1} \cdots a_n^{\beta_n} = d'a_1^{\beta_1'} \cdots a_n^{\beta_n'}.$$

We shall prove that

$$\begin{aligned} &cc'c_1^{s_1((\alpha_1,\ldots,\alpha_n),(\beta_1,\ldots,\beta_n))} \cdots c_r^{s_r((\alpha_1,\ldots,\alpha_n),(\beta_1,\ldots,\beta_n))} a_1^{\alpha_1+\beta_1} \cdots a_n^{\alpha_n+\beta_n} \\ &\quad = dd'c_1^{s_1((\alpha_1',\ldots,\alpha_n'),(\beta_1',\ldots,\beta_n'))} \cdots c_r^{s_r((\alpha_1',\ldots,\alpha_n'),(\beta_1',\ldots,\beta_n'))} a_1^{\alpha_1'+\beta_1'} \cdots a_n^{\alpha_n'+\beta_n'}. \end{aligned}$$

Since $G/[G,G]$ is the inner direct product of the subgroups $\langle a_1[G,G]\rangle, \ldots, \langle a_n[G,G]\rangle$, we get $a_j^{\alpha_j'-\alpha_j}, a_j^{\beta_j'-\beta_j} \in [G,G]$, for all $j = 1, \ldots, n$. Hence

$$\begin{aligned} cc'a_1^{\alpha_1+\beta_1} \cdots a_n^{\alpha_n+\beta_n} &= dd'a_1^{\alpha_1'-\alpha_1+\beta_1'-\beta_1} \cdots a_n^{\alpha_n'-\alpha_n+\beta_n'-\beta_n} a_1^{\alpha_1+\beta_1} \cdots a_n^{\alpha_n+\beta_n} \\ &= dd'a_1^{\alpha_1'+\beta_1'} \cdots a_n^{\alpha_n'+\beta_n'}. \end{aligned}$$

Furthermore, since $a_j^{\alpha_j'-\alpha_j}, a_j^{\beta_j'-\beta_j} \in [G,G]$, for all $j = 1, \ldots, n$, we have that $c_i^{s_i((\alpha_1'-\alpha_1,\ldots,\alpha_n'-\alpha_n),(\beta_1,\ldots,\beta_n))} = 1$ and $c_i^{s_i((\beta_1'-\beta_1,\ldots,\beta_n'-\beta_n),(\alpha_1',\ldots,\alpha_n'))} = 1$, and thus

$$\begin{aligned} c_i^{s_i((\alpha_1,\ldots,\alpha_n),(\beta_1,\ldots,\beta_n))} &= c_i^{s_i((\alpha_1',\ldots,\alpha_n'),(\beta_1,\ldots,\beta_n))} = c_i^{s_i((\beta_1,\ldots,\beta_n),(\alpha_1',\ldots,\alpha_n'))} \\ &= c_i^{s_i((\beta_1',\ldots,\beta_n'),(\alpha_1',\ldots,\alpha_n'))} = c_i^{s_i((\alpha_1',\ldots,\alpha_n'),(\beta_1',\ldots,\beta_n'))}. \end{aligned}$$

Therefore

$$\begin{aligned} &cc'c_1^{s_1((\alpha_1,\ldots,\alpha_n),(\beta_1,\ldots,\beta_n))} \cdots c_r^{s_r((\alpha_1,\ldots,\alpha_n),(\beta_1,\ldots,\beta_n))} a_1^{\alpha_1+\beta_1} \cdots a_n^{\alpha_n+\beta_n} \\ &\quad = dd'c_1^{s_1((\alpha_1',\ldots,\alpha_n'),(\beta_1',\ldots,\beta_n'))} \cdots c_r^{s_r((\alpha_1',\ldots,\alpha_n'),(\beta_1',\ldots,\beta_n'))} a_1^{\alpha_1'+\beta_1'} \cdots a_n^{\alpha_n'+\beta_n'} \end{aligned}$$

and the addition is well-defined.

Next we prove that $(G,+)$ is an abelian group. Since every map $s_i$ is symmetric modulo $n_i$, we have that $g + g' = g' + g$, for all $g, g' \in G$. It is clear that $g + 1 = g$, for all $g \in G$ and that the opposite element of $ca_1^{\alpha_1} \cdots a_n^{\alpha_n}$ is

$$c^{-1}c_1^{-s_1((\alpha_1,\ldots,\alpha_n),(-\alpha_1,\ldots,-\alpha_n))} \cdots c_r^{-s_r((\alpha_1,\ldots,\alpha_n),(-\alpha_1,\ldots,-\alpha_n))} a_1^{-\alpha_1} \cdots a_n^{-\alpha_n},$$

for all $c \in [G,G]$ and $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$.

Let $c, d, e \in [G, G]$ and $\alpha_i, \beta_i, \gamma_i \in \mathbb{Z}$, for $i = 1, \ldots, n$. We have

$$
\begin{aligned}
&ca_1^{\alpha_1} \cdots a_n^{\alpha_n} + (da_1^{\beta_1} \cdots a_n^{\beta_n} + ea_1^{\gamma_1} \ldots a_n^{\gamma_n}) \\
&\quad = ca_1^{\alpha_1} \cdots a_n^{\alpha_n} + dec_1^{s_1((\beta_1,\ldots,\beta_n),(\gamma_1,\ldots,\gamma_n))} \cdots c_r^{s_r((\beta_1,\ldots,\beta_n),(\gamma_1,\ldots,\gamma_n))} \\
&\qquad a_1^{\beta_1+\gamma_1} \cdots a_n^{\beta_n+\gamma_n} \\
&\quad = cdec_1^{s_1((\beta_1,\ldots,\beta_n),(\gamma_1,\ldots,\gamma_n))} \cdots c_r^{s_r((\beta_1,\ldots,\beta_n),(\gamma_1,\ldots,\gamma_n))} \\
&\qquad c_1^{s_1((\alpha_1,\ldots,\alpha_n),(\beta_1+\gamma_1,\ldots,\beta_n+\gamma_n))} \cdots c_r^{s_r((\alpha_1,\ldots,\alpha_n),(\beta_1+\gamma_1,\ldots,\beta_n+\gamma_n))} \\
&\qquad a_1^{\alpha_1+\beta_1+\gamma_1} \cdots a_n^{\alpha_n+\beta_n+\gamma_n} \\
&\quad = cdec_1^{s_1((\beta_1,\ldots,\beta_n),(\gamma_1,\ldots,\gamma_n))} \cdots c_r^{s_r((\beta_1,\ldots,\beta_n),(\gamma_1,\ldots,\gamma_n))} \\
&\qquad c_1^{s_1((\alpha_1,\ldots,\alpha_n),(\beta_1,\ldots,\beta_n))} \cdots c_r^{s_r((\alpha_1,\ldots,\alpha_n),(\beta_1,\ldots,\beta_n))} \\
&\qquad c_1^{s_1((\alpha_1,\ldots,\alpha_n),(\gamma_1,\ldots,\gamma_n))} \cdots c_r^{s_r((\alpha_1,\ldots,\alpha_n),(\gamma_1,\ldots,\gamma_n))} \\
&\qquad a_1^{\alpha_1+\beta_1+\gamma_1} \cdots a_n^{\alpha_n+\beta_n+\gamma_n}
\end{aligned}
$$

and

$$
\begin{aligned}
&(ca_1^{\alpha_1} \cdots a_n^{\alpha_n} + da_1^{\beta_1} \cdots a_n^{\beta_n}) + ea_1^{\gamma_1} \cdots a_n^{\gamma_n} \\
&\quad = cdc_1^{s_1((\alpha_1,\ldots,\alpha_n),(\beta_1,\ldots,\beta_n))} \cdots c_r^{s_r((\alpha_1,\ldots,\alpha_n),(\beta_1,\ldots,\beta_n))} \\
&\qquad a_1^{\alpha_1+\beta_1} \cdots a_n^{\alpha_n+\beta_n} + ea_1^{\gamma_1} \cdots a_n^{\gamma_n} \\
&\quad = cdec_1^{s_1((\alpha_1,\ldots,\alpha_n),(\beta_1,\ldots,\beta_n))} \cdots c_r^{s_r((\alpha_1,\ldots,\alpha_n),(\beta_1,\ldots,\beta_n))} \\
&\qquad c_1^{s_1((\alpha_1+\beta_1,\ldots,\alpha_n+\beta_n),(\gamma_1,\ldots,\gamma_n))} \cdots c_r^{s_r((\alpha_1+\beta_1,\ldots,\alpha_n+\beta_n),(\gamma_1,\ldots,\gamma_n))} \\
&\qquad a_1^{\alpha_1+\beta_1+\gamma_1} \cdots a_n^{\alpha_n+\beta_n+\gamma_n} \\
&\quad = cdec_1^{s_1((\alpha_1,\ldots,\alpha_n),(\beta_1,\ldots,\beta_n))} \cdots c_r^{s_r((\alpha_1,\ldots,\alpha_n),(\beta_1,\ldots,\beta_n))} \\
&\qquad c_1^{s_1((\alpha_1,\ldots,\alpha_n),(\gamma_1,\ldots,\gamma_n))} \cdots c_r^{s_r((\alpha_1,\ldots,\alpha_n),(\gamma_1,\ldots,\gamma_n))} \\
&\qquad c_1^{s_1((\beta_1,\ldots,\beta_n),(\gamma_1,\ldots,\gamma_n))} \cdots c_r^{s_r((\beta_1,\ldots,\beta_n),(\gamma_1,\ldots,\gamma_n))} \\
&\qquad a_1^{\alpha_1+\beta_1+\gamma_1} \cdots a_n^{\alpha_n+\beta_n+\gamma_n}.
\end{aligned}
$$

Therefore $(G, +)$ is an abelian group.

Third we prove that the brace condition is satisfied. We also have

$$
\begin{aligned}
&ca_1^{\alpha_1}\cdots a_n^{\alpha_n}(da_1^{\beta_1}\cdots a_n^{\beta_n}+ea_1^{\gamma_1}\cdots a_n^{\gamma_n})+ca_1^{\alpha_1}\cdots a_n^{\alpha_n}\\
&\quad=ca_1^{\alpha_1}\cdots a_n^{\alpha_n}dec_1^{s_1((\beta_1,\ldots,\beta_n),(\gamma_1,\ldots,\gamma_n))}\cdots c_r^{s_r((\beta_1,\ldots,\beta_n),(\gamma_1,\ldots,\gamma_n))}\\
&\qquad a_1^{\beta_1+\gamma_1}\cdots a_n^{\beta_n+\gamma_n}+ca_1^{\alpha_1}\cdots a_n^{\alpha_n}\\
&\quad=cdec_1^{s_1((\beta_1,\ldots,\beta_n),(\gamma_1,\ldots,\gamma_n))}\cdots c_r^{s_r((\beta_1,\ldots,\beta_n),(\gamma_1,\ldots,\gamma_n))}\\
&\qquad\left(\prod_{1\le i<j\le n}[a_j,a_i]^{\alpha_j(\beta_i+\gamma_i)}\right)a_1^{\alpha_1+\beta_1+\gamma_1}\cdots a_n^{\alpha_n+\beta_n+\gamma_n}+ca_1^{\alpha_1}\cdots a_n^{\alpha_n}\\
&\quad=c^2dec_1^{s_1((\beta_1,\ldots,\beta_n),(\gamma_1,\ldots,\gamma_n))}\cdots c_r^{s_r((\beta_1,\ldots,\beta_n),(\gamma_1,\ldots,\gamma_n))}\\
&\qquad\left(\prod_{1\le i<j\le n}[a_j,a_i]^{\alpha_j(\beta_i+\gamma_i)}\right)\\
&\qquad c_1^{s_1((\alpha_1+\beta_1+\gamma_1,\ldots,\alpha_n+\beta_n+\gamma_n),(\alpha_1,\ldots,\alpha_n))}\cdots\\
&\qquad\qquad\qquad\cdots c_r^{s_r((\alpha_1+\beta_1+\gamma_1,\ldots,\alpha_n+\beta_n+\gamma_n),(\alpha_1,\ldots,\alpha_n))}\\
&\qquad a_1^{2\alpha_1+\beta_1+\gamma_1}\cdots a_n^{2\alpha_n+\beta_n+\gamma_n}
\end{aligned}
$$

and

$$
\begin{aligned}
&ca_1^{\alpha_1}\cdots a_n^{\alpha_n}da_1^{\beta_1}\cdots a_n^{\beta_n}+ca_1^{\alpha_1}\cdots a_n^{\alpha_n}ea_1^{\gamma_1}\cdots a_n^{\gamma_n}\\
&\qquad=cd\left(\prod_{1\le i<j\le n}[a_j,a_i]^{\alpha_j\beta_i}\right)a_1^{\alpha_1+\beta_1}\cdots a_n^{\alpha_n+\beta_n}\\
&\qquad\quad+ce\left(\prod_{1\le i<j\le n}[a_j,a_i]^{\alpha_j\gamma_i}\right)a_1^{\alpha_1+\gamma_1}\cdots a_n^{\alpha_n+\gamma_n}\\
&\qquad=c^2de\left(\prod_{1\le i<j\le n}[a_j,a_i]^{\alpha_j(\beta_i+\gamma_i)}\right)\\
&\qquad\quad c_1^{s_1((\alpha_1+\beta_1,\ldots,\alpha_n+\beta_n),(\alpha_1+\gamma_1,\ldots,\alpha_n+\gamma_n))}\cdots\\
&\qquad\qquad\qquad\cdots c_r^{s_r((\alpha_1+\beta_1,\ldots,\alpha_n+\beta_n),(\alpha_1+\gamma_1,\ldots,\alpha_n+\gamma_n))}\\
&\qquad\quad a_1^{2\alpha_1+\beta_1+\gamma_1}\cdots a_n^{2\alpha_n+\beta_n+\gamma_n}.
\end{aligned}
$$

Since every $s_i$ is a symmetric bilinear map modulo $n_i$, we obtain that

$$ca_1^{\alpha_1}\cdots a_n^{\alpha_n}(da_1^{\beta_1}\cdots a_n^{\beta_n}+ea_1^{\gamma_1}\cdots a_n^{\gamma_n})+ca_1^{\alpha_1}\cdots a_n^{\alpha_n}$$
$$=ca_1^{\alpha_1}\cdots a_n^{\alpha_n}da_1^{\beta_1}\cdots a_n^{\beta_n}+ca_1^{\alpha_1}\cdots a_n^{\alpha_n}ea_1^{\gamma_1}\cdots a_n^{\gamma_n}.$$

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

It is clear that $[G,G]\subseteq \mathrm{Soc}(G)$ and $G/[G,G]$ is a standard abelian brace. By Lemma 5.1, $(G,+,\cdot)$ is a two-sided brace. This finishes the proof of (1) implies (2).

(2) implies (1). Suppose that $G$ is the multiplicative group of a left brace such that $[G,G]\subseteq \mathrm{Soc}(G)$ and $G/[G,G]$ is the standard abelian brace. For every $i=1,\dots,r$, there exists a map $s_i\colon \mathbb{Z}^n\times\mathbb{Z}^n\to\mathbb{Z}$ such that, for given $c,c'\in[G,G]$ and for $\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_n\in\mathbb{Z}$,

$$ca_1^{\alpha_1}\cdots a_n^{\alpha_n}+c'a_1^{\beta_1}\cdots a_n^{\beta_n}$$
$$=cc'c_1^{s_1((\alpha_1,\dots,\alpha_n),(\beta_1,\dots,\beta_n))}\cdots c_r^{s_r((\alpha_1,\dots,\alpha_n),(\beta_1,\dots,\beta_n))}a_1^{\alpha_1+\beta_1}\cdots a_n^{\alpha_n+\beta_n}.$$

The commutativity of the addition implies that

$$s_i((\alpha_1,\dots,\alpha_n),(\beta_1,\dots,\beta_n))\equiv s_i((\beta_1,\dots,\beta_n),(\alpha_1,\dots,\alpha_n))\ (\mathrm{mod}\, n_i).$$

So, $s_i$ is symmetric modulo $n_i$. To prove it is bilinear modulo $n_i$ as well, we first notice that the associativity of the addition implies that

$$\begin{aligned}&s_i((\alpha_1,\dots,\alpha_n),(\beta_1,\dots,\beta_n))\\&\quad+s_i((\alpha_1+\beta_1,\dots,\alpha_n+\beta_n),(\gamma_1,\dots,\gamma_n))\\&\equiv s_i((\beta_1,\dots,\beta_n),(\gamma_1,\dots,\gamma_n))\\&\quad+s_i((\alpha_1,\dots,\alpha_n),(\beta_1+\gamma_1,\dots,\beta_n+\gamma_n))\ (\mathrm{mod}\, n_i).\end{aligned}\tag{11}$$

Since, for $c,d,e\in[G,G]$,

$$ca_1^{\alpha_1}\cdots a_n^{\alpha_n}(da_1^{\beta_1}\cdots a_n^{\beta_n}+ea_1^{\gamma_1}\cdots a_n^{\gamma_n})+ca_1^{\alpha_1}\cdots a_n^{\alpha_n}$$
$$=ca_1^{\alpha_1}\cdots a_n^{\alpha_n}da_1^{\beta_1}\cdots a_n^{\beta_n}+ca_1^{\alpha_1}\cdots a_n^{\alpha_n}ea_1^{\gamma_1}\cdots a_n^{\gamma_n},$$

one can check that

$$\begin{aligned}&s_i((\alpha_1+\beta_1,\dots,\alpha_n+\beta_n),(\alpha_1+\gamma_1,\dots,\alpha_n+\gamma_n))\\&\equiv s_i((\beta_1,\dots,\beta_n),(\gamma_1,\dots,\gamma_n))\\&\quad+s_i((\alpha_1+\beta_1+\gamma_1,\dots,\alpha_n+\beta_n+\gamma_n),(\alpha_1,\dots,\alpha_n))\ (\mathrm{mod}\, n_i).\end{aligned}\tag{12}$$

By (11), we have that

$$\begin{aligned}
&s_i(((\alpha_1+\beta_1)+\gamma_1,\dots,(\alpha_n+\beta_n)+\gamma_n),(\alpha_1,\dots,\alpha_n))\\
&\quad\equiv -s_i((\alpha_1+\beta_1,\dots,\alpha_n+\beta_n),(\gamma_1,\dots,\gamma_n))\\
&\qquad + s_i((\gamma_1,\dots,\gamma_n),(\alpha_1,\dots,\alpha_n))\\
&\qquad + s_i((\alpha_1+\beta_1,\dots,\alpha_n+\beta_n),(\gamma_1+\alpha_1,\dots,\gamma_n+\alpha_n)) \pmod{n_i}.
\end{aligned}$$

Hence, from (12), we have that

$$\begin{aligned}
&s_i((\alpha_1+\beta_1,\dots,\alpha_n+\beta_n),(\alpha_1+\gamma_1,\dots,\alpha_n+\gamma_n))\\
&\quad\equiv s_i((\beta_1,\dots,\beta_n),(\gamma_1,\dots,\gamma_n))\\
&\qquad - s_i((\alpha_1+\beta_1,\dots,\alpha_n+\beta_n),(\gamma_1,\dots,\gamma_n))\\
&\qquad + s_i((\gamma_1,\dots,\gamma_n),(\alpha_1,\dots,\alpha_n))\\
&\qquad + s_i((\alpha_1+\beta_1,\dots,\alpha_n+\beta_n),(\gamma_1+\alpha_1,\dots,\gamma_n+\alpha_n)) \pmod{n_i}.
\end{aligned}$$

Therefore

$$\begin{aligned}
&s_i((\alpha_1+\beta_1,\dots,\alpha_n+\beta_n),(\gamma_1,\dots,\gamma_n))\\
&\quad\equiv s_i((\gamma_1,\dots,\gamma_n),(\alpha_1,\dots,\alpha_n))+s_i((\beta_1,\dots,\beta_n),(\gamma_1,\dots,\gamma_n))\\
&\quad\equiv s_i((\alpha_1,\dots,\alpha_n),(\gamma_1,\dots,\gamma_n))+s_i((\beta_1,\dots,\beta_n),(\gamma_1,\dots,\gamma_n)) \pmod{n_i}.
\end{aligned}$$

So $s_i$ is a symmetric bilinear map modulo $n_i$.

Let $\alpha_1,\dots,\alpha_n$ be integers such that $a_j^{\alpha_j} \in [G,G]$, for $j=1,\dots,n$. Then, since $[G,G]\subseteq \mathrm{Soc}(G)$, we have that

$$a_1^{\alpha_1}\cdots a_n^{\alpha_n} + a_1^{\beta_1}\cdots a_n^{\beta_n} = a_1^{\alpha_1}\cdots a_n^{\alpha_n} a_1^{\beta_1}\cdots a_n^{\beta_n} = a_1^{\alpha_1+\beta_1}\cdots a_n^{\alpha_n+\beta_n}.$$

On the other hand we have that

$$\begin{aligned}
&a_1^{\alpha_1}\cdots a_n^{\alpha_n} + a_1^{\beta_1}\cdots a_n^{\beta_n}\\
&\quad = c_1^{s_1((\alpha_1,\dots,\alpha_n),(\beta_1,\dots,\beta_n))}\cdots c_r^{s_r((\alpha_1,\dots,\alpha_n),(\beta_1,\dots,\beta_n))} a_1^{\alpha_1+\beta_1}\cdots a_n^{\alpha_n+\beta_n}.
\end{aligned}$$

Hence $c_1^{s_1((\alpha_1,\dots,\alpha_n),(\beta_1,\dots,\beta_n))}\cdots c_r^{s_r((\alpha_1,\dots,\alpha_n),(\beta_1,\dots,\beta_n))} = 1$. Since $[G,G]$ is the inner direct product of the subgroups $\langle c_1\rangle,\dots,\langle c_r\rangle$, we get that

$$c_i^{s_i((\alpha_1,\dots,\alpha_n),(\beta_1,\dots,\beta_n))} = 1,$$

for $i=1,\dots,r$, and this finishes the proof. □

Of course, if $G$ is a finitely generated nilpotent group of class two and $G/[G,G]$ is torsion-free then condition (1) of Theorem 5.2 is satisfied for arbitrary chosen symmetric bilinear maps.

*Added in proof:* Recently Bachiller (in his paper "Counterexample to a conjecture about braces", arXiv: 1507.02137v1[math.GR]) has shown that there exists a group of order $23^{10}$ that is not the multiplicative group of any left brace.

**Acknowledgement.** This work was done while the third author was a Fellow at the Centre for Advanced Studies of the Royal Flemish Academy of Belgium for Science and the Arts. The author would like to thank the institute for its hospitality and support.

## References

[1] Z. Arad, E. Fisman, and M. Muzychuk, The structure of metabelian finite groups, in: *"Groups '93 Galway/St. Andrews"*, Vol. 1 (Galway, 1993), London Math. Soc. Lecture Note Ser. **211**, Cambridge Univ. Press, Cambridge, 1995, pp. 6–12. DOI: 10.1017/CBO9780511629280.004.

[2] J. C. Ault and J. F. Watters, Circle groups of nilpotent rings, *Amer. Math. Monthly* **80(1)** (1973), 48–52. DOI: 10.2307/2319260.

[3] F. Cedó, E. Jespers, and J. Okniński, Braces and the Yang–Baxter equation, *Comm. Math. Phys.* **327(1)** (2014), 101–116. DOI: 10.1007/s00220-014-1935-y.

[4] F. Cedó, E. Jespers, and Á. del Río, Involutive Yang–Baxter groups, *Trans. Amer. Math. Soc.* **362(5)** (2010), 2541–2558. DOI: 10.1090/S0002-9947-09-04927-7.

[5] V. G. Drinfeld, On some unsolved problems in quantum group theory, in: *"Quantum groups"* (Leningrad, 1990), Lecture Notes in Math. **1510**, Springer, Berlin, 1992, pp. 1–8. DOI: 10.1007/BFb0101175.

[6] P. Etingof, T. Schedler, and A. Soloviev, Set-theoretical solutions to the quantum Yang–Baxter equation, *Duke Math. J.* **100(2)** (1999), 169–209. DOI: 10.1215/S0012-7094-99-10007-X5.

[7] T. Gateva-Ivanova and P. Cameron, Multipermutation solutions of the Yang–Baxter equation, *Comm. Math. Phys.* **309(3)** (2012), 583–621. DOI: 10.1007/s00220-011-1394-7.

[8] T. Gateva-Ivanova and M. Van den Bergh, Semigroups of I-type, *J. Algebra* **206(1)** (1998), 97–112. DOI: 10.1006/jabr.1997.7399.

[9] M. Hall, Jr., *"The theory of groups"*, The Macmillan Co., New York, N.Y., 1959.

[10] E. Jespers and J. Okniński, *"Noetherian semigroup algebras"*, Algebras and Applications **7**, Springer, Dordrecht, 2007.

[11] Yu. I. Manin, Some remarks on Koszul algebras and quantum groups, *Ann. Inst. Fourier (Grenoble)* **37(4)** (1987), 191–205.
[12] W. Rump, A decomposition theorem for square-free unitary solutions of the quantum Yang–Baxter equation, *Adv. Math.* **193(1)** (2005), 40–55. DOI: 10.1016/j.aim.2004.03.019.
[13] W. Rump, Braces, radical rings, and the quantum Yang–Baxter equation, *J. Algebra* **307(1)** (2007), 153–170. DOI: 10.1016/j.jalgebra.2006.03.040.
[14] W. Rump, Classification of cyclic braces, *J. Pure Appl. Algebra* **209(3)** (2007), 671–685. DOI: 10.1016/j.jpaa.2006.07.001.
[15] W. Rump, The brace of a classical group, Lecture at the conference "Advances in Group Theory and Applications", Porto Cesareo, June 10–14, 2013.

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

Eric Jespers:
Department of Mathematics
Vrije Universiteit Brussel
Pleinlaan 2
1050 Brussel
Belgium
*E-mail address*: efjesper@vub.ac.be

Jan Okniński:
Institute of Mathematics
Warsaw University
Banacha 2
02-097 Warsaw
Poland
*E-mail address*: J.Okninski@mimuw.edu.pl

Primera versió rebuda el 10 de març de 2014,
darrera versió rebuda el 2 de juliol de 2014.