Hopf Algebras and Galois Module Theory
May 29 - June 2, 2023

# *Braces of size $np$*

Teresa Crespo, Daniel Gil-Muñoz, Anna Rio, Montserrat Vela

Thursday, June 1st

## Braces

A *(left) brace* is a triple $(B, +, \cdot)$, where $B$ is a set and $+$ and $\cdot$ are operations on $B$ such that

- $(B, +)$ is an abelian group,
- $(B, \cdot)$ is a group,
- for all $a, b, c \in B$,

$$a(b + c) = ab - a + ac, \quad \text{(brace relation)}.$$

We call $(B, +)$ the *additive group* and $(B, \cdot)$ the *multiplicative group* of the brace. The cardinal of $B$ is called the *size* of the brace.

For any abelian group $(A, +)$, $(A, +, +)$ is a brace, called *trivial brace*. Any brace of prime size is trivial (Bachiller).

For $B_1$ and $B_2$ braces, a map $f : B_1 \to B_2$ is a *brace morphism* if $f(b + b') = f(b) + f(b')$ and $f(bb') = f(b)f(b')$ for all $b, b' \in B_1$. If $f$ is bijective, we say that $f$ is an *isomorphism*. In that case we say that the braces $B_1$ and $B_2$ are *isomorphic*.

## Braces vs. holomorph

If $(B,+)$ is an abelian group and $G$ a regular subgroup of $\operatorname{Hol}(B) \simeq B \rtimes \operatorname{Aut} B$, then $\pi_{1|G} : G \to B, \quad (a,f) \mapsto a$ is bijective.

For a left brace $(B,+,\cdot)$ and each $a \in B$, we have a bijective map

$$\lambda_a : B \to B, \quad b \mapsto -a + a \cdot b.$$

We have $\lambda_a(b+c) = \lambda_a(b) + \lambda_a(c)$, $a \cdot b = a + \lambda_a(b)$, $\lambda_{a \cdot b} = \lambda_a \circ \lambda_b$.

**Proposition.** (Bachiller) *Let $(B,+,\cdot)$ be a left brace. Then*

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

*is a regular subgroup of* $\operatorname{Hol}(B,+)$, *isomorphic to* $(B,\cdot)$.
*Conversely, if $(B,+)$ is an abelian group and $G$ is a regular subgroup of* $\operatorname{Hol}(B,+)$, *then $B$ is a left brace with $(B,\cdot) \simeq G$, where*

$$a \cdot b = a + f(b), \quad (\pi_{1|G})^{-1}(a) = (a,f) \in G.$$

*These assignments give a bijective correspondence between isomorphism classes of left braces $(B,+,\cdot)$ and conjugacy classes of regular subgroups of* $\operatorname{Hol}(B,+)$.

## Semidirect product of braces

Let $(B_1, +, \cdot)$ and $(B_2, +, \cdot)$ be braces and $\tau : (B_2, \cdot) \to \mathrm{Aut}(B_1, +, \cdot)$ be a group morphism. Define in $B_1 \times B_2$

$$(a, b) + (a', b') = (a + a', b + b'), \quad (a, b) \cdot (a', b') = (a \cdot \tau(b)(a'), b \cdot b')$$

Then $(B_1 \times B_2, +, \cdot)$ is a brace which is called the *semidirect product* of the braces $B_1$ and $B_2$ via $\tau$.

If $\tau$ is the trivial morphism, then $(B_1 \times B_2, +, \cdot)$ is called the *direct product* of $B_1$ and $B_2$.

**Proposition.** *Let $p$ be a prime and $n$ an integer such that $p$ does not divide $n$ and each group of order $np$ has a unique normal subgroup of order $p$. Then every left brace of size $np$ is a direct or semidirect product of the trivial brace of size $p$ and a left brace of size $n$.*

*Proof.*
Let $B$ be a left brace of size $np$ with additive group $N$ and multiplicative group $G$. By the Schur-Zassenhaus theorem,

$N = \mathbb{Z}_p \times E$ with $E$ an abelian group of order $n$,

$G = \mathbb{Z}_p \rtimes_\tau F$ with $F$ a group of order $n$ and $\tau : F \to \mathrm{Aut}(\mathbb{Z}_p)$ a group morphism.

$\mathrm{Aut}(N) \simeq \mathrm{Aut}(\mathbb{Z}_p) \times \mathrm{Aut}(E) \Rightarrow \mathrm{Hol}(N) \simeq \mathrm{Hol}(\mathbb{Z}_p) \times \mathrm{Hol}(E)$.

$$(m, k, a, g) \in \mathrm{Hol}(N), m \in \mathbb{Z}_p, k \in \mathbb{Z}_p^*, a \in E, g \in \mathrm{Aut}(E)$$

$$(m, k, a, g)(m', k', a', g') = (m + km', kk', a + g(a'), gg').$$

$\{(x, \lambda_x) : x \in N\}$ is a regular subgroup of $\mathrm{Hol}(N)$ isomorphic to $G$. For $x := (0, a) \in E$, $(x, \lambda_x) = (0, k_a, a, g_a)$, where $(k_a, g_a) = \lambda_x$. Now

$$\widetilde{F} := \{(0, k_a, a, g_a) : a \in E\}$$

is a subgroup of $G$ of order $n$, hence conjugate to $F$.

Now the unique subgroup of $\mathrm{Hol}(N)$ isomorphic to $\mathbb{Z}_p$ and normalized by $\widetilde{F}$ is

$$\langle(1, 1, 0_E, \mathrm{Id})\rangle.$$

More precisely

$$(0, k_a, a, g_a)(1, 1, 0_E, \mathrm{Id})(0, k_a, a, g_a)^{-1} = k_a(1, 1, 0_E, \mathrm{Id}).$$

We have obtained that

- $\overline{F} = \{(a, g_a) \ : \ a \in E\}$ is a regular subgroup of $\mathrm{Hol}(E)$, isomorphic to $F$,
- the map $\tau : \overline{F} \to \mathbb{Z}_p^*, (a, g_a) \mapsto k_a$ is a group morphism,
- $\langle(1, 1, 0_E, \mathrm{Id})\rangle$ is a regular subgroup of $\mathrm{Hol}(\mathbb{Z}_p)$,
- the semidirect product $\mathbb{Z}_p \rtimes_\tau \overline{F}$ is isomorphic to $G$.

Hence $B$ is the semidirect product of the trivial brace of size $p$ and the brace of size $n$ corresponding to the regular subgroup $\overline{F}$ of $\mathrm{Hol}(E)$, via $\tau$.

**Proposition.** *Let $p$ be a prime and $n$ an integer such that $p$ does not divide $n$ and each group of order $np$ has a normal subgroup of order $p$. Let $N = \mathbb{Z}_p \times E$ be an abelian group of order $np$.*
*The conjugacy classes of regular subgroups of $\mathrm{Hol}(N)$ are in one-to-one correspondence with couples $(F, \tau)$ where $F$ runs over a set of representatives of conjugacy classes of regular subgroups of $\mathrm{Hol}(E)$ and $\tau$ runs over representatives of classes of group morphisms $\tau : F \to \mathrm{Aut}(\mathbb{Z}_p)$ under the relation $\tau \simeq \tau'$ if and only if there exists $\nu \in \mathrm{Aut}(E)$ such that the corresponding inner automorphism $\Phi_\nu$ of $\mathrm{Hol}(E)$ satisfies $\Phi_\nu(F) = F$ and $\tau = \tau' \circ \Phi_\nu|_F$.*

*Proof.*
For a given couple $(F, \tau)$ the corresponding regular subgroup of $\mathrm{Hol}(N)$ isomorphic to $\mathbb{Z}_p \rtimes_\tau F$ is

$$G = \{((m, \tau(f)), f) \mid \ m \in \mathbb{Z}_p, \ f \in F\} \subseteq (\mathbb{Z}_p \rtimes \mathbb{Z}_p^*) \times \mathrm{Hol}(E) = \mathrm{Hol}(N).$$

Since we are dealing with regular subgroups, we just have to consider conjugation by elements $(i, \nu) \in \mathrm{Aut}(N) = \mathbb{Z}_p^* \times \mathrm{Aut}(E)$.

Let $\Phi_{(i,\nu)}$ be the inner automorphism corresponding to $(i,\nu)$ inside $\mathrm{Hol}(N)$. Then,

$$\begin{aligned}\Phi_{(i,\nu)}(m,k,a,g) &= (0,i,0_E,\nu)(m,k,a,g)(0,i,0_E,\nu)^{-1}\\ &= (im,ik,\nu(a),\nu g)(0,i^{-1},0_E,\nu^{-1})\\ &= (im,k,\nu(a),\nu g\nu^{-1})\end{aligned}$$

If we work in $\mathrm{Hol}(E)$, conjugation by $\nu \in \mathrm{Aut}(E)$ is

$$\Phi_\nu(a,g) = (0_E,\nu)(a,g)(0_E,\nu^{-1}) = (\nu(a),\nu g\nu^{-1}).$$

Let $G = \mathbb{Z}_p \rtimes_\tau F = \{(m,\tau(a,g),a,g) \mid m \in \mathbb{Z}_p,\ (a,g) \in F\}$. Then,

$$\Phi_{(i,\nu)}(G) = \{(im,\tau(a,g),\nu(a),\nu g\nu^{-1}) \mid m \in \mathbb{Z}_p,\ (a,g) \in F\}.$$

Since $i \in \mathbb{Z}_p^*$, $im$ runs over $\mathbb{Z}_p$ as $m$ does. Therefore, if $(F',\tau')$ is another pair, we have

$$\Phi_{(i,\nu)}(G) = \mathbb{Z}_p \rtimes_{\tau'} F' \iff F' = \Phi_\nu(F),\ \text{ and } \tau = \tau' \circ \Phi_\nu|_F.$$

Let us observe that in that case $\mathrm{Ker}\,\tau' = \Phi_\nu(\mathrm{Ker}\,\tau)$.

(H): *$p$ is an prime number and $n$ an integer such that $p$ does not divide $n$ and each group of order $np$ has a normal subgroup of order $p$.*

(H) is satisfied, in particular, if

- $p > n$,
- $n = 8$, $p \neq 2, 3, 7$,
- $n = 12$, $p \geq 7$.

Let $b(s)$ denote the number of isomorphism classes of left braces of size $s$. Bardakov, Neschadim and Yadav stated the following conjectures.

$$\text{For } \ p \geq 11, \ b(8p) = \begin{cases} 90 & \text{if } p \equiv 3, 7 \pmod 8, \\ 106 & \text{if } p \equiv 5 \pmod 8, \\ 108 & \text{if } p \equiv 1 \pmod 8. \end{cases}$$

$$\text{For } \ p \geq 7, \ b(12p) = \begin{cases} 24 & \text{if } p \equiv 11 \pmod{12}, \\ 28 & \text{if } p \equiv 5 \pmod{12}, \\ 34 & \text{if } p \equiv 7 \pmod{12}, \\ 40 & \text{if } p \equiv 1 \pmod{12}. \end{cases}$$

## Braces of size $12p$

**Corollary.** Let $p \geq 7$ be a prime. Every left brace of size $12p$ is a direct or semidirect product of the trivial brace of size $p$ and a left brace of size 12.

Left braces of size 12

| $E \backslash F$ | $C_{12}$ | $C_6 \times C_2$ | $A_4$ | $D_{2 \cdot 6}$ | $\mathrm{Dic}_{12}$ |
|---|---|---|---|---|---|
| $C_{12}$ | 1 | 1 | 0 | 2 | 1 |
| $C_6 \times C_2$ | 1 | 1 | 1 | 1 | 1 |

$E$ is the additive group and $F$ the multiplicative group.

**Proposition.** For a prime number $p$, there are 10 left braces of size $12p$ which are direct product of the unique brace of size $p$ and a brace of size 12.

**Braces with additive group $C_{12p}$ and multiplicative group $C_p \rtimes (C_6 \times C_2)$**

For $E = C_{12} = \mathbb{Z}_{12}$, we have $\mathrm{Aut}(\mathbb{Z}_{12}) = \mathbb{Z}_{12}^* = \{1, 5, 7, 11\} \simeq C_2 \times C_2$ and $\mathrm{Hol}(\mathbb{Z}_{12}) = \{(x, \ell) : x \in \mathbb{Z}_{12}, \ell \in \mathbb{Z}_{12}^*\}$.

For $F = C_6 \times C_2$, we write $F = \langle x, y \rangle$, with $x$ of order 6, $y$ of order 2.

1) There are three morphisms from $F$ to $\mathbb{Z}_p^*$ with kernel of order 6, namely

$$\tau_1 : \begin{array}{rcr} x & \mapsto & 1 \\ y & \mapsto & -1 \end{array}, \qquad \tau_2 : \begin{array}{rcr} x & \mapsto & -1 \\ y & \mapsto & -1 \end{array}, \qquad \tau_3 : \begin{array}{rcr} x & \mapsto & -1 \\ y & \mapsto & 1 \end{array}.$$

2) If $p \equiv 1 \pmod 6$, let $\zeta_6$ be a generator of the unique subgroup of order 6 of $\mathbb{Z}_p^*$. We may define six morphisms from $F$ to $\mathbb{Z}_p^*$ with a kernel of order 2, namely

$$\tau_1 : \begin{array}{l} x \mapsto \zeta_6 \\ y \mapsto 1 \end{array} \Bigg| \tau_2 : \begin{array}{l} x \mapsto \zeta_6^{-1} \\ y \mapsto 1 \end{array} \Bigg| \tau_3 : \begin{array}{l} x \mapsto \zeta_6^2 \\ y \mapsto \zeta_6^3 \end{array} \Bigg| \tau_4 : \begin{array}{l} x \mapsto \zeta_6^{-2} \\ y \mapsto \zeta_6^3 \end{array} \Bigg| \tau_5 : \begin{array}{l} x \mapsto \zeta_6 \\ y \mapsto \zeta_6^3 \end{array} \Bigg| \tau_6 : \begin{array}{l} x \mapsto \zeta_6^{-1} \\ y \mapsto \zeta_6^3 \end{array}$$

and two morphisms from $F$ to $\mathbb{Z}_p^*$ with a kernel of order 4, namely

$$\tau_1 : \begin{array}{l} x \mapsto \zeta_6^2 \\ y \mapsto 1 \end{array} \qquad \tau_2 : \begin{array}{l} x \mapsto \zeta_6^{-2} \\ y \mapsto 1. \end{array}$$

We know that in $\mathrm{Hol}(C_{12})$ there is only one regular subgroup isomorphic to $F$. We may take

$$F = \langle x = (2,1), y = (3,7) \rangle \subset \mathrm{Hol}(E)$$

We determine the conjugation relations between the morphisms $\tau : F \to \mathbb{Z}_p^*$.

1) For the morphisms from $F$ to $\mathbb{Z}_p^*$ with kernel of order 6, we have $\tau_2 = \tau_3 \Phi_{11}$ and $\tau_1$ is not conjugate to the other two, since $\mathrm{Ker}\,\tau_1 = \langle x \rangle$, $\mathrm{Ker}\,\tau_2 = \langle xy \rangle$, $\mathrm{Ker}\,\tau_3 = \langle x^2 y \rangle$, the second component of $x$ is different from those of $xy$ and $x^2y$. We obtain then two braces.

2) For the morphisms from $F$ to $\mathbb{Z}_p^*$ with a kernel of order 4, we have $\tau_1 = \tau_2 \Phi_{11}$ and we obtain then a unique brace.

3) For the morphisms from $F$ to $\mathbb{Z}_p^*$ with a kernel of order 2, we observe that $\tau_2 = \tau_1 \Phi_5$, $\tau_5 = \tau_1 \Phi_7$, $\tau_6 = \tau_1 \Phi_{11}$ and $\tau_4 = \tau_3 \Phi_{11}$. So we obtain only two braces (determined by $\tau_1$ and $\tau_3$). Note that $\tau_1$ and $\tau_3$ are not conjugate since $\mathrm{Ker}\,\tau_1 = \langle y \rangle$, $\mathrm{Ker}\,\tau_3 = \langle x^3 \rangle$.

**Proposition.** Let $p \geq 7$ be a prime number. We count the left braces with additive group $C_{12p}$ and multiplicative group $\mathbb{Z}_p \rtimes (C_6 \times C_2)$.

1) If $p \equiv 5 \pmod 6$ there are 3 such braces. One of them is a direct product and the other two have a kernel of order 6.

2) If $p \equiv 1 \pmod 6$ there are 6 such braces. One of them is a direct product, two have kernel of order 6, two have kernels of order 2 and one has kernel of order 4.

Proceeding similarly for each pair $(E, F)$, for $E$ an abelian group of order 12, and $F$ a group of order 12, we obtain the number of left braces with additive group $\mathbb{Z}_p \times E$ and multiplicative group $\mathbb{Z}_p \rtimes F$. We show the results in the following tables. In particular we have established the validity of the conjecture by Bardakov, Neschadim and Yadav.

If $p \equiv 11 \pmod{12}$

| | $C_{12}$ | $C_6 \times C_2$ | $A_4$ | $D_{2\cdot 6}$ | $\mathrm{Dic}_{12}$ | |
|---|---|---|---|---|---|---|
| $C_{12}$ | 2 | 3 | 0 | 7 | 2 | 14 |
| $C_6 \times C_2$ | 2 | 2 | 1 | 3 | 2 | 10 |
| | 4 | 5 | 1 | 10 | 4 | **24** |

If $p \equiv 5 \pmod{12}$

| | $C_{12}$ | $C_6 \times C_2$ | $A_4$ | $D_{2\cdot 6}$ | $\mathrm{Dic}_{12}$ | |
|---|---|---|---|---|---|---|
| $C_{12}$ | 3 | 3 | 0 | 7 | 3 | 16 |
| $C_6 \times C_2$ | 3 | 2 | 1 | 3 | 3 | 12 |
| | 6 | 5 | 1 | 10 | 6 | **28** |

If $p \equiv 7 \pmod{12}$

| | $C_{12}$ | $C_6 \times C_2$ | $A_4$ | $D_{2\cdot 6}$ | $\mathrm{Dic}_{12}$ | |
|---|---|---|---|---|---|---|
| $C_{12}$ | 4 | 6 | 0 | 7 | 2 | 19 |
| $C_6 \times C_2$ | 4 | 4 | 2 | 3 | 2 | 15 |
| | 8 | 10 | 2 | 10 | 4 | **34** |

If $p \equiv 1 \pmod{12}$

| | $C_{12}$ | $C_6 \times C_2$ | $A_4$ | $D_{2\cdot 6}$ | $\mathrm{Dic}_{12}$ | |
|---|---|---|---|---|---|---|
| $C_{12}$ | 6 | 6 | 0 | 7 | 3 | 22 |
| $C_6 \times C_2$ | 6 | 4 | 2 | 3 | 3 | 18 |
| | 12 | 10 | 2 | 10 | 6 | **40** |

## References


[1] D. Bachiller, *Counterexample to a conjecture about braces*, J. Algebra 453 (2016) 160-176.

[2] V.G. Bardakov, M.V. Neshchadim, M.K. Yadav, *Computing skew left braces of small orders*, Internat. J. Algebra Comput. 30 (2020), no. 4, 839–851.

[3] T. Crespo, D. Gil-Muñoz, A. Rio, M. Vela, *Left braces of size* $8p$, J. Algebra 617, (2023), 317-339.

[4] T. Crespo, D. Gil-Muñoz, A. Rio, M. Vela, *Inducing braces and Hopf Galois structures*, J. Pure Appl. Algebra 227 (2023), no. 9, Paper No. 107371.

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

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