



Inducing braces and Hopf Galois structures [☆]

Teresa Crespo ^{a,*}, Daniel Gil-Muñoz ^b, Anna Rio ^c, Montserrat Vela ^c

^a *Departament de Matemàtiques i Informàtica, Universitat de Barcelona, Gran Via de les Corts Catalanes 585, 08007, Barcelona, Spain*

^b *Charles University, Faculty of Mathematics and Physics, Department of Algebra, Sokolovska 83, 18600 Praha 8, Czech Republic*

^c *Departament de Matemàtiques, Universitat Politècnica de Catalunya, Edifici Omega, Jordi Girona, 1-3, 08034, Barcelona, Spain*



ARTICLE INFO

Article history:

Received 16 November 2022

Received in revised form 16 January 2023

Available online 28 February 2023

Communicated by A. Solotar

MSC:

Primary: 16T05; 16T25; 12F10;
secondary: 20B35; 20B05; 20D20;
20D45

Keywords:

Left braces
Holomorphs
Regular subgroups
Hopf Galois structures

ABSTRACT

Let p be a prime number and let n be an integer not divisible by p and such that every group of order np has a normal subgroup of order p . (This holds in particular for $p > n$.) Under these hypotheses, we obtain a one-to-one correspondence between the isomorphism classes of braces of size np and the set of pairs $(B_n, [\tau])$, where B_n runs over the isomorphism classes of braces of size n and $[\tau]$ runs over the classes of group morphisms from the multiplicative group of B_n to $\mathbf{Z}_p^*$ under a certain equivalence relation. This correspondence gives the classification of braces of size np from the one of braces of size n . From this result we derive a formula giving the number of Hopf Galois structures of abelian type $\mathbf{Z}_p \times E$ on a Galois extension of degree np in terms of the number of Hopf Galois structures of abelian type E on a Galois extension of degree n . For a prime number $p \geq 7$, we apply the obtained results to describe all left braces of size $12p$ and determine the number of Hopf Galois structures of abelian type on a Galois extension of degree $12p$.

© 2023 The Author(s). Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

1. Introduction

In [11] Rump introduced an algebraic structure called brace to study set-theoretic solutions of the Yang-Baxter equation. 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 and the brace relation is satisfied, namely,

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

[☆] The first author was supported by grant PID2019-107297GB-I00 (Ministerio de Ciencia, Innovación y Universidades). The second author was supported by Czech Science Foundation, grant 21-00420M, and by Charles University Research Centre program UNCE/SCI/022.

* Corresponding author.

E-mail addresses: teresa.crespo@ub.edu (T. Crespo), daniel.gil-munoz@mff.cuni.cz (D. Gil-Muñoz), ana.rio@upc.edu (A. Rio), montse.vela@upc.edu (M. Vela).

for all $a, b, c \in B$. We call $N = (B, +)$ the additive group and $G = (B, \cdot)$ the multiplicative group of the left brace. The cardinal of B is called the size of the brace. If $(B, +)$ is not abelian, the corresponding brace is called a skew brace.

Given any abelian group $(A, +)$, it is easy to check that $(A, +, +)$ is a brace. Such a brace is called a trivial brace. We note that any brace of prime size is trivial (see [2] Proposition 2.4).

Let B_1 and B_2 be left braces. A map $f : B_1 \rightarrow B_2$ is said to be 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.

In [3] Bachiller proved that given an abelian group N , there is a bijective correspondence between left braces with additive group N , and regular subgroups of $\text{Hol}(N)$ such that isomorphic left braces correspond to regular subgroups of $\text{Hol}(N)$ which are conjugate by elements of $\text{Aut}(N)$.

In [5] Lemma 2.1, it is proved that $\text{Aut}(N)$, as a subgroup of $\text{Hol}(N)$, is action-closed with respect to the conjugation action of $\text{Hol}(N)$ on the set of regular subgroups of $\text{Hol}(N)$. Therefore, given an abelian group N , the set of isomorphism classes of left braces with additive group N is in bijective correspondence with the set of conjugacy classes of regular subgroups in $\text{Hol}(N)$.

In [1] skew left braces of size pq are classified, where $p > q$ are prime numbers. In [9] a classification of left braces of order p^2q , where p, q are prime numbers such that $q > p + 1$ is given. In [5] the following conjecture on the number $b(12p)$ of isomorphism classes of left braces of size $12p$ is formulated, where p is a prime number, $p \geq 7$.

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

We note that $b(24) = 96$, $b(36) = 46$ and $b(60) = 28$ (see [14]).

Let B_1 and B_2 be left braces. Then $B_1 \times B_2$ together with $+$ and $\cdot$ defined by

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

is a left brace called the direct product of the braces B_1 and B_2 .

Let B_1 and B_2 be left braces. Let $\tau : (B_2, \cdot) \rightarrow \text{Aut}(B_1, +, \cdot)$ be a morphism of groups. Consider in $B_1 \times B_2$ the additive structure of the direct product $(B_1, +) \times (B_2, +)$

$$(a, b) + (a', b') = (a + a', b + b')$$

and the multiplicative structure of the semidirect product $(B_1, \cdot) \rtimes_{\tau} (B_2, \cdot)$

$$(a, b) \cdot (a', b') = (a\tau_b(a'), bb')$$

Then, we get a left brace, which is called the semidirect product of the left braces B_1 and B_2 via τ .

A Hopf Galois structure on a finite extension of fields K/k is a pair $(\mathcal{H}, \mu)$ where $\mathcal{H}$ is a finite cocommutative k -Hopf algebra and μ is a Hopf action of $\mathcal{H}$ on K , i.e. a k -linear map $\mu : \mathcal{H} \rightarrow \text{End}_k(K)$ giving K a left $\mathcal{H}$ -module algebra structure and inducing a bijection $K \otimes_k \mathcal{H} \rightarrow \text{End}_k(K)$. Hopf Galois extensions were introduced by Chase and Sweedler in [6]. For a Galois field extension K/k with Galois group G , Greither and Pareigis [10] give a bijective correspondence between Hopf Galois structures on K/k and regular subgroups N of $\text{Sym}(G)$ normalized by $\lambda(G)$, where λ denotes left translation. For a given Hopf Galois structure on K/k , we will refer to the isomorphism class of the corresponding group N as the type of the Hopf Galois structure. By Byott translation theorem [4], a correspondence is established between regular subgroups N of

$\text{Sym}(G)$ normalized by $\lambda(G)$ and regular subgroups of the holomorph $\text{Hol}(N) = N \rtimes \text{Aut } N$. As a corollary, Byott obtains the following formula.

Proposition 1 ([4] Corollary to Proposition 1). *Let K/k be a Galois extension with Galois group G . Let N be a group of order $|G|$. Let $a(N, G)$ denote the number of Hopf Galois structures of type N on K/k and let $b(N, G)$ denote the number of regular subgroups of $\text{Hol}(N)$ isomorphic to G . Then*

$$a(N, G) = \frac{|\text{Aut } G|}{|\text{Aut } N|} b(N, G).$$

In [7] we have established a one-to-one correspondence between the set of isomorphism classes of braces of size $8p$, for a prime number $p \neq 3, 7$, and the set of pairs consisting of an isomorphism class of braces of size 8 and a certain class of morphisms $\tau : (B_n, \circ) \rightarrow \mathbf{Z}_p^*$. We have used this result to determine all braces of size $8p$. In this paper we generalize this result to braces of size np , where p is a prime number and n an integer not divisible by p and such that every group of order np has a normal subgroup of order p . We note that these hypotheses hold in particular for $p > n$. More precisely, Proposition 4 below gives that any brace of size np may be explicitly obtained from a brace $(B_n, \cdot, \circ)$ of size n and a group morphism $\tau : (B_n, \circ) \rightarrow \mathbf{Z}_p^*$. Moreover we obtain a one-to-one correspondence between isomorphism classes of braces of size np and pairs $(B_n, [\tau])$, where B_n runs over the isomorphism classes of braces of size n and $[\tau]$ runs over a set of classes of morphisms τ from $(B_n, \circ)$ to $\mathbf{Z}_p^*$ under the relation specified in Proposition 4. From our result on braces we derive a formula giving the number of Hopf Galois structures of abelian type $\mathbf{Z}_p \times E$ on a Galois extension of degree np . For a prime number $p \geq 7$, we apply the obtained results to describe all left braces of size $12p$ and determine the number of Hopf Galois structures of abelian type on a Galois extension of degree $12p$. As a consequence of our classification of left braces of size $12p$, for p a prime number, $p \geq 7$, we establish the validity of conjecture (1).

We note that in [12] and [13], Kohl considers also Hopf Galois structures on Galois extensions of degree np , where p is a prime number and n an integer, non divisible by p . He works under the hypotheses that all groups of order np have a normal subgroup of order p and that p is not a divisor of the order of the automorphism groups of any group of order n . He applies his method to several families of Galois extensions of degree a square free integer.

From now on, p and n will always satisfy the following hypotheses.

(H): p is a 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 .

2. Braces of size np

The following proposition is a generalization of [7], Proposition 1.

Proposition 2. *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 . 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 . Then, by the Schur-Zassenhaus theorem, $N = \mathbf{Z}_p \times E$ with E an abelian group of order n and $G = \mathbf{Z}_p \rtimes_{\tau} F$ with F a group of order n and $\tau : F \rightarrow \text{Aut}(\mathbf{Z}_p)$ a group morphism (the trivial one giving the direct product). Let us observe that, since we are working with the trivial brace of size p , the group of brace automorphisms is the classical group $\text{Aut}(\mathbf{Z}_p) \simeq \mathbf{Z}_p^*$.

Then, for $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in B$,

$$\begin{aligned} (a_1, a_2)((b_1, b_2) + (c_1, c_2)) + (a_1, a_2) &= (a_1, a_2)(b_1 + c_1, b_2 + c_2) + (a_1, a_2) = \\ &= (a_1 + \tau_{a_2}(b_1 + c_1) + a_1, a_2(b_2 + c_2) + a_2). \end{aligned}$$

On the other hand,

$$(a_1, a_2)(b_1, b_2) + (a_1, a_2)(c_1, c_2) = (a_1 + \tau_{a_2}(b_1) + a_1 + \tau_{a_2}(c_1), a_2b_2 + a_2c_2).$$

Therefore, from the brace condition of B we obtain an equality in the second component which tells us that we have a brace B' of size n with additive group E and multiplicative group F . Then, B is the semidirect product via τ of the trivial brace with group $\mathbf{Z}_p$ and this brace B' . $\square$

Remark 3. The third Sylow theorem gives that the hypotheses in Proposition 2 are satisfied in particular when $p > n$.

As a corollary to Proposition 2, we obtain that for each brace of size n , there is a left brace of size np which is the direct product of the unique brace of size p and the given brace of size n . The braces of size np which are a semidirect product of the unique brace of size p and a brace of size n are determined by the following proposition, which generalizes Proposition 4 in [7].

Proposition 4. 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 $N = \mathbf{Z}_p \times E$ be an abelian group of order np .

The conjugacy classes of regular subgroups of $\text{Hol}(N)$ are in one-to-one correspondence with couples (F, τ) where F runs over a set of representatives of conjugacy classes of regular subgroups of $\text{Hol}(E)$ and τ runs over representatives of classes of group morphisms $\tau : F \rightarrow \text{Aut}(\mathbf{Z}_p)$ under the relation $\tau \simeq \tau'$ if and only if there exists $\nu \in \text{Aut}(E)$ such that the corresponding inner automorphism Φ_ν of $\text{Hol}(E)$ satisfies $\Phi_\nu(F) = F$ and $\tau = \tau' \circ \Phi_\nu|_F$.

Proof. As in Proposition 2, we may apply the Schur-Zassenhaus theorem and obtain that groups of order np are semidirect products $G = \mathbf{Z}_p \rtimes_\tau F$ with F a group of order n and $\tau : F \rightarrow \text{Aut}(\mathbf{Z}_p)$ a group morphism.

For a given couple (F, τ) the semidirect product is

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

and the action on N is given by $((m, k), f)(z, x) = (m + kz, fx)$. Since G contains $\mathbf{Z}_p$, we have transitivity in the first component and G is regular in $\text{Hol}(N)$ if and only if F is regular in $\text{Hol}(E)$.

Let us describe inner automorphisms of $\text{Hol}(N) = (\mathbf{Z}_p \rtimes \mathbf{Z}_p^*) \times (E \rtimes \text{Aut}(E))$. We write elements in $\text{Hol}(N)$ as (m, k, a, σ) accordingly. Since we are dealing with regular subgroups, we just have to consider conjugation by elements $(i, \nu) \in \text{Aut}(N) = \mathbf{Z}_p^* \times \text{Aut}(E)$. Let $\Phi_{(i, \nu)}$ be the inner automorphism corresponding to (i, ν) inside $\text{Hol}(N)$. Then,

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

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

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

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

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

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

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

Let us observe that in that case $\ker \tau' = \Phi_{\nu}(\ker \tau)$. $\square$

3. Hopf Galois structures on a Galois field extension of degree np

From Proposition 4 we obtain the following corollary.

Corollary 5. *Let E be a group of order n , $N = \mathbf{Z}_p \times E$. Let F be a regular subgroup of $\text{Hol}(E)$ and $\tau : F \rightarrow \mathbf{Z}_p^*$ a group morphism. The length of the conjugacy class of the regular subgroup of $\text{Hol}(N)$ corresponding to (F, τ) is equal to the length of the conjugacy class of F in $\text{Hol}(E)$ times the number of morphisms from F to $\mathbf{Z}_p^*$ equivalent to τ under the relation defined in Proposition 4.*

Using this corollary, we shall determine, the number of regular subgroups of the holomorph of N . Applying then Byott's formula (Proposition 1), we shall obtain the number of Hopf Galois structures of abelian type on a Galois extension of degree np . We note that all these Galois structures are induced, in the sense of [8], by Theorem 9 in [8]. In order to apply Byott's formula, we determine the automorphisms of a semidirect product $\mathbf{Z}_p \rtimes_{\tau} F$.

Let $G = \mathbf{Z}_p \rtimes F$, with F a group of order n . By the Schur-Zassenhaus theorem, any subgroup of G of order equal to $|F|$ is conjugate to F . We assume that the semidirect product is not direct, then F has exactly p conjugates, namely $F_i := (i, 1_F)F(-i, 1_F)$, $0 \leq i \leq p-1$. If φ is an automorphism of G , then $\varphi(\mathbf{Z}_p) = \mathbf{Z}_p$ and $\varphi(F)$ is a subgroup of G isomorphic to F . We have then $\varphi(F) = F_i$ for some i . Let

$$S = \{\varphi \in \text{Aut } G : \varphi(F) = F\}.$$

Clearly S is a subgroup of $\text{Aut}(G)$. Let C_i denote conjugation by $(i, 1)$ in $\text{Aut}(G)$. Then $\{C_i\}_{0 \leq i \leq p-1}$ is a transversal of S in $\text{Aut}(G)$, hence $|\text{Aut}(G)| = p|S|$.

We give now a characterization of S in terms of $\text{Aut } \mathbf{Z}_p$, $\text{Aut } F$ and the morphism $\tau : F \rightarrow \text{Aut } \mathbf{Z}_p \simeq \mathbf{Z}_p^*$ defining the semidirect product $\mathbf{Z}_p \rtimes F$.

Proposition 6. *The image of the injective map*

$$S \rightarrow \text{Aut } \mathbf{Z}_p \times \text{Aut } F, \quad \varphi \mapsto (\varphi|_{\mathbf{Z}_p}, \varphi|_F)$$

is precisely the set of pairs $(f, g) \in \text{Aut } \mathbf{Z}_p \times \text{Aut } F$ such that $\tau g = \tau$.

Proof. Let $\varphi \in \text{Aut } G$. For $x \in F$, $1 \in \mathbf{Z}_p$, we have $x1 = \tau(x)x$. Applying φ to this equality, we get $\varphi(x)\varphi(1) = \varphi(\tau(x))\varphi(x)$. Now, since $\varphi(x) \in F$ and $\varphi(1) \in \mathbf{Z}_p$, we have $\varphi(x)\varphi(1) = \tau(\varphi(x))\varphi(1)\varphi(x)$. We obtain then the equality $\varphi(\tau(x)) = \tau(\varphi(x))\varphi(1)$. This implies $\varphi|_{\mathbf{Z}_p}\tau(x) = \tau(\varphi|_F(x))\varphi|_{\mathbf{Z}_p}$ in $\text{Aut } \mathbf{Z}_p$. Since $\text{Aut } \mathbf{Z}_p$ is commutative, we obtain $\tau = \tau\varphi|_F$.

Reciprocally, let $(f, g) \in \text{Aut } \mathbf{Z}_p \times \text{Aut } F$ such that $\tau g = \tau$. We define a map φ from $\mathbf{Z}_p \times F$ to $\mathbf{Z}_p \times F$ by $\varphi(i, x) = (f(i), g(x))$. Now φ is an automorphism of $\mathbf{Z}_p \rtimes_{\tau} F$ if and only if $\varphi((i, x)(j, y)) = \varphi((i, x))\varphi((j, y))$, equivalently $(f(i + \tau(x)j), g(xy)) = (f(i), g(x))(f(j), g(y)) = (f(i) + \tau(g(x))f(j), g(x)g(y))$. Since g is an

automorphism, the two second components coincide. Since f is an automorphism, the equality of the first components is equivalent to $f(\tau(x)j) = \tau(g(x))f(j)$ for all j , equivalently $f\tau(x) = \tau(g(x))f$, for all $x \in F$, which is fulfilled, since $\tau g = \tau$ and $\text{Aut } \mathbf{Z}_p$ is commutative. $\square$

Corollary 7. For $G = \mathbf{Z}_p \rtimes_{\tau} F$, with τ a nontrivial morphism from F to $\mathbf{Z}_p^*$, we have $|\text{Aut } G| = p(p-1)|S_0|$, where $S_0 = \{g \in \text{Aut } F \mid \tau g = \tau\}$.

Proof. From the proposition we obtain clearly $S = \text{Aut } \mathbf{Z}_p \times S_0$, hence $|\text{Aut } G| = p|S| = p(p-1)|S_0|$. $\square$

4. Braces of size $12p$: direct products

There are five groups of order 12, up to isomorphism, two abelian ones C_{12} and $C_6 \times C_2$ and three non-abelian ones, the alternating group A_4 , the dihedral group $D_{2,6}$ and the dicyclic group Dic_{12} . By computation with Magma, we obtain that the number of conjugacy classes of regular subgroups of $\text{Hol}(E)$ isomorphic to F , equivalently, the number of isomorphism classes of left braces with additive group E and multiplicative group F is as shown in the following table.

$E \backslash F$	C_{12}	$C_6 \times C_2$	A_4	$D_{2,6}$	Dic_{12}
C_{12}	1	1	0	2	1
$C_6 \times C_2$	1	1	1	1	1

For p a prime number, $p \geq 7$, the Sylow theorems give that a group G of order $12p$ has a normal subgroup H_p of order p . We obtain then the following corollary to Proposition 2.

Corollary 8. 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.

From the description of the braces of size 12 and the definition of direct product of braces we obtain the following result.

Proposition 9. 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.

5. Braces of size $12p$: semidirect products

For $p \geq 7$ and $n = 12$, the hypotheses of Proposition 4 are satisfied and we shall apply it to determine the braces of size $12p$ which are semidirect products of the unique brace of size p and a brace of size 12. To this end, we shall consider the braces of order 12 with additive group E and multiplicative group F and determine the classes of the morphisms $\tau : F \rightarrow \text{Aut}(\mathbf{Z}_p)$ under the relation described in Proposition 4. We note that finding all such morphisms τ reduces to consider the normal subgroups F' of F such that F/F' is a cyclic group C whose order divides $p-1$ and taking into account the automorphisms of C . From now on, the kernel of τ will be referred to as the kernel of the brace (or conjugation class of regular subgroups) determined by the pair (F, τ) .

Remark 10 (Description of the holomorphs). We consider now the abelian groups of order 12, that is, $E = C_{12}$ and $E = C_6 \times C_2$ and describe $\text{Hol}(E)$ in each case.

For $E = C_{12} = \mathbf{Z}_{12}$, we have $\text{Aut}(\mathbf{Z}_{12}) = \mathbf{Z}_{12}^* = \{1, 5, 7, 11\} \simeq C_2 \times C_2$ and $\text{Hol}(\mathbf{Z}_{12}) = \{(x, l) : x \in \mathbf{Z}_{12}, l \in \mathbf{Z}_{12}^*\}$ with product given by $(x, l)(y, m) = (x + ly, lm)$.

For $E = C_6 \times C_2$, we have $\text{Aut}(E) \simeq D_{2.6}$. We write $C_6 \times C_2 = \langle a \rangle \times \langle b \rangle$ and consider the automorphisms ρ, σ of E defined by

$$\begin{array}{ll} \rho : & a \mapsto a^5 b \\ & b \mapsto a^3 \end{array} \quad \begin{array}{ll} \sigma : & a \mapsto a^5 \\ & b \mapsto a^3 b \end{array}.$$

We may check that ρ has order 6, σ has order 2 and $\sigma\rho\sigma = \rho^{-1}$, hence $\text{Aut}(E) = \langle \rho, \sigma \rangle$. We have $\text{Hol}(E) = \{(x, \varphi) : x \in E, \varphi \in \text{Aut } E\}$ with product defined by $(x, \varphi)(y, \psi) = (x\varphi(y), \varphi\psi)$.

We shall use the descriptions above throughout this section.

5.1. $F = C_{12}$

Let us write $F = \langle x \rangle$. We determine now the possible morphisms $\tau : F \rightarrow \mathbf{Z}_p^*$. To be used in Section 6, we compute $S_0(\tau) = \{g \in \text{Aut } F \mid \tau g = \tau\}$. We have $\text{Aut } C_{12} \simeq \mathbf{Z}_{12}^* = \{1, 5, 7, 11\}$.

- 1) There is a unique morphism $\tau : F \rightarrow \mathbf{Z}_p^*$ with kernel of order 6, namely the one sending the generator x of F to -1 . We have $S_0(\tau) = \text{Aut } F$.
- 2) When $p \equiv 1 \pmod{4}$, $\mathbf{Z}_p^*$ has a (unique) subgroup of order 4. Let ζ_4 be a generator of it. We may define two morphisms from F to $\mathbf{Z}_p^*$ with a kernel of order 3, namely

$$\tau_1 : x \mapsto \zeta_4, \quad \tau_2 : x \mapsto \zeta_4^{-1}.$$

We have $S_0(\tau_1) = S_0(\tau_2) = \{1, 5\}$.

- 3) When $p \equiv 1 \pmod{6}$, $\mathbf{Z}_p^*$ has a (unique) subgroup of order 6. Let ζ_6 be a generator of it. We may define two morphisms from F to $\mathbf{Z}_p^*$ with a kernel of order 2, namely

$$\tau_1 : x \mapsto \zeta_6, \quad \tau_2 : x \mapsto \zeta_6^{-1}$$

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

$$\tau_3 : x \mapsto \zeta_6^2, \quad \tau_4 : x \mapsto \zeta_6^{-2}.$$

We have $S_0(\tau_1) = S_0(\tau_2) = S_0(\tau_3) = S_0(\tau_4) = \{1, 7\}$.

- 4) When $p \equiv 1 \pmod{12}$, $\mathbf{Z}_p^*$ has a (unique) subgroup of order 12. Let ζ_{12} be a generator of it. We may define four morphisms from F to $\mathbf{Z}_p^*$ with a trivial kernel, namely

$$\begin{array}{ll} \tau_1 : x \mapsto \zeta_{12}, & \tau_2 : x \mapsto \zeta_{12}^5, \\ \tau_3 : x \mapsto \zeta_{12}^{-5}, & \tau_4 : x \mapsto \zeta_{12}^{-1}. \end{array}$$

We have $S_0(\tau_1) = S_0(\tau_2) = S_0(\tau_3) = S_0(\tau_4) = \{1\}$.

Case $E = C_{12}$

If $E = C_{12}$, we may take $F = \langle (1, 1) \rangle \subset \text{Hol}(E)$, i.e. we have now $x = (1, 1)$. We determine the conjugation relations between the morphisms $\tau : F \rightarrow \mathbf{Z}_p^*$.

- 1) We consider the two morphisms from F to $\mathbf{Z}_p^*$ with a kernel of order 3. We observe that $\tau_2(-1, 1) = \tau_2((1, 1)^{-1}) = \zeta_4$, hence $\tau_1 = \tau_2\Phi_{-1}$ and we obtain then one brace.

- 2) We consider the two morphisms from F to $\mathbf{Z}_p^*$ with a kernel of order 2 and the two with a kernel of order 4. We have $\tau_1 = \tau_2\Phi_{-1}$ and $\tau_3 = \tau_4\Phi_{-1}$ and obtain then two braces.
- 3) We consider the four morphisms from F to $\mathbf{Z}_p^*$ with a trivial kernel. We observe that $(1, 1)^5 = (5, 1), (1, 1)^{-5} = (-5, 1), (1, 1)^{-1} = (-1, 1)$, hence $\tau_1 = \tau_2\Phi_5 = \tau_3\Phi_{-5} = \tau_4\Phi_{-1}$ and obtain then one brace.

We state the obtained result in the following proposition.

Proposition 11. *Let $p \geq 7$ be a prime number. We count the left braces with additive group $\mathbf{Z}_p \times \mathbf{Z}_{12}$ and multiplicative group $\mathbf{Z}_p \rtimes \mathbf{Z}_{12}$.*

- 1) If $p \equiv 11 \pmod{12}$ there are 2 such braces. One of them is a direct product and the second one has a kernel of order 6.
- 2) If $p \equiv 5 \pmod{12}$ there are 3 such braces. Two of them are as in 1) and the third one has a kernel of order 3.
- 3) If $p \equiv 7 \pmod{12}$ there are 4 such braces. Two of them are as in 1) and the other two have kernels of orders 2 and 4, respectively.
- 4) If $p \equiv 1 \pmod{12}$ there are 6 such braces. One of them is a direct product and the other five have kernels of orders 6, 4, 3, 2, 1, respectively.

Case $E = C_6 \times C_2$

For $E = C_6 \times C_2$, we use the notations in Remark 10. We may take $F = \langle (ab, \varphi) \rangle \subset \text{Hol}(E)$, where φ is the order 2 automorphism defined by $\varphi(a) = a, \varphi(b) = a^3b$, i.e. $\varphi = \rho^3\sigma$. We may check that F is indeed a cyclic group of order 12 and a regular subgroup of $\text{Hol}(E)$. We have now $x = (ab, \varphi)$. We determine the conjugation relations between the morphisms $\tau : F \rightarrow \mathbf{Z}_p^*$.

- 1) For the two morphisms from F to $\mathbf{Z}_p^*$ with a kernel of order 3, we observe that $(ab, \varphi)^{-1} = (\varphi(a^{-1}b), \varphi) = (a^2b, \varphi)$, hence $\tau_2(a^2b, \varphi) = \zeta_4$. We have then $\tau_1 = \tau_2\Phi_\sigma$, since $\Phi_\sigma(ab, \rho^3\sigma) = \sigma(ab, \rho^3\sigma)\sigma^{-1} = (\sigma(ab), \sigma(\rho^3\sigma)\sigma) = (a^2b, \rho^3\sigma)$. We obtain then one brace.
- 2) For the two morphisms from F to $\mathbf{Z}_p^*$ with a kernel of order 2 and the two with a kernel of order 4, as in the preceding case, we have $\tau_1 = \tau_2\Phi_\sigma$ and $\tau_3 = \tau_4\Phi_\sigma$ and obtain then two braces.
- 3) For the four morphisms from F to $\mathbf{Z}_p^*$ with a trivial kernel, we observe that $(ab, \varphi)^5 = (a^5b, \varphi), (ab, \varphi)^{-5} = (a^4b, \varphi), (ab, \varphi)^{-1} = (a^2b, \varphi)$, hence $\tau_1 = \tau_2\Phi_{\rho^3} = \tau_3\Phi_{\rho^3\sigma} = \tau_4\Phi_\sigma$ and we obtain then one brace.

We state the obtained result in the following proposition.

Proposition 12. *Let $p \geq 7$ be a prime number. We count the left braces with additive group $\mathbf{Z}_p \times \mathbf{Z}_6 \times \mathbf{Z}_2$ and multiplicative group $\mathbf{Z}_p \rtimes \mathbf{Z}_{12}$.*

- 1) If $p \equiv 11 \pmod{12}$ there are 2 such braces. One of them is a direct product and the second one has a kernel of order 6.
- 2) If $p \equiv 5 \pmod{12}$ there are 3 such braces. Two of them are as in 1) and the third one has a kernel of order 3.
- 3) If $p \equiv 7 \pmod{12}$ there are 4 such braces. Two of them are as in 1) and the other two have kernels of orders 2 and 4, respectively.
- 4) If $p \equiv 1 \pmod{12}$ there are 6 such braces. One of them is a direct product and the other five have kernels of orders 6, 4, 3, 2, 1, respectively.

5.2. $F = C_6 \times C_2$

Let us write $F = \langle x, y \rangle$, with x of order 6, y of order 2. We determine now the possible morphisms $\tau : F \rightarrow \mathbf{Z}_p^*$. To be used in Section 6, we compute $S_0(\tau) = \{g \in \text{Aut } F \mid \tau g = \tau\}$. We use the determination of $\text{Aut } F$ given in Remark 10.

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

$$\begin{array}{lll} \tau_1 : & x \mapsto 1 & \tau_2 : x \mapsto -1 \\ & y \mapsto -1 & y \mapsto -1 \end{array} \quad \tau_3 : \begin{array}{l} x \mapsto -1 \\ y \mapsto 1 \end{array}$$

with kernels $\langle x \rangle, \langle xy \rangle, \langle x^2y \rangle$, respectively. We have $S_0(\tau_1) = \langle \rho^3, \sigma \rangle, S_0(\tau_2) = \langle \rho^3, \rho^2\sigma \rangle, S_0(\tau_3) = \langle \rho^3, \rho\sigma \rangle$.

2) In order to have a morphism τ with $\text{Ker } \tau$ of order 2 or 4, it is necessary that $p \equiv 1 \pmod{6}$. In this case, let ζ_6 be a generator of the unique subgroup of order 6 of $\mathbf{Z}_p^*$. We may define six morphisms from F to $\mathbf{Z}_p^*$ with a kernel of order 2, namely

$$\begin{array}{lll} \tau_1 : & x \mapsto \zeta_6 & \tau_2 : x \mapsto \zeta_6^{-1} \\ & y \mapsto 1 & y \mapsto 1, \end{array} \quad \text{with } \text{Ker } \tau = \langle y \rangle$$

$$\begin{array}{lll} \tau_3 : & x \mapsto \zeta_6^2 & \tau_4 : x \mapsto \zeta_6^{-2} \\ & y \mapsto \zeta_6^3 & y \mapsto \zeta_6^3, \end{array} \quad \text{with } \text{Ker } \tau = \langle x^3 \rangle$$

$$\begin{array}{lll} \tau_5 : & x \mapsto \zeta_6 & \tau_6 : x \mapsto \zeta_6^{-1} \\ & y \mapsto \zeta_6^3 & y \mapsto \zeta_6^3. \end{array} \quad \text{with } \text{Ker } \tau = \langle x^3y \rangle$$

We have $S_0(\tau_1) = S_0(\tau_2) = \langle \rho\sigma \rangle, S_0(\tau_3) = S_0(\tau_4) = \langle \rho^3\sigma \rangle, S_0(\tau_5) = S_0(\tau_6) = \langle \rho^5\sigma \rangle$. We may further define two morphisms from F to $\mathbf{Z}_p^*$ with a kernel of order 4, namely

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

We have $S_0(\tau_1) = S_0(\tau_2) = \langle \rho^2, \rho\sigma \rangle$.

Case $E = C_{12}$

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

$$F = \langle \alpha = (2, 1), \beta = (3, 7) \rangle \subset \text{Hol}(E)$$

following the notation in Remark 10.

The element α has order 6, the element β has order 2, they commute with each other and generate a regular subgroup of order 12. We have now $x = \alpha, y = \beta$. We determine the conjugation relations between the morphisms $\tau : F \rightarrow \mathbf{Z}_p^*$.

1) For the morphisms from F to $\mathbf{Z}_p^*$ with kernel of order 6, we have $\tau_2 = \tau_3\Phi_{-1}$ and τ_1 is not conjugate to the other two, since the second component of α is different from those of $\alpha\beta$ and $\alpha^2\beta$. We obtain then two braces.

- 2) For the morphisms from F to $\mathbf{Z}_p^*$ with a kernel of order 4, we observe that $\tau_2\Phi_{11}(\alpha) = \zeta_3$ and $\tau_2\Phi_{11}(\beta) = 1$, hence $\tau_1 = \tau_2\Phi_{11}$ and we obtain then a unique brace.
- 3) For the morphisms from F to $\mathbf{Z}_p^*$ with a kernel of order 2, we observe that $\tau_2 = \tau_1\Phi_5$, $\tau_5 = \tau_1\Phi_7$, $\tau_6 = \tau_1\Phi_{-1}$ and $\tau_4 = \tau_3\Phi_{-1}$. So we obtain only two braces (determined by τ_1 and τ_3).

We state the obtained result in the following proposition.

Proposition 13. *Let $p \geq 7$ be a prime number. We count the left braces with additive group $\mathbf{Z}_p \times C_{12}$ and multiplicative group $\mathbf{Z}_p \rtimes (C_6 \times C_2)$.*

- 1) If $p \equiv 11 \pmod{12}$ there are 3 such braces. One of them is a direct product and the other two have a kernel of order 6.
- 2) If $p \equiv 7 \pmod{12}$ 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.
- 3) If $p \equiv 5 \pmod{12}$ there are 3 such braces. One of them is a direct product and the other two have a kernel of order 6.
- 4) If $p \equiv 1 \pmod{12}$ there are 6 such braces. One of them is a direct product, two have kernel of order 6, two have kernels of orders 2 and one has kernel of order 4.

Case $E = C_6 \times C_2$

If $E = C_6 \times C_2$, we may take $F = \langle (a, \text{Id}), (b, \text{Id}) \rangle \subset \text{Hol}(E)$, following the notation of Remark 10. We may check that F is indeed a regular subgroup of order 12 of $\text{Hol}(E)$ isomorphic to $C_6 \times C_2$. We have now $x = (a, \text{Id}), y = (b, \text{Id})$. We determine the conjugation relations between the morphisms $\tau : F \rightarrow \mathbf{Z}_p^*$.

- 1) For the morphisms from F to $\mathbf{Z}_p^*$ with kernel of order 6, we have $\tau_1 = \tau_2\Phi_{\rho^4} = \tau_3\Phi_{\rho^5}$. We obtain then one brace.
- 2) For the morphisms from F to $\mathbf{Z}_p^*$ with a kernel of order 4, we observe that $\tau_1 = \tau_2\Phi_{\rho^3}$ and obtain then a unique brace.
- 3) For the morphisms from F to $\mathbf{Z}_p^*$ with a kernel of order 2, we observe that $\tau_6 = \tau_1\Phi_{\rho} = \tau_2\Phi_{\rho^4} = \tau_3\Phi_{\rho^2} = \tau_4\Phi_{\sigma\rho^2} = \tau_5\Phi_{\rho^3}$. So we obtain only one brace.

We state the obtained result in the following proposition.

Proposition 14. *Let $p \geq 7$ be a prime number. We count the left braces with additive group $\mathbf{Z}_p \times (C_6 \times C_2)$ and multiplicative group $\mathbf{Z}_p \rtimes (C_6 \times C_2)$.*

- 1) If $p \equiv 11 \pmod{12}$ there are 2 such braces. One of them is a direct product and the second one has a kernel of order 6.
- 2) If $p \equiv 7 \pmod{12}$ there are 4 such braces. One of them is a direct product, and the other three have kernels of orders 2, 4 and 6, respectively.
- 3) If $p \equiv 5 \pmod{12}$ there are 2 such braces. One of them is a direct product and the second one has a kernel of order 6.
- 4) If $p \equiv 1 \pmod{12}$ there are 4 such braces. One of them is a direct product, and the other three have kernels of orders 2, 4 and 6, respectively.

5.3. $F = A_4$

This case only occurs for $E = C_6 \times C_2$. We use the notation of Remark 10 for the generators of $\text{Hol}(E)$. We have $A_4 = V_4 \rtimes C_3$ and we may take $F = \langle a^3, b, (a^4, \rho^2) \rangle \subset \text{Hol}(E)$, since a^3, b are order 2 elements commuting between them and (a^4, ρ^2) has order 3 and satisfies $(a^4, \rho^2)a^3(a^4, \rho^2)^{-1} = b, (a^4, \rho^2)b(a^4, \rho^2)^{-1} = a^3b$. We may further check that F is a regular subgroup of $\text{Hol}(E)$. Since V_4 is the unique proper nontrivial normal subgroup of A_4 , we have that a nontrivial morphism from F to $\mathbf{Z}_p^*$ has image a cyclic group of order 3. We have then two cases.

- 1) If $p \not\equiv 1 \pmod{3}$, the unique morphism from F to $\mathbf{Z}_p^*$ is the trivial one and there is just one brace with additive group $\mathbf{Z}_p \times \mathbf{Z}_6 \times \mathbf{Z}_2$ and multiplicative group $\mathbf{Z}_p \rtimes A_4$, the one whose multiplicative group is a direct product.
- 2) If $p \equiv 1 \pmod{3}$, let ζ_3 be a generator of the (unique) subgroup of order 3 of $\mathbf{Z}_p^*$. We may define two morphisms from F to $\mathbf{Z}_p^*$, with kernel $\langle a^3, b \rangle$, namely

$$\tau_1 : (a^4, \rho^2) \mapsto \zeta_3, \quad \tau_2 : (a^4, \rho^2) \mapsto \zeta_3^{-1}.$$

We note that $(a^4, \rho^2)^{-1} = (a^2, \rho^4) = \sigma(a^4, \rho^2)\sigma$, hence $\tau_1 = \tau_2\Phi_\sigma$ and we obtain one brace.

We state the obtained result in the following proposition.

Proposition 15. *Let $p \geq 7$ be a prime number. We count the left braces with additive group $\mathbf{Z}_p \times \mathbf{Z}_6 \times \mathbf{Z}_2$ and multiplicative group $\mathbf{Z}_p \rtimes A_4$.*

- 1) *If $p \not\equiv 1 \pmod{3}$ there is just one such brace, which is a direct product.*
- 2) *If $p \equiv 1 \pmod{3}$ there are 2 such braces. One is a direct product and the second one has kernel isomorphic to V_4 .*

To be used in Section 6, we compute $S_0(\tau) = \{g \in \text{Aut } F \mid \tau g = \tau\}$ for the two nontrivial morphisms from F to $\mathbf{Z}_p^*$. We have $\text{Aut } A_4 \simeq S_4$ and the isomorphism is obtained by sending a permutation in S_4 to the corresponding conjugation automorphism. We obtain $S_0(\tau_1) = S_0(\tau_2) = A_4$.

5.4. $F = D_{2,6}$

Let us write $F = \langle r, s \mid r^6 = \text{Id}, s^2 = \text{Id}, srs = r^5 \rangle$. We describe the morphisms $\tau : F \rightarrow \mathbf{Z}_p^*$. To be used in Section 6, we compute $S_0(\tau) = \{g \in \text{Aut } F \mid \tau g = \tau\}$. We have $\text{Aut } D_{2,6} = \langle \rho, \sigma \rangle \simeq D_{2,6}$, where ρ and σ are defined as follows.

$$\begin{array}{ccc} \rho : & r & \mapsto r \\ & s & \mapsto rs \end{array}, \quad \begin{array}{ccc} \sigma : & r & \mapsto r^5 \\ & s & \mapsto s \end{array}.$$

The only nontrivial morphisms from F to $\mathbf{Z}_p^*$ are three morphisms with kernel of order 6, namely

$$\begin{array}{ccc} \tau_1 : & r & \mapsto 1 \\ & s & \mapsto -1 \end{array}, \quad \begin{array}{ccc} \tau_2 : & r & \mapsto -1 \\ & s & \mapsto -1 \end{array}, \quad \begin{array}{ccc} \tau_3 : & r & \mapsto -1 \\ & s & \mapsto 1 \end{array},$$

with kernels $\langle r \rangle, \langle r^2, rs \rangle$ and $\langle r^2, s \rangle$, respectively. We observe that $\text{Ker } \tau_1$ is cyclic, while $\text{Ker } \tau_2$ and $\text{Ker } \tau_3$ are isomorphic to the dihedral group $D_{2,3}$. We have $S_0(\tau_1) = \text{Aut } F, S_0(\tau_2) = S_0(\tau_3) = \langle \rho^2, \sigma \rangle$.

Case $E = C_{12}$

There are two regular subgroups of $\text{Hol}(E)$ isomorphic to $D_{2,6}$, up to conjugacy by $\text{Aut } E$,

$$F_1 = \langle \alpha_1 = (2, 1), \beta_1 = (1, 11) \rangle, \quad F_2 = \langle \alpha_2 = (1, 7), \beta_2 = (3, 11) \rangle.$$

For $i \in \{1, 2\}$, α_i has order 6, β_i has order 2, and $\alpha_i \beta_i \alpha_i = \beta_i$, so $F_i \cong D_{2,6}$. It is checked easily that F_i is regular. We have now $r = \alpha_i, s = \beta_i, i = 1, 2$.

We consider the morphisms from F to $\mathbf{Z}_p^*$ with kernel of order 6. Since $\text{Ker}(\tau_1)$ is cyclic while $\text{Ker } \tau_2$ and $\text{Ker } \tau_3$ are not, τ_1 is not conjugate to the other two morphisms. We denote $\tau_2^{(i)}, \tau_3^{(i)} : F_i \rightarrow \mathbf{Z}_p^*, i = 1, 2$. Since $\Phi_7(\alpha_1) = \alpha_1$ and $\Phi_7(\beta_1) = \alpha_1^3 \beta_1$, we obtain $\tau_2^{(1)} = \tau_3^{(1)} \Phi_7$. For $\tau_2^{(2)}$ and $\tau_3^{(2)}$ to be conjugate, we would need $\Phi_\nu(\beta_2) = \alpha_2^k \beta_2$, with an odd k . Since the second component of β_2 is 11 and the second component of $\alpha_2^k \beta_2$ is 5, for an odd k , there is no such Φ_ν . Hence $\tau_2^{(2)}$ and $\tau_3^{(2)}$ are not conjugate and we obtain five braces, two of which have order 6 cyclic kernel.

Proposition 16. *Let $p \geq 7$ be a prime number. Then there are 7 left braces with additive group $\mathbf{Z}_p \times C_{12}$ and multiplicative group $\mathbf{Z}_p \rtimes D_{2,6}$. Among these, two of them are a direct product, two other have cyclic kernel of order 6 and the other three have kernel isomorphic to $D_{2,3}$.*

Case $E = C_6 \times C_2$

If $E = C_6 \times C_2$, we may take $F = \langle (a, \text{Id}), (b, \rho^3) \rangle \subset \text{Hol}(E)$, which is regular. Indeed, one may check that (a, Id) is of order 6, (b, ρ^3) is of order 2, $(a, \text{Id})(b, \rho^3)(a, \text{Id}) = (b, \rho^3)$ and F has trivial stabilizer. We have now $r = (a, \text{Id}), s = (b, \rho^3)$.

We consider the morphisms from F to $\mathbf{Z}_p^*$ with kernel of order 6. Again, since $\text{Ker}(\tau_1) \cong C_6$ and $\text{Ker}(\tau_i) \cong D_{2,3}, i \in \{2, 3\}$, τ_1 is not conjugate to the other two morphisms. Since $\tau_2 \Phi_\sigma = \tau_3$, we obtain one brace with cyclic kernel and one brace with dihedral kernel.

Proposition 17. *Let $p \geq 7$ be a prime number. Then there are 3 left braces with additive group $\mathbf{Z}_p \times (C_6 \times C_2)$ and multiplicative group $\mathbf{Z}_p \rtimes D_{2,6}$. Among these, one of them is a direct product, one has cyclic kernel of order 6 and the other one has kernel isomorphic to $D_{2,3}$.*

5.5. $F = \text{Dic}_{12}$

The dicyclic group Dic_{12} is a group with 12 elements that can be presented as

$$\text{Dic}_{12} = \langle x, y \mid x^3 = 1, y^4 = 1, yxy^{-1} = x^2 \rangle.$$

We determine now the possible morphisms $\tau : F \rightarrow \mathbf{Z}_p^*$. To be used in Section 6, we compute $S_0(\tau) = \{g \in \text{Aut } F \mid \tau g = \tau\}$. We have $\text{Aut } \text{Dic}_{12} = \langle \rho, \sigma \rangle \simeq D_{2,6}$, where ρ and σ are defined as follows.

$$\begin{array}{ll} \rho : & x \mapsto x \\ & y \mapsto xy^{-1}, \end{array} \quad \begin{array}{ll} \sigma : & x \mapsto x^{-1} \\ & y \mapsto y \end{array}.$$

- 1) There is a unique morphism τ from F to $\mathbf{Z}_p^*$ with kernel of order 6, namely the one sending the generator x to 1 and y to -1 . We have $S_0(\tau) = \text{Aut } F$.
- 2) If $p \equiv 1 \pmod{4}$, let ζ_4 be a generator of the subgroup of order 4 of $\mathbf{Z}_p^*$. We may define two morphisms from F to $\mathbf{Z}_p^*$ with kernel $\langle x \rangle$:

$$\begin{aligned}\tau_1 : x &\mapsto 1 & \tau_2 : x &\mapsto 1 \\ y &\mapsto \zeta_4 & y &\mapsto \zeta_4^{-1}.\end{aligned}$$

We have $S_0(\tau_1) = S_0(\tau_2) = \langle \rho^2, \sigma \rangle$.

Case $E = C_{12}$

We know that in $\text{Hol}(C_{12})$ there exists only a regular subgroup isomorphic to F , up to conjugacy by $\text{Aut } E$. We may take

$$F = \langle x = (4, 1), y = (1, 5) \rangle \subset \text{Hol}(E),$$

following the notation in Remark 10. The element x has order 3, the element y has order 4 and they satisfy the relation $xyx^{-1} = x^2$. We may check that F is a regular subgroup of $\text{Hol}(C_{12})$.

We determine now the conjugation relations between the morphisms $\tau : F \rightarrow \mathbf{Z}_p^*$.

For the morphisms from F to $\mathbf{Z}_p^*$ with kernel $\langle x \rangle$, we observe that $\tau_2 = \tau_1 \Phi_7$, so we obtain, in this case, only one brace.

We state the obtained result in the following proposition.

Proposition 18. *Let $p \geq 7$ be a prime number. We count the left braces with additive group $\mathbf{Z}_p \times C_{12}$ and multiplicative group $\mathbf{Z}_p \rtimes \text{Dic}_{12}$.*

- 1) If $p \not\equiv 1 \pmod{4}$ there are 2 such braces. One of them is a direct product and the other one has a kernel of order 6.
- 2) If $p \equiv 1 \pmod{4}$ there are 3 such braces. One of them is a direct product, and the other two have kernels of order 6 and 3, respectively.

Case $E = C_6 \times C_2$

If $E = C_6 \times C_2$, there is only a conjugacy class (of length 3) of regular subgroups isomorphic to Dic_{12} .

We may take

$$F = \langle x = (a^2, Id), y = (b, \sigma) \rangle \subset \text{Hol}(E),$$

following the notation in Remark 10. The element x has order 3, the element y has order 4 and they satisfy the relation $xyx^{-1} = x^2$. We may check that F is a regular subgroup of $\text{Hol}(C_6 \times C_2)$.

We determine now the conjugation relations between the morphisms $\tau : F \rightarrow \mathbf{Z}_p^*$.

For the morphisms τ with a kernel of order 3, we observe that $\tau_2 = \tau_1 \Phi_\sigma$, so we obtain, in this case, only one brace.

We state the obtained result in the following proposition.

Proposition 19. *Let $p \geq 7$ be a prime number. We count the left braces with additive group $\mathbf{Z}_p \times (C_6 \times C_2)$ and multiplicative group $\mathbf{Z}_p \rtimes \text{Dic}_{12}$.*

- 1) If $p \not\equiv 1 \pmod{4}$ there are 2 such braces. One of them is a direct product and the other one has a kernel of order 6.
- 2) If $p \equiv 1 \pmod{4}$ there are 3 such braces. One of them is a direct product, and the other two have kernels of order 6 and 3, respectively.

5.6. Total numbers

For a prime number $p \geq 7$ we compile in the following tables the total number of left braces of size $12p$.

The additive group is $\mathbf{Z}_p \times E$ and the multiplicative group is a semidirect product $\mathbf{Z}_p \rtimes F$. In the first column we have the possible E 's and in the first row the possible F 's.

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

	C_{12}	$C_6 \times C_2$	A_4	$D_{2,6}$	Dic_{12}	
C_{12}	2	3	0	7	2	
$C_6 \times C_2$	2	2	1	3	2	
	4	5	1	10	4	24

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

	C_{12}	$C_6 \times C_2$	A_4	$D_{2,6}$	Dic_{12}	
C_{12}	3	3	0	7	3	
$C_6 \times C_2$	3	2	1	3	3	
	6	5	1	10	6	28

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

	C_{12}	$C_6 \times C_2$	A_4	$D_{2,6}$	Dic_{12}	
C_{12}	4	6	0	7	2	
$C_6 \times C_2$	4	4	2	3	2	
	8	10	2	10	4	34

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

	C_{12}	$C_6 \times C_2$	A_4	$D_{2,6}$	Dic_{12}	
C_{12}	6	6	0	7	3	
$C_6 \times C_2$	6	4	2	3	3	
	12	10	2	10	6	40

With the results summarized in the above tables, the validity of conjecture (1) is then established.

6. Hopf Galois structures on a Galois field extension of degree $12p$

Let E, F be groups of order 12 with E abelian. By computation with Magma, we obtain that the number of regular subgroups of $\text{Hol}(E)$ isomorphic to F is as shown in the following table.

$E \backslash F$	C_{12}	$C_6 \times C_2$	A_4	$D_{2,6}$	Dic_{12}
C_{12}	1	1	0	3	1
$C_6 \times C_2$	3	1	2	3	3

More precisely, for the groups F_1, F_2 defined in the case $F = D_{2,6}, E = C_{12}$, we obtain that F_1 is normal in $\text{Hol}(E)$ while the length of the conjugation class of F_2 in $\text{Hol}(E)$ is 2 and $F'_2 = \langle (7, 7), (9, 11) \rangle$ is the second subgroup in this class.

For $E = C_{12}$ or $C_6 \times C_2$, F a regular subgroup of $\text{Hol}(E)$, $N = \mathbf{Z}_p \times E$ and $\tau : F \rightarrow \mathbf{Z}_p^*$ a group morphism, Corollary 5 gives the length of the conjugacy class of the regular subgroup G of $\text{Hol}(N)$ corresponding to (F, τ) . For a fixed regular subgroup G of $\text{Hol}(N)$, we want to determine the number of regular subgroups of $\text{Hol}(N)$ isomorphic to G . This number is the sum of the lengths of the conjugacy classes corresponding to pairs (F, τ) such that $\mathbf{Z}_p \rtimes_\tau F \simeq G$. Then, we only need to consider the number of morphisms τ from F to $\mathbf{Z}_p^*$ such that $\mathbf{Z}_p \rtimes_\tau F \simeq G$, without taking into account their distribution into classes. For example, in the case $F = D_{2,6}$, $E = C_{12}$, $|\text{Ker } \tau| = 6$, we only need to consider the morphisms τ_1, τ_2, τ_3 and not the fact that their distribution into classes is different for F_1 and F_2 . We obtain the term $b(N, G)$ in Byott's formula (Proposition 1), for $N = \mathbf{Z}_p \times E$, $G = \mathbf{Z}_p \rtimes_\tau F$, as the product of the number of regular subgroups of $\text{Hol}(E)$ isomorphic to F times the number of morphisms $\tau' : F \rightarrow \mathbf{Z}_p^*$ such that $\mathbf{Z}_p \rtimes_{\tau'} F \simeq G$. Applying Corollary 7 and the determination of S_0 given in Section 5, we obtain the number of Hopf Galois structures of abelian type on a Galois field extension of degree $12p$.

The number of Hopf Galois structures of abelian type on a Galois extension with Galois group $G = \mathbf{Z}_p \rtimes_\tau F$ is as given in the following tables. The first column gives the group F and the first row the kernel of the morphism $\tau : F \rightarrow \mathbf{Z}_p^*$ defining the semidirect product. In each case, we assume that the value of p is such that a morphism $\tau : F \rightarrow \mathbf{Z}_p^*$ exists with the given kernel.

Hopf Galois structures of type C_{12p}

$F \setminus \text{Ker } \tau$	F	C_6	$D_{2,3}$	C_4	C_2^2	C_3	C_2	$\{1\}$
C_{12}	1	p	-	p	-	p	p	p
$C_6 \times C_2$	3	$3p$	-	-	$3p$	-	$3p$	-
A_4	0	-	-	-	0	-	-	-
$D_{2,6}$	9	$9p$	$9p$	-	-	-	-	-
Dic_{12}	3	$3p$	-	-	-	$3p$	-	-

Hopf Galois structures of type $C_{6p} \times C_2$

$F \setminus \text{Ker } \tau$	F	C_6	$D_{2,3}$	C_4	C_2^2	C_3	C_2	$\{1\}$
C_{12}	1	p	-	p	-	p	p	p
$C_6 \times C_2$	1	p	-	-	p	-	p	-
A_4	4	-	-	-	$4p$	-	-	-
$D_{2,6}$	3	$3p$	$3p$	-	-	-	-	-
Dic_{12}	3	$3p$	-	-	-	$3p$	-	-

Acknowledgements

We thank the referee for his/her corrections and remarks which helped improving the quality of the paper.

References

- [1] E. Acri, M. Bonatto, Skew braces of size pq , *Commun. Algebra* 48 (5) (2020) 1872–2881.
- [2] D. Bachiller, Classification of braces of order p^3 , *J. Pure Appl. Algebra* 219 (2015) 3568–3603.
- [3] D. Bachiller, Counterexample to a conjecture about braces, *J. Algebra* 453 (2016) 160–176.
- [4] N. Byott, Uniqueness of Hopf Galois structure for separable field extensions, *Commun. Algebra* 24 (10) (1996) 3217–7228.
- [5] V.G. Bardakov, M.V. Neshchadim, M.K. Yadav, Computing skew left braces of small orders, *Int. J. Algebra Comput.* 30 (4) (2020) 839–951.
- [6] S.U. Chase, M. Sweedler, *Hopf Algebras and Galois Theory*, LNM, vol. 97, Springer-Verlag, Berlin, 1969.
- [7] T. Crespo, D. Gil-Muñoz, A. Río, M. Vela, Left braces of size $8p$, *J. Algebra* 617 (2023) 317–339.
- [8] T. Crespo, A. Río, M. Vela, Induced Hopf Galois structures, *J. Algebra* 457 (2016) 312–322.

- [9] C. Dietzel, Braces of order p^2q , *J. Algebra Appl.* 20 (8) (2021) 2150140.
- [10] C. Greither, B. Pareigis, Hopf Galois theory for separable field extensions, *J. Algebra* 106 (1987) 239–258.
- [11] W. Rump, Braces, radical rings, and the quantum Yang–Baxter equation, *J. Algebra* 307 (2007) 153–170.
- [12] T. Kohl, Regular permutation groups of order mp and Hopf Galois structures, *Algebra Number Theory* 7 (9) (2013) 2203–2240.
- [13] T. Kohl, Hopf–Galois structures arising from groups with unique subgroup of order p , *Algebra Number Theory* 10 (1) (2016) 37–59.
- [14] L. Vendramin, Problems on Skew Left Braces, *Advances in Group Theory and Applications*, vol. 7, 2019, pp. 15–57.