New York Journal of Mathematics

New York J. Math. **25** (2019) 574–588.

Bi-skew braces and Hopf Galois structures

Lindsay N. Childs

Abstract. A skew brace G is a set with two group operations, one defining a (not necessarily abelian) "additive group" on G and the other a "circle group" on G, so that G with the two operations satisfies a relation analogous to distributivity. If G is a skew brace, then G yields a Hopf Galois structure of type equal to the additive group of G on any Galois extension of fields with Galois group isomorphic to the circle group of G. A skew brace G is a bi-skew brace if it is also a skew brace with the roles of the circle and additive group reversed. In that event, then G also corresponds to a Hopf Galois structure of type equal to the circle group on a Galois extension of fields with Galois group isomorphic to the additive group. Many non-trivial examples exist. One source is radical rings A with $A^3 = 0$, where one of the groups is abelian and the other need not be. We find that the left braces of degree p^3 classified by Bachiller are bi-skew braces if and only they are radical rings. A different source of bi-skew braces is semidirect products of arbitrary finite groups, which yield many examples where both groups are non-abelian, and a skew brace proof of a result of Crespo, Rio and Vela that if G is a semidirect product of two finite groups H and J, then any Galois extension of fields with Galois group G has a Hopf Galois structure of type equal to the direct product of H and J.

Contents

Received April 2, 2019.

2010 *Mathematics Subject Classification.* 12F10, 16T05.

Key words and phrases. skew brace, Hopf Galois extension, Galois extension of fields, semidirect product, radical algebra.

ISSN 1076-9803/2019

1. Introduction, history

1.1. Hopf Galois structures. Let L/K be a G-Galois extension of fields: that is, a Galois extension of fields with Galois group $G = (G, \circ)$. By E. Artin's classic treatment of Galois theory we know that

$$L \otimes L \cong Hom_L(LG, L) = (LG)^*.$$

Chase and Sweedler [8] generalized the concept of Galois extension by replacing the group ring of the Galois group by a Hopf algebra, as follows: suppose L is an H-module algebra for H a cocommutative K-Hopf algebra H. Then L/K is an H-Hopf Galois extension L/K if

$$L \otimes_K L \cong \mathrm{Hom}_L(L \otimes_K H, L) = (L \otimes H)^*.$$

Then, as Greither and Pareigis [14] observed, $L \otimes_K L$ is a ring direct sum of copies of L, so $L \otimes H = LN$ for some subgroup N of $\mathrm{Perm}(G)$ that is normalized by the image $\lambda_\circ(G)$ of the left regular representation $\lambda_\circ : G \to \mathrm{Perm}(G)$, and H can be recovered by Galois descent: $H = LN^G$.

If L/K is a Galois extension with Galois group G and is an H-Hopf Galois extension where $L \otimes_K H = KN$, then we say that the type of H is the isomorphism type of the group N.

Since N is a regular subgroup of $\mathrm{Perm}(G)$, the map $\varphi : N \to G$ given by $n \mapsto n(e)$ is a bijection, where e is the identity element of G. Let $g = \varphi(n)$. For x in G, define $\lambda_\star : G \to \mathrm{Perm}(G)$ by

$$\lambda_\star(g)(x) = g \star x = \varphi(n) \star x = n(x).$$

Then $\star$ is a new group operation on G so that $\varphi : N \to \lambda_\star(G)$ is an isomorphism, and $\lambda_\star$ is the left regular representation map for this new operation.

Thus:

Theorem 1.1. *Every Hopf Galois structure of type N on a $G = (G, \circ)$-Galois extension yields a second operation $\star$ on G so that $(G, \star) \cong N$. Then $\lambda_\circ(G)$ is contained in* $\mathrm{Hol}(G, \star)$*, the normalizer in* $\mathrm{Perm}(G)$ *of $\lambda_\star(G)$.*

If a G-Galois extension has a Hopf Galois structure of type N, we'll say that the ordered pair (G, N) of abstract groups (of equal order) is realizable.

There has been much interest since the mid '90s around the qualitative question of realizability, and if so, the quantitative question of counting the number of Hopf Galois structures of type N on a G-Galois extension.

1.2. Skew left braces.

Definition 1. A skew left brace (or for short, skew brace) is a finite set B with two operations, $\star$ and $\circ$, so that $(B, \star)$ is a group (the "additive group"), $(B, \circ)$ is a group, and the compatibility condition

$$a \circ (b \star c) = (a \circ b) \star a^{-1} \star (a \circ c)$$

holds for all a, b, c in B. Here a^{-1} is the inverse of a in $(B, \star)$. Denote the inverse of a in $(B, \circ)$ by $\overline{a}$. A left brace is a skew left brace with abelian additive group.

If B has two operations $\star$ and $\circ$ and is a skew brace with $(B, \star)$ the additive group, then we write $B = B(\circ, \star)$ (i. e. the additive group operation is on the right).

Skew braces were introduced in [15] as a non-commutative generalization of left braces of [18], which in turn generalize radical algebras. Skew braces have been studied in [4] and in [19]. Initial interest in braces and skew braces was motivated by the search for set-theoretic solutions of the Yang-Baxter equation. But there is also a close connection between skew braces and Hopf Galois structures on Galois extensions of fields. This connection evolved from the discovery by [7] of the relationship between radical algebras and regular subgroups of the affine group, and its subsequent generalization and application to abelian Hopf Galois structures on elementary abelian Galois extensions of fields in [13]. Bachiller in [3] observed that the connection in [13] extends to a close relationship between abelian Hopf Galois structures on Galois extensions of fields and left braces. That relationship was extended to skew braces and arbitrary Hopf Galois structures in the appendix by Byott and Vendramin in [19], and has already been used to study Hopf Galois structures, for example in [17] and [10].

Associated to a set B with two group operations $\circ$ and $\star$ are the two left regular representation maps:

$$\begin{aligned}\lambda_\star : &B \to \mathrm{Perm}(B), \lambda_\star(b)(x) = b \star x,\\ \lambda_\circ : &B \to \mathrm{Perm}(B), \lambda_\circ(b)(x) = b \circ x.\end{aligned}$$

Let $\mathcal{L} : B \to \mathrm{Perm}(B)$ by $\mathcal{L}_b(x) = \lambda_\star(b)^{-1}\lambda_\circ(b)(x)$. for b, x in B. Then Proposition 1.9 of [15] is

Proposition 1.2. $(B, \circ, \star)$ *is a skew brace if and only if the group homomorphism* $\lambda_\circ : (B, \circ) \to \mathrm{Perm}(B)$ *has image in* $\mathrm{Hol}(B, \star) = \lambda_\star(B)\mathrm{Aut}(B) \subset \mathrm{Perm}(B)$.

Proof. For all b, x, y in B, the left skew brace property:

$$b \circ (x \star y) = (b \circ x) \star b^{-1} \star (b \circ y)$$

holds iff

$$b^{-1} \star (b \circ (x \star y)) = (b^{-1} \star (b \circ x)) \star (b^{-1} \star (b \circ y)),$$

iff

$$\lambda_\star^{-1}(b)\lambda_\circ(g)(x \star y) = (\lambda_\star^{-1}(b)\lambda_\circ(b)(x)) \star (\lambda_\star^{-1}(b)\lambda_\circ(b)(y))$$

iff

$$\mathcal{L}_b(x \star y) = \mathcal{L}_b(x) * \mathcal{L}_b(y)$$

iff $\mathcal{L}_b$ is in $\mathrm{Aut}(B, \star)$ for all b in B,
iff $\lambda_\circ = \lambda_\star\mathcal{L} : B \to \mathrm{Perm}(B)$ has image in $\lambda_\star(B)\mathrm{Aut}(B) = \mathrm{Hol}(B)$. □

For $(G, \circ, \star)$ a skew left brace, the map

$$\mathcal{L} : (G, \circ) \to \mathrm{Aut}(G, \star)$$

defined by $g \mapsto \mathcal{L}_g$ is a group homomorphism: see Corollary 1.10 of [15].

In the brace literature the map $\mathcal{L}_g$ is often denoted by λ_g. Here we reserve λ for left regular representation maps.

2. Connecting skew braces with Hopf Galois structures

Let L/K be a Galois extension with Galois group $G = (G, \circ)$. Hopf Galois structures on L/K of a given type $(G, \star)$ correspond by Galois descent [14] to regular subgroups N of $\mathrm{Perm}(G)$ isomorphic to $(G, \star)$ and normalized by $\lambda_\circ G$.

Proposition 2.1. *Let L/K be a Galois extension with group $G = (G, \circ)$. Let H be a K-Hopf algebra giving a Hopf Galois structure of type M on L/K. Then $(G, \circ)$ has a skew left brace structure with additive group $(G, \star) \cong M$.*

This follows from Theorem 1.1 by the characterization of skew left braces in Proposition 1.2.

Conversely,

Proposition 2.2. *Let $(G, \circ, \star)$ be a skew brace. Let L/K be a Galois extension with Galois group $(G, \circ)$. Then L/K has a Hopf Galois structure of type $(G, \star)$.*

Proof. Given the skew brace structure $(G, \circ, \star)$ on the Galois group $(G, \circ)$ of L/K, we have by Proposition 1.2 that $\lambda_\circ(G)$ is contained in $\mathrm{Hol}(G, \star)$, and so the subgroup $N = \lambda_\star(G) \subset \mathrm{Perm}(G)$ is normalized by $\lambda_\circ(G)$. Thus N corresponds by Galois descent to a Hopf Galois structure on L/K of type $(G, \star)$. □

But the correspondence between regular subgroups N of $\mathrm{Perm}(\Gamma)$ isomorphic to $(G, \star)$ and isomorphism types of skew braces $(G, \circ, \star)$ with $(G, \circ) \cong \Gamma$ and $(G, \star) \cong N$ is not bijective. We have (c. f. Corollary 2.4 of [17]):

Proposition 2.3 (Byott, Zenouz)**.** *Given an isomorphism type $(B, \circ, \star)$ of skew left brace, the number of Hopf Galois structures on a Galois extension L/K with Galois group isomorphic to $(B, \circ)$ and skew brace isomorphic to $(B, \circ, \star)$ is*

$$\mathrm{Aut}(B, \circ)/\mathrm{Aut}_{sb}(B, \circ, \star).$$

Here $\mathrm{Aut}_{sb}(B, \circ, \star)$ is the group of skew brace automorphisms of $(B, \circ, \star)$, that is, maps from B to B that are simultaneously group automorphisms of $(B, \star)$ and of $(B, \circ)$.

As noted earlier, there has been considerable interest among researchers in Hopf Galois theory on the questions, given a G-Galois extension of fields, what are the possible types of Hopf Galois structures on the extension, or, given a group N, for which G is there a G-Galois extension of fields with a Hopf Galois structure of type N? Concisely, which pairs (G, N) are realizable? There has also been considerable interest among researchers on braces and, more recently, skew braces, on the question, which pairs (G, N) of finite groups can be the additive, resp. circle group of a skew brace? The two question are the same. As an indication of interest in the brace question, we note that at least a dozen of the 50 problems on skew braces in Vendramin's recent manuscript, "Problems on skew left braces" [21] relate to that question.

3. Bi-skew braces

A bi-skew brace is a finite set B with two operations in which either operation can define the additive group. More precisely,

Definition 2. A bi-skew brace is a finite set B with two operations, $\star$ and $\circ$ so that $(B, \star)$ is a group, $(B, \circ)$ is a group, and the two compatibility conditions

$$a \circ (b \star c) = (a \circ b) \star a^{-1} \star (a \circ c)$$

and

$$a \star (b \circ c) = (a \star b) \circ \overline{a} \circ (a \star c)$$

hold for all a, b, c in B.

Thus B with the two operations is a skew left brace with either group acting as the additive group.

Example 3.1. A trivial example: A group G with operation $\star$ is a bi-skew brace with $\circ = \star$.

Almost as trivial: A group G with operation $\star$ is a bi-skew brace with $\circ$ defined by $g \circ h = h * g$. (See Example 1.5 of [19].)

We'll see many more examples below.

Given a skew brace B with circle group isomorphic to Γ and additive group isomorphic to G, the pair (Γ, G) is realizable. If B is a bi-skew brace, then the pair (G, Γ) is also realizable.

More generally we have the following quantitative result, an immediate consequence of Proposition 2.3.

Proposition 3.2. *Let $(B, \circ, \star)$ be a bi-skew brace with $(B, \circ) \cong \Gamma$ and $(B, \star) \cong G$. Let $e_B(\Gamma, [G])$ be the set of Hopf Galois structures of type G on a Galois extension L/K with Galois group Γ where the Hopf Galois structures come from B,and let $e_B(G, [\Gamma])$ be the set of Hopf Galois structures of type Γ on a Galois extension L'/K' with Galois group G where the Hopf Galois structures come from B. Then*

$$e_B(\Gamma, [G]) \cdot |\mathrm{Aut}(G)| = e_B(G, [\Gamma]) \cdot |\mathrm{Aut}(\Gamma)|.$$

Proof. Let B be a skew brace with additive group $\cong G$ and circle group $\cong \Gamma$. Then by Proposition 2.3,

$$e_B(\Gamma, [G]) = \frac{|\mathrm{Aut}(\Gamma)|}{|\mathrm{Aut}_{sb}(B)|}.$$

For a bi-skew brace B, the group of skew brace automorphisms of $(B, \circ, \star)$ is identical to the group of skew brace automorphisms of $(B, \star, \circ)$. The result follows immediately. □

4. Bi-skew braces from radical algebras

Here is a collection of non-trivial examples of bi-skew braces.

Proposition 4.1. *Let $(A, +, \cdot)$ be a nilpotent $\mathbb{F}_p$-algebra of $\mathbb{F}_p$-dimension n. Define the circle operation on A by*

$$a \circ b = a + b + a \cdot b.$$

Then the skew brace $(A, \circ, +)$ is a bi-skew brace if and only if $A^3 = 0$ (i. e. for every a, b, c in A, $a \cdot b \cdot c = 0$).

Proof. As observed in [18], every nilpotent $\mathbb{F}_p$-algebra yields a left brace $(A, \circ, +)$, because $(A, \circ)$ is a group (the inverse of a is $-a + a^2 - a^3 + \ldots$), and for all a, b, c in A,

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

To consider the possibility that $(A, +, \circ,)$ is also a skew brace we first observe that in A,

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

Now consider the skew brace condition (*):

$$a + (b \circ c) = (a + b) \circ \overline{a} \circ (a + c),$$

where $\overline{a}$ is the $\circ$-inverse of a. If this holds for all a, b, c, then it holds modulo the ideal A^4.

The left side of (*) is

$$a + b + c + b \cdot c.$$

The right side of (*) is

$$\begin{aligned}&(a + b) + \overline{a} + (a + c)\\ &+ (a + b) \cdot \overline{a} + (a + b) \cdot (a + c) + \overline{a} \cdot (a + c)\\ &+ (a + b) \cdot \overline{a} \cdot (a + c).\end{aligned}$$

Modulo A^4, $\overline{a} = -a + a^2 - a^3$ (where $a^n = a \cdot a \cdot \ldots \cdot a$ (n factors). Viewing the right side modulo A^4, we obtain

$$\begin{aligned}&(a + b) + (-a + a^2 - a^3) + (a + c)\\ &+ (a + b) \cdot (-a + a^2) + (a + b) \cdot (a + c) + (-a + a^2) \cdot (a + c)\\ &+ (a + b) \cdot (-a) \cdot (a + c).\end{aligned}$$

In the algebra $(A, +, \cdot)$ this last expression reduces to

$$a + b + c + b \cdot c + b \cdot a \cdot c.$$

Thus, if $A^3 = 0$, then $b \cdot a \cdot c = 0$ and (*) holds for all a, b, c in A. On the other hand, if $A^3 \neq 0$, then there exist a, b, c so that $b \cdot a \cdot c \neq 0$ in A, hence in A/A^4. So the skew brace condition (*) fails in A. □

To get a sense of how many examples there are, we note Theorem 2.2 of [16]:

Theorem 4.2. *(Kruse-Price) The number of isomorphism classes of $\mathbb{F}_p$-algebras A of dimension n with $A^3 = 0$ is p^α where $\alpha = \frac{4}{27}n^3 + O(n^2)$.*

In [12], de Graaf determines all isomorphism types of radical algebras A of dimension ≤ 4 over a finite field. Some of the algebras A are noncommutative and have $A^3 = 0$. Here is a dimension 3 example.

Example 4.3. Let $A = A^0_{3,4}$ be the three-dimensional $\mathbb{F}_p$-algebra of de Graaf. Then

$$A^0_{3,4} = \langle a, b, c | a^2 = c, ab = c \rangle$$

(so all other products of two of a, b, c are zero). Note that $A^3 = 0$.

Let $x = c, y = b, z = a - b$, then the multiplication of the basis elements x, y, z is given by $zy = x$ and all other products are zero.

Mapping A to $\mathbb{F}_p^3$ by sending x, y, z to the standard basis vectors in $\mathbb{F}_p^3$ and defining $\overline{u} \circ \overline{v} = \overline{u} + \overline{v} + \overline{u} \cdot \overline{v}$ in A as usual, we find that

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 + z_1 y_2 \\ y_1 + y_2 \\ z_1 + z_2 \end{pmatrix}.$$

This is the circle operation for the second brace with additive group $(\mathbb{Z}/(p))^3$ and socle of order p^2 of Theorem 3.2 of Bachiller's classification of left braces in [2]. The circle group $(A, \circ)$ is isomorphic to the Heisenberg group, the unique non-abelian group of order p^3 and exponent p.

Since $A^3 = 0$, this brace is a bi-skew brace: $(A, +, \circ)$ is a skew brace with additive group $(A, \circ)$ isomorphic to the Heisenberg group.

5. Bachiller's classification of left braces of order p^3

A left brace $(B, +, \circ)$ is two-sided if

$$(a + b) \circ c = (a \circ c) - c + (b \circ c)$$

for all a, b, c in B. If we define a multiplication $x \cdot y$ by

$$x \circ y = x + y + x \cdot y,$$

then the formula above is equivalent to right distributivity in $(B, +, \cdot)$. Rump [18] showed that a brace is two-sided if and only if $(B, +, \cdot)$ is a radical ring.

Bachiller [2] classified the left braces $B = (B, \circ, +)$ of order p^3. In this section we show that the left braces classified by Bachiller that are bi-skew braces are exactly the braces that are two-sided, hence that are radical rings.

The additive group $(B, +)$ of a left brace of order p^3 must be isomorphic to $\mathbb{Z}/(p^3), \mathbb{Z}/(p) \times \mathbb{Z}/(p^2)$ or $(\mathbb{Z}/(p))^3$. We divide the examination into three cases.

Case 1. $(B, +) = (\mathbb{Z}/(p))^3$. For $p > 3$ there are eight forms of isomorphism types of left braces $(B, +, \cdot)$, some with parameters. For such a brace, write

$$(B, +) = \{\mathbf{u} = \begin{pmatrix} x \\ y \\ z \end{pmatrix} : x, y, z \in \mathbb{Z}_(p)\}.$$

Then the circle operation in every case has the form

$$\mathbf{u}_1 \circ \mathbf{u}_2 = \mathbf{u}_1 + \mathbf{u}_2 + \begin{pmatrix} f \\ g \\ h \end{pmatrix}$$

where

$$\begin{aligned} f &= \mathbf{u}_1^T M_f \mathbf{u}_2 + q_f(\mathbf{u}_1, \mathbf{u}_2) \\ g &= \mathbf{u}_1^T M_g \mathbf{u}_2 + q_g(\mathbf{u}_1, \mathbf{u}_2) \\ h &= \mathbf{u}_1^T M_h \mathbf{u}_2 + q_h(\mathbf{u}_1, \mathbf{u}_2) \end{aligned}$$

where M_f, M_g, M_h are in $M_3(\mathbb{Z}/(p^3))$ and q_f, q_g, q_h are quadratic functions of the components of $\mathbf{u}_1$.

Case 2. $(B, +) = \mathbb{Z}/(p) \times \mathbb{Z}/(p^2)$. For $p > 3$ there are fifteen forms of isomorphism types of left braces $(B, +, \cdot)$, some involving integer parameters. For such a brace, write

$$(B, +) = \{\mathbf{u} = \begin{pmatrix} x \\ y \end{pmatrix} : x \in \mathbb{Z}/(p), y \in \mathbb{Z}/(p^2)\}.$$

Then the circle operation in every case has the form

$$\begin{aligned} \mathbf{u}_1 \circ \mathbf{u}_2 &= \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} + \begin{pmatrix} f(\mathbf{u}_1, \mathbf{u}_2) \\ pg(\mathbf{u}_1, \mathbf{u}_2) \end{pmatrix} \end{aligned}$$

where both $f(\mathbf{u}_1, \mathbf{u}_2)$ and $g(\mathbf{u}_1, \mathbf{u}_2)$ have the form

$$(x_1, y_1) M \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} + q(\mathbf{u}_1, \mathbf{u}_2)$$

where M is in $M_2(\mathbb{Z}/(p))$ and $q(\mathbf{u}_1, \mathbf{u}_2)$ is a quadratic function of the components of $\mathbf{u}_1$.

Case 3. $(B, +) = \mathbb{Z}/(p^3) = \{\mathbf{u} = (x) | x \in \mathbb{Z}/(p^3)\}$. Then B is a radical algebra with multiplication $(x_1) \cdot (x_2) = (p^r x_1 x_2)$, and

$$\mathbf{u_1} \circ \mathbf{u_2} = (x_1) \circ (x_2) = (x_1 + x_2 + p^r x_1 x_2)$$

for $r = 0, 1, 2$. If $r = 1$, then

$$(x_1) \circ (x_2) \circ (x_3) = (x_1 + x_2 + x_3 + p^2 x_1 x_2 x_3),$$

so $B^3 \neq 0$. In the cases $r = 0, 2$, $B^3 = 0$, so $(B, \circ, +)$ is also a skew brace.

We have

Proposition 5.1. *For $p > 3$, in Cases 1 and 2, a left brace $B = (B, \circ, +)$ of order p^3 as classified in* [2] *is a radical algebra if and only if the quadratic functions q_f, q_g, resp. q_f, q_g, q_h are zero.*

Proof. To see if a given left brace in Bachiller's classification is a radical ring, it suffices to check right distributivity, where the multiplication $\cdot$ in $(B, \circ, +)$ is defined by

$$\mathbf{u}_1 \circ \mathbf{u}_2 = \mathbf{u}_1 + \mathbf{u}_2 + \mathbf{u}_1 \cdot \mathbf{u}_2.$$

One sees routinely that for each case, right distributivity holds if and only if the functions that are quadratic in the components of $\mathbf{u}_1$ are zero. □

One can see easily that each radical ring $(B, +, \cdot)$ in Cases 1 and 2 has $B^3 = 0$. Hence,

Corollary 5.2. *With one exception, every left brace $(B, \circ, +)$ of order p^3 where $(B, +, \cdot)$ is a radical ring yields a bi-skew brace.*

The exception is the brace with additive group $\mathbb{Z}/(p^3)$ and circle operation $x \circ y = pxy$.

Of the 26 isomorphism forms of left braces of order p^3 found by Bachiller, two forms have $(B, +) \cong \mathbb{Z}/(p^3)$ and are bi-skew braces with $(B, \circ) \cong \mathbb{Z}/(p^3)$, seven forms have $(B, +) \cong \mathbb{Z}/(p) \times \mathbb{Z}/(p^2)$, $(B, \circ) \cong M_3(p)$ and are bi-skew braces, and four forms have $(B, +) \cong \mathbb{Z}/(p^3)$, $(B, \circ) \cong M_{(p)}$ and are bi-skew braces. Here $M_3(p)$ is the unique non-abelian group of order p^3 and exponent p^2, while $M_{(p)}$ is the Heisenberg group, of order p^3 and exponent p.

Remark 5.3. For each of the four bi-skew braces $A = (A, \circ, +)$ arising from a non-commutative radical algebra A with $A^3 = 0$, $(A, +) = C_p^3$ and $(A, \circ) = M_{(p)}$, the Heisenberg group of order p^3, Proposition 2.3 yields the quantitative formula

$$e_A(C_p^3, [M_{(p)}]) \cdot |\mathrm{Aut}(M_{(p)})| = e_A(M_{(p)}, [C_p^3]) \cdot |\mathrm{Aut}(C_p^3)|.$$

Now $|\mathrm{Aut}(C_p^3)| = (p^3 - 1)(p^2 - 1)(p - 1)$ and $|\mathrm{Aut}(M_{(p)})| = |C_p^3||GL_2(\mathbb{F}_p)| = p^3 \cdot (p^2 - 1)(p - 1)$, so

$$e_A(M_{(p)}, [C_p^3]) = (p^3 - 1) e_A(M_{(p)}, [C_p^3]).$$

In words, given Galois extensions K/k with Galois group $\Gamma \cong C_p^3$ and K'/k' with Galois group $G \cong M_{(p)}$, for each Hopf Galois structure of type C_p^3 arising from the bi-skew brace A on K'/k', there are $p^3 - 1$ Hopf Galois structures of type $M_{(p)}$ arising from A on K/k.

The numbers $e_B(C_p^3, [M_{(p)}])$ for skew braces B with additive group $M_{(p)}$ and circle group C_p^3 may be found in Section 4 of [17].

6. On Bachiller's exponent result

Let p be prime and $B = (B, \circ, +)$ be a brace of order p^n. Then $(B, +)$ is an abelian p-group, hence of the form

$$(B, +) = \mathbb{Z}_{p^{a_1}} \times \mathbb{Z}_{p^{a_2}} \times \ldots \times \mathbb{Z}_{p^{a_m}}$$

with $a_1 \leq a_2 \leq \ldots \leq a_m$. Generalizing [13] for $(B, +)$ a radical ring, Bachiller [3] proved that if $m + 2 \leq p$, then for every b in B, the order of b in $(B, \circ)$ is equal to the order of b in $(B, +)$. In particular, if $\circ$ is commutative, then $(B, \circ) \cong (B, +)$. This result is illustrated with the examples in the last section.

The limitation on m and p is necessary: see [9], which constructs examples equivalent to left braces $(B, \circ, \star)$ where $(B, \star) \cong \mathbb{Z}_p^m$ and $(B, \circ)$ is the group of principal units of $\mathbb{F}_p[x]/(x^{m+1})$ and has exponent p^e where $p^{e-1} \leq m < p^e$.

Given an $\mathbb{F}_p$-algebra A with $(A, +)$ of order p^n, $(A, +)$ has exponent p, so if $n + 2 \leq p$, then $(A, \circ)$ has exponent p. Thus for large p, the possible isomorphism types of Galois groups G of order p^n that have Hopf Galois structures arising from identifying G as the circle group of an $\mathbb{F}_p$-algebra are among those groups of order p^n and exponent p. There is some fairly recent literature counting the groups of order p^n for $p > n + 2$ and $n \leq 7$. This literature is reviewed in [20], a paper in which Vaughan-Lee gives an explicit polynomial of degree 4 in p,

$$p^4 + 2p^3 + 147p^2 + (3p + 29)gcd(p - 1, 3) + 5gcd(p - 1, 4) + 1246,$$

that counts the number of groups of order p^8 and exponent p. How many of these groups can be the circle group of an $\mathbb{F}_p$-algebra of dimension 8 is unknown (to me). On the other hand, Bachiller [3] has found a group of order p^{10} and exponent p for $p > 12$ that is not the circle group of a brace with additive group an elementary abelian group of order p^{10}.

7. Bi-skew braces and semidirect products

Now we consider another large class of bi-skew braces.

Let G be a finite group with a pair of complementary subgroups G_L, G_R. This means: $G_L \cap G_R = 1$ and $|G_L||G_R| = |G|$, or equivalently, each g in G is uniquely a product $g = g_L \cdot g_R$ with g_L in G_L, g_R in G_R. In [19], Section 2, these groups G are said to have an exact factorization through G_L and G_R. Byott [5] observed that for any such group $G = G_L \cdot G_R$, there is a Hopf Galois structure of type G on a Galois extension L/K with Galois group $G_L \times G_R$. For let β_L, β_R be the pair of homomorphisms from $G_L \times G_R$ to G given by

$$\beta_L(g_L, g_R) = g_L, \quad \beta_R(g_L, g_R) = g_R^{-1}.$$

Then $\beta : G_L \times G_R \to \mathrm{Hol}(G)$ by

$$\beta(g_L, g_R) = \lambda(g_L)\rho(g_R) = \lambda(g_L g_R^{-1})C(g_R)$$

is a regular embedding from $G_L \times G_R$ to $\lambda(G) \rtimes \mathrm{InAut}(G) \subset \mathrm{Hol}(G)$. (Here $C(g)(x) = gxg^{-1}$ is conjugation by g.) Thus we obtain a Hopf Galois structure of type G on L/K.

The corresponding $\circ$-structure on $G(,\cdot)$ is induced by $b : G_L \times G_R$ given by $b(g_L, g_R) = \beta((g_L, g_R))(1) = g_L g_R^{-1}$. Thus

$$\begin{aligned} b(g_L, g_R) \circ b(h_L, h_R) &= (g_L g_R^{-1}) \circ (h_L h_R^{-1}) \\ &= g_L h_L h_R^{-1} g_R^{-1} \\ &= (g_L h_L)(g_R h_R)^{-1} \\ &= b((g_L h_L, g_R h_R) \\ &= b((g_L, g_R)(h_L, h_R)). \end{aligned}$$

Then $(G, \circ, \cdot)$ is a left skew brace, where $(G, \cdot) = G = G_L G_R$ with its given operation, and $(G, \circ) \cong G_L \times G_R$.

It is easy to check that the skew brace relation

$$x \circ (y \cdot z) = (x \circ y) \cdot x^{-1} \cdot (x \circ z)$$

holds: both sides are equal to $x y_L z y_R^{-1}$.

Thus Byott's observation implies the existence of skew braces with additive group any group G with complementary subgroups G_L and G_R: the circle group is isomorphic to $G_L \times G_R$. This recovers Theorem 2.3 of [19] (which obtains G as a skew brace directly, not considering the corresponding Hopf Galois structure, and includes several nice examples).

Now consider the special case where $G = G_L \rtimes G_R$ is a semidirect product of two finite groups G_L and G_R, where G_L is normal in G.

Denote the group operation in G by $\cdot$, which we will often omit. Thus for x, y in G, $xy = x \cdot y$.

In the semidirect product, an element x_R of G_R acts on y_L in G_L by conjugation:

$$x_R^{-1} y_L = (x_R^{-1} y_L x_R) x_R^{-1}.$$

Then

$$\begin{aligned} xy &= x_L x_R^{-1} y_L y_R^{-1} \\ &= x_L (x_R^{-1} y_L x_R) x_R^{-1} y_R^{-1}. \end{aligned}$$

As above, we also define the direct product operation $\circ$ on G by

$$\begin{aligned} x \circ y &= x_L x_R^{-1} \circ y_L y_R^{-1} \\ &= x_L y_L y_R^{-1} x_R^{-1} \\ &= x_L y x_R^{-1}. \end{aligned}$$

For semidirect products, we have

Proposition 7.1. $(G, \circ, \cdot)$ *is a bi-skew brace.*

Proof. We need to check the relation

$$x \cdot (y \circ z) = (x \cdot y) \circ \overline{x} \circ (x \cdot z) \qquad (*)$$

where if $x = x_L x_R^{-1}$, then $\overline{x} = x_L^{-1} x_R$ is the $\circ$-inverse of x.

Note that

$$\begin{aligned} xy &= x_L x_R^{-1} y_L y_R^{-1} \\ &= x_L (x_R^{-1} y_L x_R) x_R^{-1} y_R^{-1}, \end{aligned}$$

so $(xy)_L = x_L(x_R^{-1} y_L x_R)$ and $(xy)_R^{-1} = x_R^{-1} y_R^{-1}$.

Now the left side of (*) is

$$x \cdot (y \circ z) = x y_L z y_R^{-1}.$$

The right side of (*) is

$$\begin{aligned} (xy) \circ \overline{x} \circ (xz) &= xy \circ x_L^{-1} x_R \circ xz \\ &= xy \circ x_L^{-1} x z x_R \\ &= xy \circ x_R^{-1} z x_R \\ &= (xy)_L x_R^{-1} z x_R (xy)_R^{-1} \\ &= (x_L(x_R^{-1} y_L x_R)) x_R^{-1} z x_R (x_R^{-1} y_R^{-1}) \\ &= x y_L z y_R^{-1}. \end{aligned}$$

Hence formula (*) holds and $(G, \circ, \cdot)$ is also a skew brace, with additive group $(G, \circ)$.

Thus given a semidirect product $G = G_L \rtimes G_R$, if we let $\cdot$ be the usual multiplication in G, and let $\circ$ be the multiplication on G is given by $x_L x_R^{-1} \circ y_L y_R^{-1} = x_L y_L y_R^{-1} x_R^{-1} = x_L y_L (x_R y_R)^{-1}$, then $(G, \cdot, \circ)$ is a bi-skew brace. □

This immediately yields a result of Crespo, Rio and Vela [11]:

Corollary 7.2. *Let $G = H \rtimes J$ be a semidirect product and let $\Gamma = H \times J$. Then $(H \rtimes J, H \times J)$ is realizable: every G-Galois extension of fields has a Hopf Galois structure of type Γ.*

[11] obtained this result by their method of induced Hopf Galois structures.

We note some examples related to previous work on Hopf Galois structures.

Example 7.3. In [1], Alabdali and Byott look at Hopf Galois structures on a Γ- Galois extension K/k of squarefree degree n. They show that if $\Gamma = C_n$ is cyclic, then for every group G of order n, (C_n, G) is realizable, and in fact they count the number of Hopf Galois structures of type G on K/k.

They observe that every group G of squarefree order n is metabelian, that is, there is an abelian normal subgroup A of G so that G/A is abelian. Since n is squarefree, necessarily $r = |A|$ and $s = |G/A|$ are coprime. By the Schur-Zassenhaus Theorem, it follows that G is a semidirect product,

$G = A \rtimes G/A$. Thus, by the discussion above on groups with complementary subgroups, for every group G of squarefree order n, (C_n, G) is realizable.

It follows from Corollary 7.2 that (G, C_n) is also realizable, that is,

Corollary 7.4. *Every Galois extension K/k of squarefree order n has a Hopf Galois structure of cyclic type.*

Example 7.5. In [6], we let L/K be a Galois extension with Galois group Γ, a non-cyclic abelian p-group of order p^n, $n \geq 3$. We showed that L/K admits a nonabelian Hopf Galois structure. The idea is to write $\Gamma = A \times B$, in such a way that there exists a non-abelian semidirect product $G = A \rtimes B$. Thus (Γ, G) is realizable. It follows from Corollary 7.2 that (G, Γ) is also realizable. More generally,

Corollary 7.6. *Given $G = A \rtimes B$ where A, B are abelian, then $(G, A \times B)$ is realizable. Thus a G-Galois extension admits an abelian Hopf Galois structure.*

Example 7.7. Moving away from the abelian case, an obvious class of examples is to take $G = \mathrm{Hol}(N) \cong N \rtimes \mathrm{Aut}(N)$ for any finite group N. Letting $\Gamma = N \times \mathrm{Aut}(N)$, we have that both (Γ, G) and (G, Γ) are realizable. If N is non-abelian, then both Γ and G are non-abelian.

For a small example, let $G = M_{(p)} \rtimes \mathrm{Aut}(M_{(p)})$, and let $\Gamma = M_{(p)} \times \mathrm{Aut}(M_{(p)})$. Here $M_{(p)}$ is the Heisenberg group over $\mathbb{F}_p$, which can be identified as the subgroup of $\mathrm{GL}_3(\mathbb{F}_p)$ consisting of upper triangular 3×3 matrices with diagonal entries $= 1$, and $\mathrm{Aut}(M_{(p)})$ is isomorphic to $C_p^2 \rtimes \mathrm{GL}_2(\mathbb{F}_p)$ [17]. Then G is a bi-skew brace of order $p^6(p^2-1)(p-1)$ with both additive and circle groups non-abelian.

Remark 7.8. We note that Proposition 7.1 need not hold if $G = HJ$ and H is not a normal subgroup of G. For a small example, let $G = S_4 = S_3 \cdot C_4$ where $S_3 = \mathrm{Perm}(\{1,2,3\})$ and C_4 is generated by the cycle $(1,2,3,4)$. Letting $\star$ be the usual operation in S_4 and $\circ$ be the operation in S_4 induced from the componentwise operation on $S_3 \times C_4$, $(S_4, \circ, \star)$ is a skew brace. But, as is easily checked, the skew brace defining relation for $(S_4, \star, \circ)$ does not always hold. For example, letting $x = x_R^{-1} = (1234)$, $y = y_L = (12)$ and $z = z_R^{-1} = (13)(24)$ (cycle notation), I found that $x \star (y \circ z) = (132)$, while

$$(x \star y) \circ \overline{x} \circ (x \star z) = (134).$$

Remark 7.9. We observe that there are bi-skew braces arising from radical algebras that do not arise from semidirect products.

A bi-skew brace arising from a semidirect product $G = H \rtimes J$ of groups as above has $(G, \star)$ a semidirect product and $(G, \circ)$ a direct product $H \times J$. Thus a bi-skew brace $(G, \circ, \star)$ arising from a semidirect product $H \rtimes J$ has the property that H and J are subgroups of both $(G, \circ)$ and $(G, \star)$, where the operations $\circ$ and $\star$ coincide on H and, if J is abelian, on J.

A skew brace $(A, \circ, +)$ arising from a radical $\mathbb{F}_p$-algebra $(A, +, \cdot)$ has additive group $(A, +)$ isomorphic to C_p^n. Thus if the skew brace $(A, \circ, +)$ arising from a radical $\mathbb{F}_p$-algebra also arose from a semidirect product, then the group $(A, +)$ would be an elementary abelian group, and the group $(A, \circ)$ would be a semidirect product of two elementary abelian subgroups, where on the subgroups, $\circ$ and $+$ are the same and the multiplication $\cdot$ is trivial.

Consider the radical $\mathbb{F}_p$-algebra A of dimension 6, with generators x, y, z, a, b, c and relations

$$xy = a, yz = b, zx = c$$

with all other products of generators $= 0$. Then the center of $(A, \circ)$ is $\langle a, b, c\rangle = A^2$, on which $\circ$ is the same as $+$.

Let $\alpha = rx + sy + tz + d$ where d is in A^2 and r, s, t are in $\mathbb{F}_p$. Then

$$\alpha \circ \alpha = \alpha + \alpha + rsa + stb + trc.$$

So $\alpha + \alpha = \alpha \circ \alpha$ if and only if $\alpha \cdot \alpha = 0$, if and only if at least two of r, s and t are zero. Also, since x, y and z do not commute pairwise in $(A, \cdot)$, any subgroup of $(A, +)$ containing two of x, y and z will not have $\circ = +$.

Thus if H and K are $\circ$-subgroups of A on which $\circ = +$, then $H \times K$ can contain at most two of x, y and z. So $H \times K$ cannot equal $(A, +)$.

References

[1] Alabdali, Ali A.; Byott, Nigel P. Counting Hopf–Galois structures on cyclic field extensions of squarefree degree. *J. Algebra* **493** (2018), 1–19. MR3715201, Zbl 06798687, arXiv:1703.09636, doi: 10.1016/j.jalgebra.2017.09.009. 585

[2] Bachiller, David. Classification of braces of order p^3. *J. Pure Appl. Algebra* **219** (2015), no. 8, 3568–3603. MR3320237, Zbl 1312.81099, arXiv:1407.5224, doi: 10.1016/j.jpaa.2014.12.013. 580, 581, 582

[3] Bachiller, David. Counterexample to a conjecture about braces. *J. Algebra* **453** (2016), 160–176. MR3465351, Zbl 1338.16022, arXiv:1507.02137, doi: 10.1016/j.jalgebra.2016.01.011. 576, 583

[4] Bachiller, David. Solutions of the Yang–Baxter equation associated to skew left braces, with applications to racks. *J. Knot Theory Ramifications* **27** (2018), no. 8, 1850055, 36 pp. MR3835326, Zbl 06916027, arXiv:1611.08138, doi: 10.1142/S0218216518500554. 576

[5] Byott, Nigel P. Solubility criteria for Hopf–Galois structures. *New York J. Math.* **21** (2015), 883–903. MR3425626, Zbl 1358.12001, arXiv:1412.5923. 583

[6] Byott, Nigel P.; Childs, Lindsay N. Fixed-point free pairs of homomorphisms and nonabelian Hopf–Galois structures. *New York J. Math.* **18** (2012), 707–731. MR2991421, Zbl 1282.12002. 586

[7] Caranti, Andrea; Dalla Volta, Francesca; Sala, Massimiliano. Abelian regular subgroups of the affine group and radical rings. *Publ. Math. Debrecen* **69** (2006), no. 3, 297–308. MR2273982, Zbl 1123.20002, arXiv:math/0510166. 576

[8] Chase, Stephen U.; Sweedler, Moss E. Hopf algebras and Galois theory. Lecture Notes in Mathematics, 97. *Springer-Verlag, Berlin-New York*, 1969. ii+133 pp. MR0260724, Zbl 0197.01403, doi: 10.1007/BFb0101433. 575

[9] Childs, Lindsay N. Some Hopf Galois structures arising from elementary abelian p-groups. *Proc. Amer. Math. Soc.* **135** (2007), no. 11, 3453–3460. MR2336557, Zbl 1128.16022, doi: 10.1090/S0002-9939-07-08888-0. 583

[10] Childs, Lindsay N. Skew braces and the Galois correspondence for Hopf Galois structures. *J. Algebra* **511** (2018), 270–291. MR3834774, Zbl 1396.12003, arXiv:1802.03448, doi: 10.1016/j.jalgebra.2018.06.023. 576

[11] Crespo, Teresa; Rio, Anna; Vela, Montserrat. Induced Hopf Galois structures. *J. Algebra* **457** (2016), 312–322. MR3490084, Zbl 06575146, arXiv:1505.07587, doi: 10.1016/j.jalgebra.2016.03.012. 585

[12] De Graaf, Willem A. Classification of nilpotent associative algebras of small dimension. *Internat. J. Algebra Comput.* **28** (2018), no. 1, 133–161. MR3768261, Zbl 06850907, arXiv:1009.5339, doi: 10.1142/S0218196718500078. 580

[13] Featherstonhaugh, S. C.; Caranti, Andrea; Childs, Lindsay N. Abelian Hopf Galois structures on prime-power Galois field extensions. *Trans. Amer. Math. Soc.* **364** (2012), no. 7, 3675–3684. MR2901229, Zbl 1287.12002, doi: 10.1090/S0002-9947-2012-05503-6. 576, 583

[14] Greither, Cornelius; Pareigis, Bodo. Hopf Galois theory for separable field extensions. *J. Algebra* **106** (1987), no. 1, 239–258. MR0878476, Zbl 0615.12026, doi: 10.1016/0021-8693(87)90029-9. 575, 577

[15] Guarneri, L.; Vendramin, Leandro. Skew braces and the Yang–Baxter equation. *Math. Comp.* **86** (2017), no. 307, 2519–2534. MR3647970, Zbl 1371.16037, arXiv:1511.03171, doi: 10.1090/mcom/3161. 576, 577

[16] Kruse, Robert L.; Price, David T. Enumerating finite rings. *J. London Math. Soc. (2)* **2** (1970), 149–159. MR0251079, Zbl 0188.08601, doi: 10.1112/jlms/s2-2.1.149. 580

[17] Nejabati Zenouz, Kayvan. Skew braces and Hopf–Galois structures of Heisenberg type. *J. Algebra* **524** (2019), 187–225. MR3905210, Zbl 07027115, arXiv:1804.01360, doi: 10.1016/j.jalgebra.2019.01.012. 576, 577, 583, 586

[18] Rump, Wolfgang. Braces, radical rings, and the quantum Yang–Baxter equation. *J. Algebra* **307** (2007), no. 1, 153–170. MR2278047, Zbl 1115.16022, doi: 10.1016/j.jalgebra.2006.03.040. 576, 579, 580

[19] Smoktunowicz, Agata; Vendramin, Leandro. On skew braces (with an appendix by N. Byott and L. Vendramin). *J. Comb. Algebra* **2** (2018), no.1, 47–86. MR3763907, Zbl 06857320, arXiv:1705.06958, doi: 10.4171/JCA/2-1-3. 576, 578, 583, 584

[20] Vaughan-Lee, Michael. Groups of order p^8 and exponent p. *Int. J. Group Theory* **4** (2015), no. 4, 25–42. MR3416635, doi: 10.22108/IJGT.2015.5758. 583

[21] Vendramin, Leandro. Problems on skew left braces. To appear in *Adv. Group Theory Appli.* **7** (2019), 15–37. arXiv:1807.06411. 578

(Lindsay N. Childs) Department of Mathematics and Statistics, University at Albany, Albany, NY 12222, USA.
lchilds@albany.edu

This paper is available via http://nyjm.albany.edu/j/2019/25-26.html.