Bi-skew braces and Hopf Galois structures

Lindsay N. Childs
University at Albany
Albany, NY 12222

Introduction

Let L/K be a G-Galois extension of fields: that is, a Galois extension of fields with Galois group G. Since Greither and Pareigis's pioneering work in 1987, there has been interest in determining the Hopf Galois structures on a G-Galois extension.
If L/K is an H-Hopf Galois extension for H a cocommutative K-Hopf algebra, then $L \otimes_K H \cong LN$ where N is a regular subgroup of $\mathrm{Perm}(G)$ normalized by the image $\lambda(G)$ of the left regular representation $\lambda : G \to \mathrm{Perm}(G)$ given by $\lambda(g)(g') = gg'$ for g, g' in G. If N is isomorphic to a given abstract group M, we say that the H-Hopf Galois extension has type M.

Realizability

If a G-Galois extension has a Hopf Galois structure of type M, we'll say that the ordered pair (G, M) of 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 M on a G-Galois extension.

I'll mostly focus on the qualitative question here.
But I'll reframe the question first.

(Left) skew braces

A skew brace is a set B with two group operations, $\star$ and $\circ$, satisfying a certain compatibility condition analogous to left distributivity. It has been known for two or three years that if $(B, \circ, \star)$ is a skew brace with additive group $M = (B, \star)$ and circle group $G = (B, \circ)$, then the pair (G, M) is realizable.

I'll sketch the ideas below.

Bi-skew braces

The main novelty of this paper is to define a bi-skew brace, a set B with two group operations $\star$ and $\circ$, so that B is a skew brace with either group $M = (B, \star)$ or $G = (B, \circ)$ playing the role of the additive group. Given a bi-skew brace, then both (G, M) and (M, G) are realizable.

Many non-trivial examples exist, as we'll see. They yield new examples of realizable pairs of groups in Hopf Galois theory.

To be more precise,...

What is a skew brace?

Definition

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 $(B, \star)$. If $(B, \star)$ is abelian, B is called a left brace.

The inverse of a in $(B, \circ)$ is denoted by $\overline{a}$. It is known that in a skew brace, the identity elements of the two groups are equal.
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).

A special case–radical rings

Radical rings are examples of left braces. A radical ring is a finite ring $(A, +, \cdot)$ with the property that if we define

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

then $(A, \circ)$ is a group. Then $(A, \circ, +)$ is a brace. In $(A, +, \cdot)$ the defining formula

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

quickly reduces to left distributivity: $a(b + c) = ab + ac$.
But there are braces that do not arise from radical rings.

History ...

Skew braces were introduced in [GV17] as a non-commutative generalization of left braces of [Rum07], which in turn generalize radical algebras. 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 Caranti, della Volta and Sala [CDVS06] of the relationship between radical $\mathbb{F}_p$-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 [FCC12].

Bachiller in [Bac16] observed that the connection in [FCC12] generalizes to a close connection between abelian Hopf Galois structures on Galois extensions of fields and left braces. That connection was extended to skew braces and arbitrary Hopf Galois structures in the appendix by Byott and Vendramin in [SV18], and has already been used to study Hopf Galois structures, in particular in the thesis of Zenouz [Zen18], and in [Ch18].

The left representation maps $\lambda_\star, \lambda_\circ$

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

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

Then (c.f. Guarneri-Vendramin [GV17], Proposition 1.9) we have

Theorem

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

Connection with Hopf Galois structures ...

We sketch the connection between skew braces and Hopf Galois structures.

Suppose $(G, \circ, \star)$ is a skew brace.

Recall that if K/k is a $(G, \circ)$-Galois extension, and N is a regular subgroup of $\mathrm{Perm}(G)$ normalized by $\lambda_\circ(G)$, then $K[N]^G = H$ acts on K/k and makes K/K a Hopf Galois extension of type N. And conversely, by Greither-Pareigis.

To see how this relates to skew braces, we have

Theorem

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

The idea is that given a skew brace structure $(G, \circ, \star)$ on the Galois group $(G, \circ)$ of K/k, then by [GV17], $\lambda_\circ(G)$ is contained in $\mathrm{Hol}(G, \star)$, the normalizer in $\mathrm{Perm}(G)$ of $N = \lambda_\star(G)$, and so, obviously, $N \subset \mathrm{Perm}(G)$ is a regular subgroup of $\mathrm{Perm}(G)$ that is normalized by $\lambda_\circ(G)$. Thus N corresponds by Galois descent to a Hopf Galois structure on K/k of type $(G, \star)$.

Conversely...

In the other direction, if K/k is a G-Galois extension and has a H Hopf Galois structure of type N, then H yields a regular subgroup M of $\mathrm{Perm}(G)$ isomorphic to N that is normalized by $\lambda_\circ(G)$. Then the bijection $N \to G$ obtained from regularity defines a group structure $\star$ on G to make $(G, \star)$ isomorphic to N, in such a way that $N = \lambda_\star(G)$ is normalized by $\lambda_\circ(G)$.

So $\lambda_\circ(G)$ is in $\mathrm{Hol}(G, \star) \subset \mathrm{Perm}(G)$. By the Guarneri-Vendramin characterization of skew braces, $(G, \circ, \star)$ is then a skew brace.

Not bijective

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. [Ze18], Corollary 2.4):

Theorem (Byott, Zenouz)

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

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

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

New stuff

All of this has been known for a while, and most of it, in some form or other, is in Zenouz's paper [Zen18] or the Byott-Vendramin appendix to Smoktunowicz and Vendramin's paper [SV18].
But now for the main new idea of this talk.

Bi-skew braces

Definition

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 a bi-skew brace is a skew brace in which either operation can define the additive group.

Are there examples?

Trivial examples

A group G with operation $\star$ is a bi-skew brace with $\circ = \star$.

A non-abelian group G with operation $\star$ is a bi-skew brace with $\circ$ defined by $g \circ h = h * g$.

There are other examples.

The reason other examples would be interesting relates to the realizability question.

Bi-skew braces and realizability

Suppose $(B, \circ, \star)$ is a bi-skew brace. If $(B, \circ) \cong \Gamma$ and $(B, \star) \cong N$, then every Γ-Galois extension has a Hopf Galois structure of type N, and every N-Galois extension has a Hopf Galois structure of type Γ. So both (Γ, N) and (N, Γ) are realizable.
There is also a quantitative consequence.

A quantitative result

Theorem

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

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

This is a trivial consequence of the quantitative result of Byott-Zenouz cited above. I'll give an example below.

Non-trivial examples I

Here is our first class of non-trivial examples of bi-skew braces.

Theorem

Let $(A, +, \cdot)$ be a nilpotent $\mathbb{F}_p$- algebra of $\mathbb{F}_p$-dimension n. Then $(A, \circ, +)$ is a left brace where the circle operation on A is defined by

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

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

We know $(A, \circ, +)$ is a skew left brace. But also $(A, +, \circ)$ is a skew left brace if $A^3 = 0$:

Why?

We need to show that

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

If this holds for all a, b, c, then it holds modulo the ideal A^4. Recalling that $a \circ b = a + b + ab$ we see that the left side of $a + (b \circ c) = (a + b) \circ \overline{a} \circ (a + c)$ is

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

The right side is

$$(a + b) + \overline{a} + (a + c) + (a + b) \cdot \overline{a} + (a + b) \circ (a + c) + \overline{a} \circ (a + c) + (a + b) \cdot \overline{a} \cdot (a + c).$$

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

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

The left side was

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

So the skew brace property holds for all a, b, c in A iff $A^3 = 0$.
Thus, many radical $\mathbb{F}_p$-algebras yield bi-skew braces. In fact,

Theorem

(Kruse-Price)[KP70, Theorem 2.2] The number of isomorphism classes of $\mathbb{F}_p$-algebras A of dimension n with $A^3 = 0$ is p^α where $\alpha = \frac{4}{27}n^3 + O(n^2)$.

A first non-trivial example

Let A be the $\mathbb{F}_p$-algebra

$$A = \langle a, b, c | a^2 = c, ab = c \rangle$$

(so all other products of two of a, b, c are zero). Note that $A^3 = 0$. Then $(A, \circ, +)$ is a bi-skew brace where $(A, +) \cong C_p^3$ and $(A, \circ) \cong H_3(p)$, the Heisenberg group, the unique non-abelian group of order p^3 and exponent p. So both $(H_3(p), C_p^3)$ and $(C_p^3, H_3(p))$ are realizable.

A quantitative result

Since $(A, \circ, +)$ is a bi-skew brace where $M = (A, +) \cong C_p^3$ and $\Gamma = (A, \circ) \cong H_{(p)}$, the formula

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

yields

$$e_A(H_3(p), [C_p^3]) = (p^3 - 1) e_A(C_p^3, [H_3(p)]).$$

In words, given Galois extensions K/k with Galois group $\Gamma \cong C_p^3$ and K'/k' with Galois group $G \cong H_3(p)$, 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 $H_3(p)$ arising from A on K/k.

Sources of small skew braces

To get a sense of how many skew braces are bi-skew braces, I browsed into some classifications of small examples.

Radical algebras, braces, and skew braces of order p^3 have been classified by de Graaf, Bachiller and Zenouz, respectively. I looked in particular at Bachiller's, looking for bi-skew braces.

Bachiller's classification

Of the 26 isomorphism types of left braces of order p^3 found by Bachiller, seven types have $(B,+) \cong C_p \times C_{(p^2)}$ and $(B,\circ) \cong M_3(p)$ and are bi-skew braces, and four types have $(B,+) \cong C_p^3$ and $(B,\circ) \cong H_3(p)$ and are bi-skew braces. Here $M_3(p)$ is the unique non-abelian group of order p^3 and exponent p^2, while $H_3(p)$ is the Heisenberg group of order p^3 and exponent p. In particular, $(C_p \times C_{p^2}, M_3(p))$ and $(M_3(p), C_p \times C_{p^2})$ are realizable, as are $(C_p^3, H_3(p))$ and $H_3(p), C_p^3)$.

Note that the exponents of the groups in the realizable pairs are equal. That illustrates Bachiller's exponent result:

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 a result in [FCC12] for $(B, +)$ a radical ring, Bachiller 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 $(B, \circ) \cong (B, +)$.

In particular, for 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 of type C_p^n that arise from identifying G as the circle group of an $\mathbb{F}_p$-algebra are among those groups of order p^n and exponent p.

Group results

There is some fairly recent literature counting the groups of order p^n for $p > n+2$ and $n \leq 8$. This literature is reviewed in [VL14], 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).

But Bachiller [Bac16] found a group of order p^{10} and exponent p for $p > 12$ that is not the circle group of a brace (and therefore is not the circle group of a radical $\mathbb{F}_p$-algebra of order p^{10}. Thus for $p > 12$ there is a non-abelian group Γ of order p^{10} and exponent p so that a Γ-Galois extension does not have a Hopf Galois structure of elementary abelian type: (Γ, C_p^{10}) is not realizable.

Another class of bi-skew braces: semidirect products

Let $G = G_L \rtimes G_R$ be a semidirect product of two finite groups G_L and G_R, where G_L is normal in G and the action of G_R on G_L is by conjugation. Denote the group operation in G by $\cdot$, which we will often omit.

An element of G has a unique decomposition as $x = x_L x_R^{-1}$ for x_L in G_L, x_R in G_R. Then

$$y_R x_L = (y_R x_L y_R^{-1}) y_R.$$

So multiplication is by

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

Along with the given group operation on G we also define the direct product operation $\circ$, as follows:

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

$(G, \circ) \cong G_L \times G_R$

Note that the map $G_L \times G_R \to (G, \circ)$ by

$$(x_L, x_R) \mapsto x_L x_R^{-1}$$

is an isomorphism, for

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

$(G, \circ, \cdot)$ is a skew brace

To see that $(G, \circ, \cdot)$ is a skew brace, we look at the formula

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

for x, y, z in G, where x^{-1} is the inverse of x in $(G, \cdot)$. A computation shows that both sides of the formula are equal to

$$x_L yz x_R^{-1}.$$

$(G, \cdot, \circ)$ is also a skew brace

To see that $(G, \cdot, \circ)$ is a skew brace, we check the formula

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

where $\overline{x}$ is the $\circ$-inverse of x. It turns out that both sides of this formula are equal to $xy_L z y_R^{-1}$.

So:

Theorem (SDP)

Let $H \rtimes J$ be any semidirect product, and let $H \times J$ be the corresponding direct product. Then both $(H \rtimes J, H \times J)$ and $(H \times J, H \rtimes J)$ are realizable.

Examples I: Crespo, Rio, Vela

For $\Gamma = H \times J, G = H \rtimes J$, the fact that (Γ, G) is realizable follows from the method of fixed point free pairs of homomorphisms from Γ to G, which showed up in some generality in Byott and Childs [BC12], where we showed that, for example, every Galois extension with Galois group an abelian p-group has a non-abelian Hopf Galois structure. Byott in 2015 observed that the fixed point free pairs idea extends to the case where $G = HJ$ where H and J are complementary subgroups, then letting $\Gamma = H \times J$, then (Γ, G) is realizable.
Using their method of induced Hopf Galois structures, Crespo, Rio and Vela proved in 2016 that if $G = H \rtimes J$ is a semidirect product, and $\Gamma = H \times J$, then (G, Γ) is realizable.
The method of fixed point free pairs + Theorem [SDP] yields the CRV result.

Limit on [SDP]

Theorem [SDP] does not extend in general to groups with complementary subgroups that are not semidirect products. For example,

$$S_4 = S_3 \cdot C_4 = \mathrm{Perm}(1,2,3) \cdot \langle (1,2,3,4) \rangle.$$

Of course S_3 and C_4 are not normal subgroups of S_4.
It turns out that S_4 is a slew brace but not a bi-skew brace with second operation induced from the direct product $\mathrm{Perm}(1,2,3) \times \langle (1,2,3,4) \rangle$.
So the fact that a semidirect product of groups yields a bi-skew brace does not extend to a general group with a pair of complementary subgroups.

Examples II: Alabdali and Byott [18]

Alabdali and Byott look at Hopf Galois structures on a C_n- Galois extension K/k of squarefree degree n. They show that 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.

Every group G of squarefree order n is metabelian, that is, G has an abelian normal subgroup A 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, $G = A \rtimes G/A$. So [AB18] shows: For every group G of squarefree order, (C_n, G) is realizable. And [SDP] above shows that (G, C_n) is also realizable, that is,

Corollary

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

Of course this is a corollary of the CRV result

Examples III

For an infinite class of bi-skew braces with non-isomorphic non-abelian groups, consider

$$G = \mathrm{Hol}(N) \cong N \rtimes \mathrm{Aut}(N)$$

for any non-abelian finite group N. Letting $\Gamma = N \times \mathrm{Aut}(N)$, we have that both (Γ, G) and (G, Γ) are realizable.

For a small example, let $G = H_3(p) \rtimes \mathrm{Aut}(H_3(p))$, and let $\Gamma = H_3(p) \times \mathrm{Aut}(H_3(p))$. Here $H_3(p)$ 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 $\mathrm{Aut}(H_3(p))$ is isomorphic to $C_p^2 \rtimes GL_2(\mathbb{F}_p)$ [Ze18]. Then G is a bi-skew brace of order $p^6(p^2 - 1)(p - 1)$ with both additive and circle groups non-abelian.

Postscript

It turns out that the two large classes of bi-skew braces are distinct. Clearly there are many bi-skew braces arising from semidirect products that don't come from radical algebras. But there are also bi-skew braces arising from radical algebras that don't arise from semidirect products.
An example is the $\mathbb{F}_p$-algebra A with $\mathbb{F}_p$-basis $\{x, y, z, a, b, c\}$ with multiplication of basis elements: $xy = a, yz = b, zx = c$ and all other products $= 0$. Then $A^3 = 0$, so $(A, \circ, +)$ is a bi-skew brace. The additive group $(A, +)$ is elementary abelian of order p^6, and the circle group $(A, \circ)$ cannot be a semidirect product of two elementary abelian subgroups of $(A, \circ)$.

Many thanks to Rob Underwood for everything he did to make the AUM workshop such a success, and to Rob and Alan Koch for organizing the very interesting Auburn AMS Special Session.