Bi-Skew Braces and Hopf–Galois structures with a surjective Hopf–Galois correspondence

Joint work with Lorenzo Stefanello

Senne Trappeniers

July 28 2023

VRIJE
UNIVERSITEIT
BRUSSEL

Skew braces

Definition ([GV17])

A skew (left) brace is a triple $(A, +, \circ)$ where

- A is a set,
- $(A, +)$ and $(A, \circ)$ are groups,
- for all $a, b, c \in A$, the equality

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

$(A, +)$ is called the additive group and $(A, \circ)$ the multiplicative group.

λ-map

Given a skew brace $(A, +, \circ)$ and $a, b \in A$, we define

$$\lambda_a(b) = -a + a \circ b.$$

Then we obtain a group homomorphism

$$\lambda : (A, \circ) \to \mathrm{Aut}(A, +), \quad a \mapsto \lambda_a.$$

Definition

A left ideal of a skew brace $(A, +, \circ)$ is a subgroup I of $(A, +)$ such that $\lambda_a(I) = I$ for all $a \in A$. It is automatically also a subgroup of $(A, \circ)$.

Bi-skew braces

Definition ([Chi19])

A skew brace $(A, +, \circ)$ is a bi-skew brace if also $(A, \circ, +)$ is a skew brace.

Easy examples

Let $(A, \circ)$ be a group.

- The trivial skew brace $(A, \circ, \circ)$ is a bi-skew brace.
- The almost trivial skew brace $(A, \circ_{\mathrm{op}}, \circ)$ is a bi-skew brace.

Why bi-skew braces?

- A finite skew brace $(A, +, \circ)$ yields a Hopf-Galois structure of type $(A, +)$ on a Galois extensions with Galois group isomorphic to $(A, \circ)$. So for a given multiplicative group, how do we construct an additive group?
- Most constructions: additive group $\to$ multiplicative group.

Why bi-skew braces?

- A finite skew brace $(A, +, \circ)$ yields a Hopf-Galois structure of type $(A, +)$ on a Galois extensions with Galois group isomorphic to $(A, \circ)$. So for a given multiplicative group, how do we construct an additive group?
- Most constructions: additive group $\to$ multiplicative group.
- No distinction for bi-skew braces!

Bi-skew braces

Theorem ([Car20])

Let $(A, +, \circ)$ *be a skew brace, the following properties are equivalent:*

1. A *is a bi-skew brace.*
2. $\lambda : (A, \circ) \to \mathrm{Aut}(A, \circ)$ *is a homomorphism.*
3. $\lambda : (A, +) \to \mathrm{Aut}(A, +)$ *is an anti-homomorphism.*
4. $\lambda_a \lambda_b \lambda_a^{-1} = \lambda_{\lambda_a(b)}$ *for all* $a, b \in A$.

Brace blocks

Definition ([Koc21])

Let A be a set. A brace block, denoted by $((A, \circ_i) \mid i \in I)$, consists of a family of group operations $((A, \circ_i) \mid i \in I)$ on A such that for all $i, j \in I$, $(A, \circ_i, \circ_j)$ is a skew brace.

Brace blocks

Definition ([Koc21])

Let A be a set. A brace block, denoted by $((A, \circ_i) \mid i \in I)$, consists of a family of group operations $((A, \circ_i) \mid i \in I)$ on A such that for all $i, j \in I$, $(A, \circ_i, \circ_j)$ is a skew brace.

Clearly all skew braces $(A, \circ_i, \circ_j)$ must be bi-skew braces.

Brace blocks

Example

Given a bi-skew brace $(A, +, \circ)$, we have a brace block $((A, +), (A, \circ))$.

General construction

Theorem ([ST23a])

Let $(\lambda_i : (A,+) \to \mathrm{Aut}(A,+) \mid i \in I)$ *be anti-homomorphisms. Then the following are equivalent:*

1. *The family* $(A,+) \cup ((A,\circ_i) \mid i \in I)$*, where* $a \circ_i b = a + {}^{\lambda_i(a)}b$*, forms a brace block.*
2. *For all* $\alpha, \beta \in (\lambda_i : (A,+) \to \mathrm{Aut}(A,+) \mid i \in I)$ *and* $a, b \in A$*,*

$$\alpha_a \beta_b \alpha_a^{-1} = \beta_{\alpha_a(b)}. \tag{1}$$

General construction

Theorem ([ST23a])

Let $(\lambda_i : (A, +) \to \mathrm{Aut}(A, +) \mid i \in I)$ *be anti-homomorphisms. Then the following are equivalent:*

1. *The family* $(A, +) \cup ((A, \circ_i) \mid i \in I)$*, where* $a \circ_i b = a + {}^{\lambda_i(a)}b$*, forms a brace block.*
2. *For all* $\alpha, \beta \in (\lambda_i : (A, +) \to \mathrm{Aut}(A, +) \mid i \in I)$ *and* $a, b \in A$*,*

$$\alpha_a \beta_b \alpha_a^{-1} = \beta_{\alpha_a(b)}. \tag{1}$$

Is this actually useful to construct brace blocks?

A more manageable construction

If all α_a and β_b commute, then (1) becomes

$$\beta_b = \beta_{\alpha_a(b)}.$$

A more manageable construction

If all α_a and β_b commute, then (1) becomes

$$\beta_b = \beta_{\alpha_a(b)}.$$

Theorem ([ST23a])

Let $(A,+)$ be a group, let M be an abelian subgroup of $\mathrm{Aut}(A,+)$, and let $\mathcal{S}$ be the set of group (anti-)homomorphisms $\lambda\colon A \to M$ such that $\lambda_{\psi(a)} = \lambda_a$ for all $a \in A$ and $\psi \in M$. Then $((A, \circ_\lambda) \mid \lambda \in \mathcal{S})$ is a brace block, where

$$a \circ_\lambda b = a + \lambda_a(b).$$

A more manageable construction

Is it too restrictive to ask that all λ map into abelian subgroup?

A more manageable construction

Is it too restrictive to ask that all λ map into abelian subgroup?
Not at all! All known constructions of brace blocks [BNY23, CS21, CS22, Koc22] satisfy this property.

A more manageable construction

The question remains: how can we find abelian subgroups M of $\mathrm{Aut}(A,+)$ and maps λ satisfying $\lambda_{\psi(a)} = \lambda_a$ for all $a \in A$, $\psi \in M$?

Our intermediate construction with inner automorphisms

Choose an abelian $M \leq \mathrm{Inn}(A,+)$ and let $\mathcal{S}$ be the group homomorphisms $\lambda : A \to M$ such that $\lambda_{\psi(a)} = \lambda_a$ for all $\psi \in M$.

Our intermediate construction with inner automorphisms

Choose an abelian $M \leq \mathrm{Inn}(A,+)$ and let $\mathcal{S}$ be the group homomorphisms $\lambda : A \to M$ such that $\lambda_{\psi(a)} = \lambda_a$ for all $\psi \in M$. As for any ψ, there exists $b \in A$ such that $\psi(a) = b + a - b$, we find for any $\lambda : A \to M$ that

$$\lambda_{\psi(a)} = \lambda_{b+a-b} = \lambda_b \lambda_a \lambda_b^{-1} = \lambda_a.$$

Corollary ([CS22])

Let $(A,+)$ be a group, let M be an abelian subgroup of $\mathrm{Inn}(A,+)$, and let $\mathcal{S} = \mathrm{Hom}(A,M)$. Then $((A,\circ_\lambda) \mid \lambda \in \mathcal{S})$ is a brace block, where

$$a \circ_\lambda b = a + \lambda_a(b).$$

Surjective Hopf-Galois correspondence

Proposition ([ST23b])

Let L/K be a Galois extension with Galois group $(A, \circ)$. For a skew brace $(A, +, \circ)$ and its related Hopf-Galois structure H, we have a bijective correspondence

$$\{\text{left ideals of } (A, +, \circ)\}$$
$$\updownarrow$$
$$\{\text{intermediate fields of } L/K \text{ in the Hopf-Galois correspondence}\}$$

In light of the usual Galois correspondence, if we want the Hopf-Galois correspondence to be surjective, we need that every subgroup of $(A, \circ)$ is a left ideal of $(A, +, \circ)$.

Skew braces with surjective HG-correspondence

Recall that for a bi-skew brace $(A, +, \circ)$, $\lambda_a \in \mathrm{Aut}(A, \circ)$ for all $a \in A$. So we are interested in automorphisms of $(A, \circ)$ that map every subgroup to itself: these are called power automorphisms.

Skew braces with surjective HG-correspondence

For a group G, we define the norm $N(G)$ as the intersection of the normalizers of all subgroups of (G). Then the inner automorphisms coming from elements in $N(G)$ are precisely the inner power automorphisms. By [Sch60] we know that $N(G)$ is contained in the second center of G.

Bi-skew braces with surjective correspondence

Corollary ([CS22])

Let $(A, \circ)$ be a group, let M be an abelian subgroup of $\mathrm{Inn}(A, \circ)$, and let $\mathcal{S} = \mathrm{Hom}(A, M)$. Then $((A, \circ_\lambda) \mid \lambda \in \mathcal{S})$ is a brace block, where

$$a +_\lambda b = a \circ \lambda_a(b).$$

By taking $M = N(A, \circ)/Z(A, \circ) \subseteq \mathrm{Inn}(A, \circ)$ we find a brace block $((A, +_\lambda) \mid \lambda \in \mathrm{Hom}(A, M))$. So in particular we obtain bi-skew braces $(A, +_\lambda, \circ)$ yielding a surjective HG-correspondence.

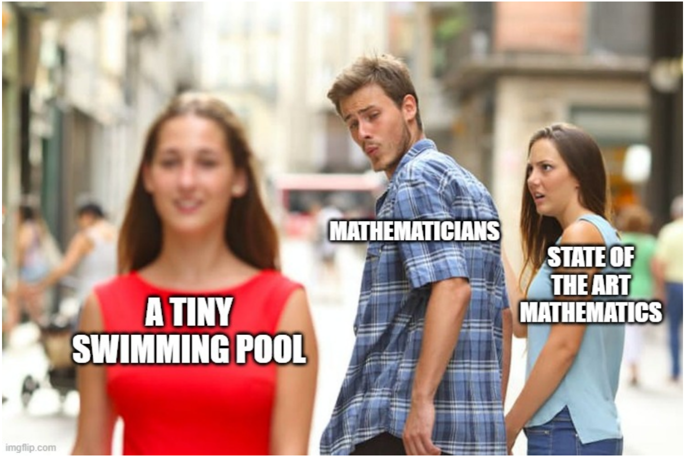
An example

Let $(A, \circ) = Q_8$. Every subgroup of $(A, \circ)$ is normal, so $N(A, \circ) = A$. Hence $M = N(A, \circ)/Z(A, \circ) = A/Z(A, \circ) \cong C_2^2$. It follows that

$$|\mathcal{S}| = |\mathrm{Hom}(A, M)| = |\mathrm{Hom}(C_2^2, C_2^2)| = |M_2(\mathbb{F}_2)| = 16$$

We obtain a brace block $((A, +_i) \mid i \in \{1, ..., 16\})$ such that for all i, $(A, +_i, \circ)$ yields a surjective HG-correspondence on Galois extensions with Galois group Q_8.

The end


MATHEMATICIANS
STATE OF THE ART MATHEMATICS
A TINY SWIMMING POOL
imgflip.com

Valeriy G. Bardakov, Mikhail V. Neshchadim, and Manoj K. Yadav.
Symmetric skew braces and brace systems.
Forum Mathematicum, 35(3):713–738, 2023.

A. Caranti.
Bi-skew braces and regular subgroups of the holomorph.
Journal of Algebra, 562(July):647–665, 2020.

L. N. Childs.
Bi-skew braces and Hopf Galois structures.
New York Journal of Mathematics, 25:574–588, 2019.

A. Caranti and L. Stefanello.
From endomorphisms to bi-skew braces, regular subgroups, the Yang–Baxter equation, and Hopf–Galois structures.
Journal of Algebra, 587(June):462–487, 2021.

A. Caranti and L. Stefanello.
Brace blocks from bilinear maps and liftings of endomorphisms.

Journal of Algebra, 610:831–851, 2022.

L. Guarnieri and L. Vendramin.
Skew braces and the Yang–Baxter equation.
Mathematics of Computation, 86(307):2519–2534, 2017.

A. Koch.
Abelian maps, bi-skew braces, and opposite pairs of Hopf-Galois structures, 2021.

A. Koch.
Abelian maps, brace blocks, and solutions to the Yang-Baxter equation.
Journal of Pure and Applied Algebra, 226(9):1–15, 2022.

Eugene Schenkman.
On the norm of a group.
Illinois J. Math., 4:150–152, 1960.

L. Stefanello and S. Trappeniers.
On bi-skew braces and brace blocks.
Journal of Pure and Applied Algebra, 227(5), 2023.

Lorenzo Stefanello and Senne Trappeniers.
On the connection between Hopf–Galois structures and skew braces.
Bulletin of the London Mathematical Society, 2023.