Some problems on skew braces

Leandro Vendramin

Vrije Universiteit Brussel

The Interplay Between Skew Braces and Hopf-Galois Theory
April 2023

I will discuss some problems related to the structure of skew braces.

A skew brace is a triple $(A,+,\circ)$, where $(A,+)$ and $(A,\circ)$ are groups and

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

holds for all $a,b,c\in A$.

Terminology:

- $(A,+)$ is the additive group of A (even if it is non-abelian) .
- $(A,\circ)$ is the multiplicative group of A.
- A is of abelian type if its additive group is abelian.

Etingof, Schedler and Soloviev[1] proved that the multiplicative group of a finite skew brace of abelian type is always solvable.

Question

Is every solvable finite group the multiplicative group of a skew brace of abelian type?

The answer is no. Using ideas of Rump and Lie theory, Bachiller[2] found a counterexample.

Problem

Find a minimal counterexample.

[1] Duke Math. J. 100 (1999), no. 2, 169–209.

[2] J. Algebra 453 (2016), 160–176.

Some comments:

- These problems are discrete analogs of (disproved) a conjecture of Milnor in the theory of flat manifolds.
- Bachiller's result depends on heavy computer calculations.
- We need to understand Bachiller's paper!

More challenging:

Problem

Which finite solvable groups appear as multiplicative groups of skew braces of abelian type?

One could also ask similar questions for skew braces of nilpotent type, which are skew braces with nilpotent additive group. Almost nothing is known in this case!

Another challenging problem related to solvability is the following conjecture:

Problem (Byott)

Let A be a finite skew brace such that $(A,+)$ is solvable. Is $(A,\circ)$ solvable?

The problem appeared in one of Byott's papers on Hopf–Galois structures. See also Problem 19.91 of *The Kourovka Notebook, by Khukhro and Mazurov*.

Let p be a prime number and G be a finite p-group. For $k \geq 1$, let

$$G^k = \langle g^k : g \in G \rangle.$$

Then G^k is a normal subgroup of G.

We say that G is powerful if the following conditions hold: if $p > 2$, then G/G^p is abelian; or if $p = 2$, then G/G^4 is abelian.

The notion goes back to Lubotzky and Mann and plays an important role in several areas of group theory.

A skew brace A is right nilpotent (RP) if $A^{(n)} = \{0\}$ for some n, where $A^{(1)} = A$ and

$$A^{(k+1)} = A^{(k)} * A = \langle x * a : x \in A^{(k)},\, a \in A \rangle_+,$$

and $y * z = -y + y \circ z - z$.

Conjecture (Shalev–Smoktunowicz)

Let p be a prime number and A be a skew brace of abelian type of size p^m. If the multiplicative group of A is powerful, then A is right nilpotent.

They formulated the conjecture for skew braces of abelian type. However, computer calculations suggest that the conjecture might be true in full generality (or at least for skew braces of nilpotent type).

Isoclinism of skew braces is a certain equivalence relation on skew braces. The notion is based on that of group theory and it was introduced[3] with my Ph.D. student Thomas Letourmy.

[3] arXiv:2211.14414.

The correspondence between skew braces and regular subgroups of the holomorph suggests a deep connection between skew braces and Hopf–Galois structures.

Question

Does isoclinism of skew braces have applications to the theory of Hopf–Galois structures?

A skew brace $(A, +, \circ)$ is said to be a bi-skew brace if $(A, \circ, +)$ is also a skew brace. The notion was introduced by Childs and has applications in Hopf–Galois theory.

Conjecture

Let A and B be finite isoclinic skew braces. Then A is a bi-skew brace if and only if B is a bi-skew brace.

Computer experiments support the conjecture.

Recently, Smoktunowicz[4] proved that there exists a bijective correspondence between right nilpotent skew braces of abelian type of size p^m (p prime) strongly nilpotent pre-Lie rings of size p^m.

Question

Is the notion of isoclinism of skew braces compatible with Smoktunowicz' bijective correspondence between skew braces of abelian type and pre-Lie rings?

[4] Adv. Math. 409 (2022), part B, Paper No. 108683, 33 pp.

Isoclinism of skew braces suggest an equivalence relation on the space of solutions to the Yang–Baxter equation.

A solution (to the Yang–Baxter equation) is a pair (X, r), where X is a set and

$$r\colon X \times X \to X \times X, \quad r(x, y) = (\sigma_x(y), \tau_y(x)),$$

is a bijective map such that

- the maps $\sigma_x\colon X \to X$ are bijective for all $x \in X$,
- the maps $\tau_x\colon X \to X$ are bijective for all $x \in X$, and
- $r_1 r_2 r_1 = r_2 r_1 r_2$, where

$$r_1 = r \times \mathrm{id} \quad \text{and} \quad r_2 = \mathrm{id} \times r.$$

To keep it simple, we will consider only involutive solutions, that is solutions (X, r) such that $r^2 = \mathrm{id}$.

Let (X, r) be a solution.

- The structure group of (X, r) is the group $G(X, r)$ with generators X and relations $xy = uv$ whenever $r(x, y) = (u, v)$.
- The permutation group of (X, r) is the group $\mathcal{G}(X, r) = \langle \sigma_x : x \in X \rangle$.

Facts:

- Both $G(X, r)$ and $\mathcal{G}(X, r)$ are skew braces (of abelian type).
- $\mathcal{G}(X, r)$ is a quotient of $G(X, r)$.

Important fact:
Let (X, r) be a solution. For $x, y \in X$ we define

$$x \sim y \Longleftrightarrow \sigma_x = \sigma_y.$$

This equivalence relation induces a solution on $X/\sim$,

$$\mathrm{Ret}(X, r) = (X/\sim, \overline{r}),$$

the retraction of X.

A solution (X, r) is multipermutation (MP) if there exist $n \geq 1$ such that $|\mathrm{Ret}^n(X, r)| = 1$.

Problem

Prove that "almost all" solutions are MP.

For example, there are 4895272 solutions of size ten and only 28832 are not MP.

Some comments:

- (X, r) is MP $\iff G(X, r)$ is RN $\iff \mathcal{G}(X, r)$ is RN.
- Isoclinism may be helpful here!

Example 1:
Let $X = \{1, 2, 3, 4, 5\}$ and $r(x, y) = (\sigma_x(y), \tau_y(x))$, where

$$\sigma_1 = \sigma_2 = \sigma_3 = \mathrm{id}, \quad \sigma_4 = (45), \quad \sigma_5 = (23)(45)$$

and

$$\tau_y(x) = \sigma_{\sigma_x(y)}^{-1}(y).$$

Then (X, r) is MP.

Example 2:
Let $X = \{1, 2, 3, 4\}$ and $r(x, y) = (\sigma_x(y), \tau_y(x))$, where

$$\sigma_1 = \sigma_2 = \mathrm{id}, \quad \sigma_3 = (34), \quad \sigma_4 = (12)(34)$$

and

$$\tau_y(x) = \sigma^{-1}_{\sigma_x(y)}(y).$$

Then (X, r) is MP.

We say that two solutions (X, r) and (Y, s) are permutation isoclinic if the skew braces $\mathcal{G}(X, r)$ and $\mathcal{G}(Y, s)$ are isoclinic.

The solutions of Examples 1 and 2 are permutation isoclinic.

Fact:
Let (X, r) and (Y, s) be permutation isoclinic solutions. Then (X, r) is MP if and only if (Y, s) is MP.

Problem

Construct finite solutions (say of small size) up to isoclinism.

We can also say that (X, r) and (Y, s) are isoclinic if and only if the skew braces $G(X, r)$ and $G(Y, s)$ are isoclinic.

Problem

What is the relationship between isoclinic solutions and permutation isoclinic solutions?

Let (X, r) be a solution. Motivated by the theory of braid groups Dehornoy[5] used Garside theory to construct a certain finite quotient of the structure group. These Coxeter-like groups are indeed skew braces of abelian type.

Problem

What about considering the equivalence relation on the space of solutions induced by isoclinism of their Coxeter-like quotients?

[5] Adv. Math. 282 (2015), 93–127.