Group theoretical problems on skew left braces

An application of group theory

Marco Damele
Dipartimento di Matematica e informatica
Università degli studi di Cagliari

April 3, 2025

Introduction

The Yang-Baxter equation are some equations that first appeared in theoretical physics and statistical mechanics in the work of Yang [Yang, 1967] and Baxter [Baxter, 1972]. Formally:

Definition

A set-theoretical solution of the Yang Baxter equation (YBE) is a pair (X, r) where X is a set and:

$$r : X \times X \longrightarrow X \times X, (x, y) \mapsto (\sigma_x(y), \tau_y(x))$$

is a bijective map such that

$$(r \times Id)(Id \times r)(r \times Id) = (Id \times r)(r \times Id)(Id \times r)$$

where Id is the identity map of $X \times X$ The solution (X, r) is called:

- non-degenerate if $\forall\ x \in X\ \sigma_x, \tau_x$ are bijective.
- involutive if $r^2 = Id_{X \times X}$

Introduction

Let's see some examples of solutions:

Example

The pair $(\mathbf{Z}, r)$ where $r(a, b) = (a+1, b+1)$ is a solution to the YBE

Example

Let X be a set and $r(x, y) = (y, x)$. Then (X, r) is an involutive non-degenerate solution of the YBE

Example

Let G be a group. Then:

1. (G, r_1) with $r_1(g, h) = (h, h^{-1}gh)$ is a non-degenerate solution of the YBE
2. (G, r_2) with $r_2(g, h) = (g^2h, h^{-1}g^{-1}h)$ is a non-degenerate solution of the YBE

Are there good methods to contruct all finite non-degenerate involutive solutions to the Yang–Baxter equation? In [Bachiller et al., 2015] Bachiller, Ced ́o and Jespers, give a method to construct all finite solutions of a given size. For it to work, one needs the classification of left braces, that is to say abelian group $(A, +)$ with another group operation $\cdot : (a, b) \in A \times A \longrightarrow ab \in A$ such that the following compatibility relation is satisfied: $a(b + c) = ab - a + ac$ for all $a, b, c \in A$. Is there an algebraic structure similar to the brace structure useful for studying non-involutive solutions? In [Guarnieri and Vendramin, 2016] Vendramin and Guarnieri introduce the notion of skew brace and provides an affirmative answer to the above question.

Definition

A skew (left) brace is a triple $(A, \cdot, \circ)$ such that $(A, \cdot)$ and $(A, \circ)$ are groups such that for all $a, b, c \in A$

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

where a^{-1} is the inverse of a with respect to the operation $\cdot$. Generally $(A, \cdot)$ is called the additive group and $(A, \circ)$ the multiplicative group of the skew left brace.

Example of skew left brace

Example (Trivial Skew left brace)

Let $(A, \cdot)$ be a group. Then $(A, \cdot, \circ)$ is a skew brace where $a \circ b = a \cdot b$ for all $a, b \in A$.

Example

Let $n \in \mathbf{N}_{\geq 2}$ and g a generators for $\mathbf{Z}_n$ with the usual group operation $\cdot$. Define the new operation $g^a \circ g^b = g^{(-1)^b a + b}$. Then $(\mathbf{Z}_n, \cdot, \circ)$ is a skew left brace.

The next example shows how group theory produce skew left brace.

Example (Theorem 2.3,[Smoktunowicz and Vendramin, 2018])

Let $(A, \cdot)$ be a group that factorize through two subgroups B and C, i.e $A = BC$. Then $(A, \cdot, \circ)$ is a skew left brace with $a \circ a' = ba'c$ where $a = bc \in BC, a' \in A$ and $(A, \circ) \simeq B \times C$. For example $\mathbf{A}_5$ factor through the subgroups $A = \langle (123), (12)(34) \rangle \simeq \mathbf{A}_4$, $B = \langle (12345) \rangle \simeq \mathbf{Z}_5$ so by above example there is a skew left brace with additive group $\mathbf{A}_5$ and multiplicative group $\mathbf{A}_4 \times \mathbf{Z}_5$.

Example of skew left brace

There are also some connection with ring theory

Example (Theorem 3.6, [Vendramin, 2024])

Let $(R, +, \cdot)$ be a commuative ring and let $J(R)$ be the jacobson radical of R. Then $(J(R), \circ, +)$ is a skew left brace where $a \circ b = ab + a + b$. In general if $(R, +, \cdot)$ is a radical ring then $(R, +, \circ)$ is a skew left brace where $a \circ b = ab + a + b$.

Example

A triple $(R, +, \cdot)$ such that $(R, +)$ is a group (not necessarily abelian), $(R, \cdot)$ is a semigroup such that $x(y + z) = xy + xz$ for every $x, y, z \in R$ is called a *near ring*. A subgroup M of $(N, +)$ is said to be a construction subgroup if $1 + M$ is a subgroup of the multiplicative subgroup N^* of units of N. M is a skew left brace with the operation: $m \cdot n = m + n$ and $m \circ n = m + (1 + m)n$.

More example and connection with other branches of mathematics can be found in [Smoktunowicz and Vendramin, 2018]

Introduction

To see how skew brace are related to the YBE we first introduce the so called "lambda-map". If A is a skew left brace the map:

$$\lambda : (A, \circ) \longrightarrow Aut((A, \cdot))$$

$$a \mapsto \lambda_a : A \longrightarrow A, b \mapsto a^{-1}(a \circ b)$$

is a group homomorphism [Corollary 1.10, [Guarnieri and Vendramin, 2016]]. This is a really important map since expresses the operation $\circ$ in terms of the operation $\cdot$ and viceversa: $a \circ b = a\lambda_a(b), ab = a \circ \lambda_{\bar{a}}(b)\ \forall a, b \in A$ where $\bar{a}$ is the inverse of a with respect to $\circ$. The following theorem tell us that skew left braces produces solution to the YBE:

Theorem (Theorem 3.1, [Guarnieri and Vendramin, 2016])

Let A be a skew left brace. Then (A, r_A) is a non degenerate solution of the YBE where

$$r_A(a, b) = (\lambda_a(b), \lambda^{-1}_{\lambda_a(b)}((a \circ b)^{-1}a(a \circ b)))$$

Moroever this solution is involutive $\iff$ $(A, \cdot)$ is abelian.

Introduction

Let (X, r) be a solution of the YBE. We define the structure group of (X, r) as the group $G(X, r) := \langle X \mid x \circ y = \sigma_x(y) \circ \tau_y(x) \rangle$ that is to say the group generated by X and relation given by $xy = uv$ where $r(x, y) = uv$. Morover let ι be the natural embedding of X in $G(X, r)$ so that every element $x \in X$ is mapped to itself.

Theorem (Theorem 3.9, [Guarnieri and Vendramin, 2016])

If (X, r) is an on-degenerate solution of YBE, there is a unique brace structure over $G(X, r)$ such that

$$r_{G(X,r)}(\iota \times \iota) = (\iota \times \iota)r$$

Furthermore, if B is a skew left brace and $f : X \longrightarrow B$ is a map such that $(f \times f)r = r_B(f \times f)$, then there exists a unique skew brace homomorphism $\phi : G(X, r) \longrightarrow B$ such that $f = \phi\iota$ and $(\phi \times \phi)r_G(X, r) = r_B(\phi \times \phi)$

This two theorems tell us that studying skew left brace by a theoretical point of view seems to be the best way to develop the study of the YBE.

Topic of the seminar

In this seminar we will study the following problems:

1. Given a finite group $(A, \cdot)$. Determine all the skew left brace structure over $(A, \cdot)$.
2. Given a finite skew braces $(A, \cdot, \circ)$ such that $(A, \cdot)$ is nilpotent, is $(A, \circ)$ solvable ?
3. Given a finite skew braces $(A, \cdot, \circ)$ such that $(A, \cdot)$ is solvable, is $(A, \circ)$ solvable ?

Holomorph of a group

We begin with the definition of the holomorph of a group.

Definition (Holomorph of a group)

Let A be a group. The holomorph of A is the semidirect product $Hol(A) := Aut(A) \ltimes_\phi A$ where $\phi : Aut(A) \longrightarrow Aut(A)$ is the identity map. Explicitly $Hol(A)$ is the group whose underlying set is $Aut(A) \times A$ and the operation being:

$$(f, a)(g, b) = (fg, af(b)) \;\forall\; f, g \in Aut(A), \;\forall\; a, b \in A$$

Example

Let's compute the holomorph of $\mathbf{Z}_3 = \langle x \rangle = \{1, x, x^2\}$. We have $Aut(\mathbf{Z}_3) = \langle \sigma \rangle = \{1, \sigma\}$ where $\sigma(x) = x^2$. Therefore $Hol(\mathbf{Z}_3) = Aut(\mathbf{Z}_3) \ltimes_\phi \mathbf{Z}_3$ has order $3 \cdot 2 = 6$. Hence by the classification theorem of groups of order 6 we get $Hol(\mathbf{Z}_3) \simeq \mathbf{Z}_6$ or $Hol(\mathbf{Z}_3) \simeq \mathbf{S}_3$. Since ϕ is not the trivial action we get $Hol(\mathbf{Z}_3) \simeq \mathbf{S}_3$.

As we will see skew left brace structure over A are encoded in $Hol(A)$, however very little is known about the holomorph of finite groups.

Constructing skew left braces

In order to justify the connection between skew left brace and the holomorph we need the following definition:

Definition (Regular subgroup)

Let A be a group. A subgroup H of $Hol(A)$ is said to be regular if for every $a \in A$ $\exists !$ $(f, x) \in H : xf(a) = 1$.

Let $\pi_2 : Hol(A) \longrightarrow A, (f, a) \mapsto a$. We have the following:

Lemma (Lemma 4.1, [Guarnieri and Vendramin, 2016])

Let A be a group and $H \leq Hol(A)$ be a regular subgroup of $Hol(A)$. Then $\pi_2|_H : H \longrightarrow A$ is bijective.

Example

By Lemma 16 above the only regular subgroup of $Hol(\mathbf{Z}_3)$ is $\mathbf{Z}_3$.

Constructing skew left braces

Proof of Lemma 16.

We first prove $\pi_2|_H$ is injective. Let $(f, a), (g, b) \in H$ such that $\pi(f, a) = \pi(g, b)$. Then $a = b$. Since H is a subgroup we have $(f, a)^{-1}, (g, a)^{-1} \in H$. Now $(f, a)^{-1} = (f^{-1}, f^{-1}(a^{-1}))$, $(g, a)^{-1} = (g^{-1}, g^{-1}(b^{-1}))$ and $f^{-1}(a^{-1})f^{-1}(a) = g^{-1}(a^{-1})g^{-1}(a) = 1$ so $f^{-1} = g^{-1}$ thus $f = g$. Now we prove $\pi_2|_H$ is surjective. Take $a \in A$. Since H is regular there is $(f, x) \in H$ such that $xf(a) = 1$ so that $x = f(a^{-1})$. Consider $(f^{-1}, a) = (f, x)^{-1} \in H$. Then $\pi_2|_H(f^{-1}, a) = a$ and the claim follows. □

Definition

We say that two skew left brace $(A, \cdot, \circ), (B, \times, *)$ are isomorphic if there is $\phi : A \to B$ bijective such that $\forall\ a, b \in A$:

1. $\phi(ab) = \phi(a) \times \phi(b)$
2. $\phi(a \circ b) = \phi(a) * \phi(b)$

Constructing skew left brace

Theorem (Theorem 4.2, Proposition 4.3, [Guarnieri and Vendramin, 2016])

Let $(A, \cdot)$ *a finite group. Then the map:*

$$\{skew\ brace\ over\ (A, \cdot)\} \xrightarrow{\Phi} \{regular\ subgroup\ of\ Hol(A)\}$$

$$(A, \cdot, \circ) \mapsto \{(\lambda_a, a) : a \in A\}$$

is well defined with inverse:

$$\{regular\ subgroup\ of\ Hol(A)\} \xrightarrow{\Psi} \{skew\ brace\ over\ (A, \cdot)\}$$

$$H \mapsto (A, \cdot, \circ)$$

$$where\ a \circ b = af(b)\ and\ (\pi_2|_H)^{-1}(a) = (f, b)$$

Moreover $(A, \cdot, \circ) \simeq (A, \times, *) \iff \exists\ \phi \in Aut(A) : \phi\Phi((A, \cdot, \circ))\phi^{-1} = \Phi((A, \times, *))$

Constructing skew left brace

Sketch of the proof of Theorem 19.

We first prove the two maps are well defined. If $(A, \cdot, \circ)$ is a skew left brace and $a, b \in A$ we have: $(\lambda_a, a)(\lambda_b, b) = (\lambda_{a\circ b}, a\lambda_a(b)) = (\lambda_{a\circ b}, a \circ b)$ and $(\lambda_a, a)^{-1} = (\lambda_a^{-1}, \lambda_a^{-1}(a^{-1})) = (\lambda_{\overline{a}}, \overline{a})$ therefore $\{(\lambda_a, a) : a \in A\} \leq Hol(A)$. Morover take $a \in A$. Then $(\lambda_{\overline{a}}, \overline{a})$ satisfy $\overline{a}\lambda_{\overline{a}}(a) = 1$. Morover if (λ_b, b) satisy $b\lambda_b(a) = 1$ then $b = \overline{a}$. Thus $\{(\lambda_a, a) : a \in A\}$ is a regular subgroup of $Hol(A)$. Viceversa if $H \leq Hol(A)$ is a regular subgroup by Lemma 16 $\pi_2|_H$ is bijective so we can consider the group $(A, \circ)$ where for every $a, b \in A$ we have: $a \circ b = \pi_2|_H((\pi_2|_H)^{-1}(a)(\pi_2|_H)^{-1}(b) = af(b)$ where $(\pi_2|_H)^{-1} = (f, a)$. Note that $(A, \cdot, \circ)$ is a skew left braces since if $a, b, c \in A$ we have $a \circ (bc) = af(bc)af(b)f(c) = af(b)a^{-1}af(c) = (a \circ b)a^{-1}(a \circ c)$. The fact that they are the inverse of each oter is a simple calculation. Now if the skew left braces $(A, \cdot, \circ)$, $(A, \cdot, \times)$ are isomorphic through ϕ a straightforward calculation shows that $\{(\lambda_a, a) : a \in A\}$ is conjugate to $\{(\mu_a, a) : a \in A\}$ through ϕ, where $\mu_a : A \longrightarrow A, b \mapsto a^{-1}(a \times b)$. Viceversa if $H, K \leq Hol(A)$ are conjugate by an element ψ of $Aut(A)$ then ψ is an isomorphism between the skew left braces they determine. □

Constructing skew left brace

We are now ready to give an algorithm that will produce all skew left brace structure over a finite group A:

Algorithm [Algorithm 5.1, [Guarnieri and Vendramin, 2016]]

Let A be a finite group. To construct all skew left braces over A we proceed as follows:

1. Compute the holomorph $Hol(A)$ of A.
2. Compute the list of regular subgroup of $Hol(A)$ of order $|A|$ up to conjugation by elements of $Aut(A)$.
3. For each rappresentative H of regular subgroup of $Hol(A)$ construct the map $\rho : A \longrightarrow H, a \mapsto (f, f(a^{-1})) \in H$. The triple yields a skew left brace structure over A with multiplication given by $a \circ b = \rho^{-1}(\rho(a)\rho(b)) \ \forall \ a, b \in A$

To enumerate all skew left brace structures over A the third step of the algorithm is not needed. In [Guarnieri and Vendramin, 2016] called $c(n)$ the number of non-isomorphic skew left brace of order n. They compute $c(n)$ for some values of n. The number $c(32), c(64), c(81)$ and $c(96)$ are still unknown !. If one is interested in the classification of skew left brace of size pq with p, q primes can look at [Acri and Bonatto, 2020].

Skew Braces of χ-type

We now start the study of skew left braces by investigating the interplay between the underlying group structures. We start with the following:

Definition (Definition 1.1, [Cedó et al., 2018])

Let χ be a property of groups. A skew left brace $(A, \cdot, \circ)$ is said of χ-type if $(A, \cdot)$ is a χ-group.

We therefore can pose the general question:

Question: If $(A, \cdot, \circ)$ is a χ-type skew left brace, is $(A, \circ)$ a χ-group ?

In general this is not true. Indeed if $(A, \cdot, \circ)$ is a left brace, that is to say, $(A, \cdot)$ is abelian, the group $(A, \circ)$ doesn't need to be abelian as this example show.

Example (Example 1.4, [Guarnieri and Vendramin, 2016])

Let A, B two groups and $\alpha : A \longrightarrow Aut(B)$ an homomorphism. Then $(A \times B, \cdot, \circ)$ is a skew left brace where: $(a, b)(c, d) = (ac, bd), (a, b) \circ (c, d) = (ac, b\alpha(a)(d))$. Now consider A,B abelian such that there is $\alpha \in Hom(A, Aut(B)) : \alpha \neq 1$. Then $(A \times B,+,\circ)$ is of abelian type but $(A \times B, \circ)$ is not abelian.

Skew brace with Nilpotent additive group

Even if the answer is negative we can ask what is the influence of the χ-property to the group $(A, \circ)$. We can start with the following:
Question: If $(A, \cdot, \circ)$ is a finite nilpotent skew brace, is $(A, \circ)$ solvable ?
As we will see this kind of problem require a deep use of group theory. We recall some basic definitions:

Definition

A finite group G is said to be nilpotent if every p-sylow subgroup of G is normal.

For example finite abelian group are nilpotent. Moreover:

Definition

A finite group G is said to be solvable if there is a series of subgroup:
$1 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \ldots \trianglelefteq N_t \trianglelefteq G$ such that for every $i = 0, \ldots, t-1$ N_{i+1}/N_i is abelian.

Recall that nilpotent implies solvable but not viceversa.

Skew brace with Nilpotent additive group

The following is a milestone in group theory:

Theorem (Theorem 9.1.8, [Robinson, 1996])

Let G be a finite group. If for every prime p such that $p||G|$ there is $H \leq G$ such that $(|H|, p) = 1$ then G is solvable.

As a consequence we have the following:

Theorem (Corollary 1.23, [Smoktunowicz and Vendramin, 2018])

Let $(A, \cdot, \circ)$ be a nilpotent finite skew brace. Then $(A, \circ)$ is solvable.

Before proving the theorem let's see a property of skew left braces that will help us relax some notation:

Proposition

Let $(A, \cdot, \circ)$ be a skew left brace. Then $1_{(A,\cdot)} = 1_{(A,\circ)}$

Skew brace with Nilpotent additive group

Proof of Proposition 1.

Let $a \in A$ and $1 = 1_{(A,\cdot)}$ Then: $a \circ 1 = (a \circ 1)a^{-1}(a \circ 1)$ so $a \circ 1 = a = a \circ 1_{(A,\circ)}$ and therefore $1 = 1_{(A,\circ)}$. □

Proof of Theorem 25.

Let $p_1, \ldots, p_k$ the prime divisor of $|A|$ and P_j the p_j-sylow of $(A, \cdot)$ for $j \in \{1, \ldots, k\}$. We first prove that $(P_1, \circ) \leq (A, \circ)$. Let $a \in A$ and $b \in P_1$. Then $a \circ b = a\lambda_a(b)$ so it sufficient to show that $\lambda_a(b) \in P_1$. Suppose $|P_1| = p_1^{\alpha_1}$. Then $1 = \lambda_a(b^{p_1^{\alpha_1}}) = \lambda_a(b)^{p_1^{\alpha_1}}$ so $\lambda_a(b) \in P_1$. Therefore we have also that $\bar{a} = \lambda_a^{-1}(a^{-1}) \in P_1$. A little induction shows that $P_1 P_2 \ldots P_{j-1} P_{j+1} \ldots P_k \leq (A, \circ)$ and so the claim follows from [Theorem 9.1.8, [Robinson, 1996]] □

Other questions: Let A be a finite skew brace with nilpotent multiplicative group. Is the additive group solvable?

Finite skew brace with solvable additive group

The problem wether a finite solvable skew left brace has a solvable multiplicative group is still an open problem. In the infinite case this is not true (see [Example 3.2,[Nasybullov, 2018]]. In the finite case a lot of computation seems to show that the answer is affirmative. We want to give an affirmative answer of this question in a particular case. Again we will do strong use of group theory. Recall that if G is a group and $H \leq G$ we write "H char G", and say that H is a characteristic subgroup of G, if for every $\phi \in Aut(G)$ we have $\phi(H) \leq H$. Moreover we will denote with $G^{'}$ the commutator subgroup of G, that is to say:

$$G^{'} := \langle [g, h] := ghg^{-1}h^{-1} | g, h \in G \rangle$$

Recall that $G^{'}$ char G. We begin with the following:

Lemma (Lemma 2.1, [Smoktunowicz and Vendramin, 2018])

Let G be a finite group, p prime such that $p | [G : G^{'}]$. Then there is H char G such that $G/H \simeq (\mathbf{Z}_p)^n$ for some $n \in \mathbf{N}_{>0}$.

Finite skew brace with solvable additive group

We first begin with the following:

Lemma

Let G be a finite group and N char G. Let $N \leq H$ such that H/N char G/N, then H char G.

Proof.

Let $\phi \in Aut(G)$. We want to prove that $\phi(H) \leq H$. Consider the map

$$\psi_\phi : G/N \Longrightarrow G/N, gN \mapsto \phi(g)N$$

This is a well defined map since N char G and morover $\psi_\phi \in Aut(G/N)$. Therefore if $h \in H$ we get: $\psi_\phi(hN) \in H/N$ and so $\phi(h)N \in H/N$ which imply $\phi(h) \in H$. □

Finite skew brace with solvable additive group

Proof of Lemma 26.

Since $G/G^{'}$ is an abelian finite group we have that: $G/G^{'} \simeq \mathbf{Z}_{p^{\alpha_1}} \times \ldots \times \mathbf{Z}_{p^{\alpha_k}} \times A$ where α_i is a positive integer for every $i \in \{1, \ldots, k\}$ and A is the product of all the remaining q-sylow of $G/G^{'}$. Let $H/G^{'} = \mathbf{Z}_{p^{\alpha_1 - 1}} \times \ldots \times \mathbf{Z}_{p^{\alpha_k - 1}} \times A$. Then $H/G^{'}$ char $G/G^{'}$ since $H/G^{'}$ is a product of characteristic subgroup. Therefore, since $G^{'}$ char G by last lemma we get H char G with $G/H \simeq (G/G')/(H/G^{'}) \simeq (Z_p)^k$. □

The following theorem is a consequence of the classification of finite simple groups:

Theorem (Lemma 2, [Syskin, 1979])

Let G be a finite group whose order is not divisible by 3 and $G = AB$ where $A, B \leq G$ are solvable. Then G is solvable.

As a consequence we have the following:

Finite skew brace with solvable additive group

Theorem (Corollary 2.2, [Gorshkov and Nasybullov, 2020])

Let $(A, \cdot, \circ)$ a finite skew brace : $(A, \cdot)$ is solvable. If 3 dosen't divide $|A|$ then $(A, \circ)$ is solvable.

Proof.

Suppose the theorem is not true and let $(A, \cdot, \circ)$ a minimal counterexample (That is to say a counterexample with $|A|$ minimal). Since $(A, \cdot)$ is solvable the index $[(A, \cdot) : A^{'}] \neq 1$ so it is divisible by some prime p. By Lemma 26 there is H char $(A, \cdot)$ of index p^n. We first prove that $H \leq (A, \circ)$. Let $a, b \in H$. Since $\lambda_a \in Aut((A, \cdot))$ and H char $(A, \cdot)$ we have $\lambda_a(b) \in H$. Therefore $a \circ b = a\lambda_a(b) \in H$. Similarly $\overline{a} \in H$. Therefore $(H, \circ, \cdot)$ is a skew brace and we can assume H is not all A. Therefore by minimality we get that $(H, \circ)$ is solvable. Let P be a p-sylow of $(A, \circ)$. We have $([(A, \circ) : (H, \circ)], [(A, \circ), P]) = 1$ so $(A, \circ) = (H, \circ) \circ P$. Now $(H, \circ)$ and P are solvable, so the claim follows from Theorem 28. □

Two-sided skew brace

We want to present another case in which a solvable finite skew brace has solvable multiplicative group.

Definition

A skew brace $(A, \cdot, \circ)$ is said to be a *two-sided skew brace* if $\forall\ a, b, c \in A$ we have

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

For example a skew brace with abelian multiplicative group is a two-sided skew brace. A direct calculation shows that if $(A, \cdot, \circ)$ is a two-sided skew brace, for every $c \in A$ the map $\varphi_c : (A, \cdot) \longrightarrow (A, \cdot)$, $a \mapsto c \circ a \circ c^{-1}$ is an automorphism. We have the following:

Theorem (Theorem 4.3, [Nasybullov, 2019])

Let $(A, \cdot, \circ)$ a finite two-sided skew brace. If $(A, \cdot)$ is solvable, then $(A, \circ)$ is solvable.

Two-sided skew brace

Proof.

By contradiction suppose it is not true and let $(A, \cdot, \circ)$ be a minimal counterexample. As we have seen $(A, \cdot)$ cannot be abelian, so that $H \neq 1$ where H is the commutator subgroup of $(A, \cdot)$. Since H char $(A, \cdot)$ we have that $H \leq (A, \circ)$ so that $(H, \cdot, \circ)$ is a skew left brace. Therefore H is a solvable subgroup of $(A, \circ)$. Morover note that $H \trianglelefteq (A, \circ)$ since H char $(A, \cdot)$ and φ_c is an automorphism of $(A, \cdot)$ for every $c \in A$. Therefore we can consider the skew brace $(A/H, \cdot, \circ)$ where $A/H := \{aH \mid a \in A\}$ with the operations $(aH)(bH) = abH$ and $(aH) \circ (bH) = (a \circ b)H$. Again by minimality $(A/H, \circ)$ is solvable, so that $(A, \circ)$ is solvable. We got a contradiction so the theorem is proved. □

Remark

If $(A, \cdot, \circ)$ *is a skew brace, a subset* $I \subset A$ *such that* $I \trianglelefteq (A, \cdot), I \trianglelefteq (A, \circ)$ *and* $\lambda_a(I) \leq I \; \forall \; a \in A$ *is called an ideal of* A*. For every ideal* I *of* A *is well defined the skew brace* $(A/I, \cdot, \circ)$ *as defined in the previous proof.*

References

Acri, E. and Bonatto, M. (2020).
Skew braces of size pq.
Communications in Algebra, 48(5):1872–1881.

Bachiller, D., Cedo, F., and Jespers, E. (2015).
Solutions of the yang-baxter equation associated with a left brace.

Baxter, R. J. (1972).
Partition function of the eight-vertex lattice model.
Annals of Physics, 70(1):193–228.

Cedó, F., Smoktunowicz, A., and Vendramin, L. (2018).
Skew left braces of nilpotent type.
Proceedings of the London Mathematical Society, 118(6):1367–1392.

Gorshkov, I. and Nasybullov, T. (2020).
Finite skew braces with solvable additive group.

Guarnieri, L. and Vendramin, L. (2016).
Skew braces and the yang–baxter equation.
Mathematics of Computation, 86(307):2519–2534.

Nasybullov, T. (2018).
Connections between properties of the additive and the multiplicative groups of a two-sided skew brace.

Nasybullov, T. (2019).
Connections between properties of the additive and the multiplicative groups of a two-sided skew brace.
Journal of Algebra, 540:156–167.

Robinson, D. (1996).
A Course in the Theory of Groups.
Graduate Texts in Mathematics. Springer New York.

Smoktunowicz, A. and Vendramin, L. (2018).
On skew braces (with an appendix by n. byott and l. vendramin).
Journal of Combinatorial Algebra, 2(1):47–86.

Syskin, S. A. (1979).
A problem of R. Baer.
Sibirsk. Mat. Zh., 20(3):679–681, 696.

Vendramin, L. (2024).

Skew Braces: A Brief Survey, page 153–175.

Springer Nature Switzerland.

Yang, C. N. (1967).

Some exact results for the many-body problem in one dimension with repulsive delta-function interaction.

Phys. Rev. Lett., 19:1312–1315.

Thank you for your attention !