Skew left braces and 2-reductive solutions of the Yang–Baxter equation

Přemysl Jedlička
with Agata Pilitowska

Department of Mathematics
Faculty of Engineering (former Technical Faculty)
Czech University of Life Sciences (former Czech University of Agriculture) in Prague

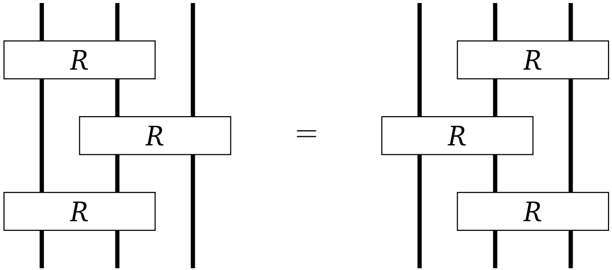
6th June 2023

Yang–Baxter equation

Definition

Let V be a vector space. A homomorphism $R: V \otimes V \to V \otimes V$ is called a *solution of Yang–Baxter equation* if it satisfies

$$(R \otimes \mathrm{id}_V)(\mathrm{id}_V \otimes R)(R \otimes \mathrm{id}_V) = (\mathrm{id}_V \otimes R)(R \otimes \mathrm{id}_V)(\mathrm{id}_V \otimes R).$$



Set-theoretic solutions

Definition

Let X be a set. A mapping $r : X \times X \to X \times X$ is called a *set-theoretic solution of Yang–Baxter equation* if it satisfies

$$(r \times \mathrm{id}_X)(\mathrm{id}_X \times r)(r \times \mathrm{id}_X) = (\mathrm{id}_X \times r)(r \times \mathrm{id}_X)(\mathrm{id}_X \times r).$$

A solution $r : (x,y) \mapsto (\sigma_x(y), \tau_y(x))$ is called *bijective* if r is a bijection. It is called *non-degenerate* if σ_x and τ_y are bijections, for all $x,y \in X$.

Involutive solutions

Observation

A structure (X,r) is a solution if and only if σ_x and τ_y are permutations, for all $x,y\in X$, satisfying

$$\sigma_x\sigma_y=\sigma_{\sigma_x(y)}\sigma_{\tau_y(x)}$$
$$\tau_{\sigma_{\tau_y(x)}(z)}\sigma_x(y)=\sigma_{\tau_{\sigma_y(z)}(x)}\tau_z(y)$$
$$\tau_x\tau_y=\tau_{\tau_x(y)}\tau_{\sigma_y(x)}$$

Definition

A solution is called *involutive* if $r^2=\mathrm{id}_{X^2}$.

Observation

If r is involutive then $\tau_y(x)=\sigma^{-1}_{\sigma_x(y)}(x)$.

Involutive solutions

Observation

A structure (X,r) *is a solution if and only if* σ_x *and* τ_y *are permutations, for all* $x,y \in X$*, satisfying*

$$\sigma_x\sigma_y = \sigma_{\sigma_x(y)}\sigma_{\tau_y(x)}$$

$$\tau_{\sigma_{\tau_y(x)}(z)}\sigma_x(y) = \sigma_{\tau_{\sigma_y(z)}(x)}\tau_z(y)$$

$$\tau_x\tau_y = \tau_{\tau_x(y)}\tau_{\sigma_y(x)}$$

Definition

A solution is called *involutive* if $r^2 = \mathrm{id}_{X^2}$.

Observation

If r *is involutive then* $\tau_y(x) = \sigma^{-1}_{\sigma_x(y)}(x)$.

Involutive solutions

Observation

A structure (X,r) is a solution if and only if σ_x and τ_y are permutations, for all $x,y \in X$, satisfying

$$\sigma_x\sigma_y = \sigma_{\sigma_x(y)}\sigma_{\tau_y(x)}$$

$$\tau_{\sigma_{\tau_y(x)}(z)}\sigma_x(y) = \sigma_{\tau_{\sigma_y(z)}(x)}\tau_z(y)$$

$$\tau_x\tau_y = \tau_{\tau_x(y)}\tau_{\sigma_y(x)}$$

Definition

A solution is called *involutive* if $r^2 = \mathrm{id}_{X^2}$.

Observation

If r is involutive then $\tau_y(x) = \sigma^{-1}_{\sigma_x(y)}(x)$.

Left braces

Definition (W. Rump)

A set B equipped with operations $+$ and $\circ$ is called a *left brace* if

- $(B, +)$ is an abelian group;
- $(B, \circ)$ is a group;
- for all $a, b, c \in B$, we have $a \circ (b + c) = a \circ b + a \circ c - a$.

Example

Let R be a ring and let $n \in J(R)$. Let

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

Then $(B, +, \circ)$ is a left brace.

Left braces

Definition (W. Rump)

A set B equipped with operations $+$ and $\circ$ is called a *left brace* if

- $(B,+)$ is an abelian group;
- $(B,\circ)$ is a group;
- for all $a,b,c\in B$, we have $a\circ(b+c)=a\circ b+a\circ c-a$.

Example

Let R be a ring and let $n\in J(R)$. Let

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

Then $(B,+,\circ)$ is a left brace.

Involutive solutions associated to left braces

Proposition

Let $(B, +, \circ)$ *be a left brace. The mapping* $\lambda : B \to \mathfrak{S}_B$ *defined by*

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

is a homomorphism $B \to \mathrm{Aut}(B, +)$.

Proposition

Let $(B, +, \circ)$ *be a left brace. If we define* $r : B^2 \to B^2$ *as*

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

then (B, r) *is an involutive solution.*

Involutive solutions associated to left braces

Proposition

Let $(B, +, \circ)$ *be a left brace. The mapping* $\lambda : B \to \mathfrak{S}_B$ *defined by*

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

is a homomorphism $B \to \mathrm{Aut}(B, +)$.

Proposition

Let $(B, +, \circ)$ *be a left brace. If we define* $r : B^2 \to B^2$ *as*

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

then (B, r) *is an involutive solution.*

Retracts of involutive solutions

Definition

Let (X, σ, τ) be an involutive solution. We define a relation $\sim$ on X

$$x \sim y \text{ if and only if } \sigma_x = \sigma_y.$$

The set $\{[x]_\sim \mid x \in X\}$ with operations

$$\sigma_{[x]_\sim}([y]_\sim) = [\sigma_x(y)]_\sim \qquad \text{and} \qquad \tau_{[y]_\sim}([x]_\sim) = [\tau_y(x)]_\sim$$

is called the *retract* of X and denoted by $\mathrm{Ret}(X)$.

Theorem (P. Etingof, T. Schedler, A. Soloviev)

Let (X, σ, τ) be an involutive solution. Then $\mathrm{Ret}(X)$ is a well-defined involutive solution.

Definition

We say that an involutive solution (X, σ, τ) has *multipermutation level k* if k is the smallest integer such that $|\mathrm{Ret}^k(X)| = 1$.

Retracts of involutive solutions

Definition

Let (X, σ, τ) be an involutive solution. We define a relation $\sim$ on X

$$x \sim y \text{ if and only if } \sigma_x = \sigma_y.$$

The set $\{[x]_\sim \mid x \in X\}$ with operations

$$\sigma_{[x]_\sim}([y]_\sim) = [\sigma_x(y)]_\sim \qquad \text{and} \qquad \tau_{[y]_\sim}([x]_\sim) = [\tau_y(x)]_\sim$$

is called the *retract* of X and denoted by $\mathrm{Ret}(X)$.

Theorem (P. Etingof, T. Schedler, A. Soloviev)

Let (X, σ, τ) be an involutive solution. Then $\mathrm{Ret}(X)$ is a well-defined involutive solution.

Definition

We say that an involutive solution (X, σ, τ) has *multipermutation level k* if k is the smallest integer such that $|\mathrm{Ret}^k(X)| = 1$.

Retracts of involutive solutions

Definition

Let (X,σ,τ) be an involutive solution. We define a relation $\sim$ on X

$$x \sim y \text{ if and only if } \sigma_x = \sigma_y.$$

The set $\{[x]_\sim \mid x \in X\}$ with operations

$$\sigma_{[x]_\sim}([y]_\sim) = [\sigma_x(y)]_\sim \qquad \text{and} \qquad \tau_{[y]_\sim}([x]_\sim) = [\tau_y(x)]_\sim$$

is called the *retract* of X and denoted by $\mathrm{Ret}(X)$.

Theorem (P. Etingof, T. Schedler, A. Soloviev)

Let (X,σ,τ) be an involutive solution. Then $\mathrm{Ret}(X)$ is a well-defined involutive solution.

Definition

We say that an involutive solution (X,σ,τ) has *multipermutation level k* if k is the smallest integer such that $|\mathrm{Ret}^k(X)| = 1$.

Retracts of involutive solutions

Definition

Let (X, σ, τ) be an involutive solution. We define a relation $\sim$ on X

$$x \sim y \text{ if and only if } \sigma_x = \sigma_y.$$

The set $\{[x]_\sim \mid x \in X\}$ with operations

$$\sigma_{[x]_\sim}([y]_\sim) = [\sigma_x(y)]_\sim \qquad \text{and} \qquad \tau_{[y]_\sim}([x]_\sim) = [\tau_y(x)]_\sim$$

is called the *retract* of X and denoted by $\mathrm{Ret}(X)$.

Theorem (P. Etingof, T. Schedler, A. Soloviev)

Let (X, σ, τ) be an involutive solution. Then $\mathrm{Ret}(X)$ is a well-defined involutive solution.

Definition

We say that an involutive solution (X, σ, τ) has *multipermutation level k* if k is the smallest integer such that $|\mathrm{Ret}^k(X)| = 1$.

Example on multipermutation level

Example

Let R be a commutative ring and let $n \in R$ be a nilpotent element of degree k. Then, when defining

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

we have

$$\lambda_a(c) = anc + c$$

and

$$a \sim b \text{ if and only if } na = nb.$$

Hence $\operatorname{Ret}(R) \cong nR$ and (R, r) is an involutive solution of multipermutation level k.

Ideals in left braces

Definition

A subset I of a left brace $(B, +, \circ)$ is called an *ideal* if I is a subgroup of $(B, +)$, I is a normal subgroup of $(B, \circ)$ and $\lambda_a(I) \subseteq I$, for each $a \in B$.

Definition

The set

$$\mathrm{Soc}(B) = \{s \in B \mid \forall a \in B \quad s + a = s \circ a\}$$

is an ideal of B called the *socle*.

Observation

$\mathrm{Soc}(B) = \mathrm{Ker}\,\lambda$

Ideals in left braces

Definition

A subset I of a left brace $(B, +, \circ)$ is called an *ideal* if I is a subgroup of $(B, +)$, I is a normal subgroup of $(B, \circ)$ and $\lambda_a(I) \subseteq I$, for each $a \in B$.

Definition

The set

$$\mathrm{Soc}(B) = \{s \in B \mid \forall a \in B \quad s + a = s \circ a\}$$

is an ideal of B called the *socle*.

Observation

$\mathrm{Soc}(B) = \mathrm{Ker}\,\lambda$

Ideals in left braces

Definition

A subset I of a left brace $(B, +, \circ)$ is called an *ideal* if I is a subgroup of $(B, +)$, I is a normal subgroup of $(B, \circ)$ and $\lambda_a(I) \subseteq I$, for each $a \in B$.

Definition

The set

$$\mathrm{Soc}(B) = \{s \in B \mid \forall a \in B \quad s + a = s \circ a\}$$

is an ideal of B called the *socle*.

Observation

$\mathrm{Soc}(B) = \mathrm{Ker}\,\lambda$

Nilpotency of left braces

Definition

Let $(B, +, \circ)$ be a left brace. We define

- $B_0 = B$,
- $B_{i+1} = B_i/\mathrm{Soc}(B_i)$, for $i \geqslant 0$.

We say that B is *nilpotent* of class k if k is the least integer such that $|B_k| = 1$.

Theorem (W. Rump)

A left brace $(B, +, \circ)$ is nilpotent of class k if and only if its associated solution has multipermutation level k

Nilpotency of left braces

Definition

Let $(B, +, \circ)$ be a left brace. We define

- $B_0 = B$,
- $B_{i+1} = B_i / \mathrm{Soc}(B_i)$, for $i \geqslant 0$.

We say that B is *nilpotent* of class k if k is the least integer such that $|B_k| = 1$.

Theorem (W. Rump)

A left brace $(B, +, \circ)$ is nilpotent of class k if and only if its associated solution has multipermutation level k

2-reductive solutions

Definition

We say that an involutive solution is 2-reductive if, for all $x, y, z \in X$, $\sigma_{\sigma_x(y)}(z) = \sigma_y(z)$.

Proposition (T. Gateva-Ivanova)

Let (X, σ, τ) be an involutive solution. Then the following conditions are equivalent:

- *X is 2-reductive,*
- *$\sigma_x \in \mathrm{Aut}(X)$, for each $x \in X$, i.e. $\sigma_x\sigma_y(z) = \sigma_{\sigma_x(y)}\sigma_x(z)$,*
- *X has multip. level at most 2 and, for all $x \in X$, $\tau_x = \sigma_x^{-1}$.*

Corollary

Let (X, σ, τ) be a 2-reductive involutive solution then $\sigma_x\sigma_y = \sigma_y\sigma_x$, for all $x, y \in X$.

2-reductive solutions

Definition

We say that an involutive solution is 2-reductive if, for all $x, y, z \in X$, $\sigma_{\sigma_x(y)}(z) = \sigma_y(z)$.

Proposition (T. Gateva-Ivanova)

Let (X, σ, τ) be an involutive solution. Then the following conditions are equivalent:

- *X is 2-reductive,*
- *$\sigma_x \in \mathrm{Aut}(X)$, for each $x \in X$, i.e. $\sigma_x\sigma_y(z) = \sigma_{\sigma_x(y)}\sigma_x(z)$,*
- *X has multip. level at most 2 and, for all $x \in X$, $\tau_x = \sigma_x^{-1}$.*

Corollary

Let (X, σ, τ) be a 2-reductive involutive solution then $\sigma_x\sigma_y = \sigma_y\sigma_x$, for all $x, y \in X$.

2-reductive solutions

Definition

We say that an involutive solution is 2-reductive if, for all $x, y, z \in X$, $\sigma_{\sigma_x(y)}(z) = \sigma_y(z)$.

Proposition (T. Gateva-Ivanova)

Let (X, σ, τ) be an involutive solution. Then the following conditions are equivalent:

- *X is 2-reductive,*
- *$\sigma_x \in \mathrm{Aut}(X)$, for each $x \in X$, i.e. $\sigma_x \sigma_y(z) = \sigma_{\sigma_x(y)} \sigma_x(z)$,*
- *X has multip. level at most 2 and, for all $x \in X$, $\tau_x = \sigma_x^{-1}$.*

Corollary

Let (X, σ, τ) be a 2-reductive involutive solution then $\sigma_x \sigma_y = \sigma_y \sigma_x$, for all $x, y \in X$.

2-reductive solutions

Definition

We say that an involutive solution is 2-reductive if, for all $x, y, z \in X$, $\sigma_{\sigma_x(y)}(z) = \sigma_y(z)$.

Proposition (T. Gateva-Ivanova)

Let (X, σ, τ) be an involutive solution. Then the following conditions are equivalent:

- *X is 2-reductive,*
- *$\sigma_x \in \mathrm{Aut}(X)$, for each $x \in X$, i.e. $\sigma_x\sigma_y(z) = \sigma_{\sigma_x(y)}\sigma_x(z)$,*
- *X has multip. level at most 2 and, for all $x \in X$, $\tau_x = \sigma_x^{-1}$.*

Corollary

Let (X, σ, τ) be a 2-reductive involutive solution then $\sigma_x\sigma_y = \sigma_y\sigma_x$, for all $x, y \in X$.

2-reductive solutions

Definition

We say that an involutive solution is 2-reductive if, for all $x, y, z \in X$, $\sigma_{\sigma_x(y)}(z) = \sigma_y(z)$.

Proposition (T. Gateva-Ivanova)

Let (X, σ, τ) be an involutive solution. Then the following conditions are equivalent:

- *X is 2-reductive,*
- *$\sigma_x \in \mathrm{Aut}(X)$, for each $x \in X$, i.e. $\sigma_x\sigma_y(z) = \sigma_{\sigma_x(y)}\sigma_x(z)$,*
- *X has multip. level at most 2 and, for all $x \in X$, $\tau_x = \sigma_x^{-1}$.*

Corollary

Let (X, σ, τ) be a 2-reductive involutive solution then $\sigma_x\sigma_y = \sigma_y\sigma_x$, for all $x, y \in X$.

2-reductive solutions

Definition

We say that an involutive solution is 2-reductive if, for all $x, y, z \in X$, $\sigma_{\sigma_x(y)}(z) = \sigma_y(z)$.

Proposition (T. Gateva-Ivanova)

Let (X, σ, τ) be an involutive solution. Then the following conditions are equivalent:

- *X is 2-reductive,*
- *$\sigma_x \in \mathrm{Aut}(X)$, for each $x \in X$, i.e. $\sigma_x\sigma_y(z) = \sigma_{\sigma_x(y)}\sigma_x(z)$,*
- *X has multip. level at most 2 and, for all $x \in X$, $\tau_x = \sigma_x^{-1}$.*

Corollary

Let (X, σ, τ) be a 2-reductive involutive solution then $\sigma_x\sigma_y = \sigma_y\sigma_x$, for all $x, y \in X$.

Construction of involutive 2-reductive solutions

Theorem (P. J., A. Pilitowska, A. Zamojska-Dzienio)

Let us have

- *an index set* I,
- *abelian groups* A_i, *for* $i \in I$,
- *a matrix of constants* $c_{i,j} \in A_j$, *for* $i, j \in I$.

Then the set $X = \bigsqcup_{i \in I} A_i$ *with operation* $\sigma : X \times X \to X$ *defined by*

$$\sigma_a(b) = b + c_{i,j}, \qquad \text{for } a \in A_i \text{ and } b \in A_j$$

is a 2-reductive involutive solution.
Conversely, every 2-reductive involutive solution can be obtained this way.

Corollary

Each abelian group is isomorphic to the permutation group of a 2-reductive involutive solution.

Construction of involutive 2-reductive solutions

Theorem (P. J., A. Pilitowska, A. Zamojska-Dzienio)

Let us have

- *an index set I,*
- *abelian groups A_i, for $i \in I$,*
- *a matrix of constants $c_{i,j} \in A_j$, for $i, j \in I$.*

Then the set $X = \bigsqcup_{i \in I} A_i$ with operation $\sigma : X \times X \to X$ defined by

$$\sigma_a(b) = b + c_{i,j}, \qquad \text{for } a \in A_i \text{ and } b \in A_j$$

is a 2-reductive involutive solution.
Conversely, every 2-reductive involutive solution can be obtained this way.

Corollary

Each abelian group is isomorphic to the permutation group of a 2-reductive involutive solution.

Numbers of 2-reductive solutions

n	1	2	3	4	5	6	7	8
involutive solutions	1	2	5	23	88	595	3456	34530
multip. level 2	1	2	5	19	70	359	2095	16332
2-reductive	1	2	5	17	65	323	1960	15421
mp level 2, not 2-red.	0	0	0	2	5	36	135	911

n	9	10	11
2-reductive	155889	2064688	35982357

n	12	13	14
2-reductive	832698007	25731050861	1067863092309

Left braces and 2-reductive solutions

Definition (L. Childs)

A left brace $(B, +, \cdot)$ is called a bi-left brace if

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

for all $a, b, c \in B$.

Theorem (L. Stefanello, S. Trappeniers)

Let $(B, +, \circ)$ be a left brace. Then its associated solution is 2-reductive if and only if B is a bi-left brace.

Left braces and 2-reductive solutions

Definition (L. Childs)

A left brace $(B, +, \cdot)$ is called a bi-left brace if

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

for all $a, b, c \in B$.

Theorem (L. Stefanello, S. Trappeniers)

Let $(B, +, \circ)$ be a left brace. Then its associated solution is 2-reductive if and only if B is a bi-left brace.

Retracts of non-involutive solutions

Definition

Let (X, σ, τ) be a solution. We define a relation $\sim$ on X as

$$x \sim y \text{ if and only if } \sigma_x = \sigma_y \text{ and } \tau_x = \tau_y.$$

The *retract* and the *multipermutation level* are defined analogously as in the involutive case.

Theorem

Let (X, σ, τ) be a solution. Then $\mathrm{Ret}(X)$ is a well-defined solution.

2019: V. Lebed, L. Vendramin: injective case
2019: P. J., A. Pilitowska, A. Zamojska-Dzienio: general case
2022: F. Cedó, E. Jespers, Ł. Kubat, A. Van Antwerpen, C. Verwimp: shorter proof

Retracts of non-involutive solutions

Definition

Let (X, σ, τ) be a solution. We define a relation $\sim$ on X as

$$x \sim y \text{ if and only if } \sigma_x = \sigma_y \text{ and } \tau_x = \tau_y.$$

The *retract* and the *multipermutation level* are defined analogously as in the involutive case.

Theorem

Let (X, σ, τ) be a solution. Then $\mathrm{Ret}(X)$ is a well-defined solution.

2019: V. Lebed, L. Vendramin: injective case
2019: P. J., A. Pilitowska, A. Zamojska-Dzienio: general case
2022: F. Cedó, E. Jespers, Ł. Kubat, A. Van Antwerpen, C. Verwimp: shorter proof

Retracts of non-involutive solutions

Definition

Let (X, σ, τ) be a solution. We define a relation $\sim$ on X as

$$x \sim y \text{ if and only if } \sigma_x = \sigma_y \text{ and } \tau_x = \tau_y.$$

The *retract* and the *multipermutation level* are defined analogously as in the involutive case.

Theorem

Let (X, σ, τ) *be a solution. Then* $\mathrm{Ret}(X)$ *is a well-defined solution.*

2019: V. Lebed, L. Vendramin: injective case
2019: P. J., A. Pilitowska, A. Zamojska-Dzienio: general case
2022: F. Cedó, E. Jespers, Ł. Kubat, A. Van Antwerpen, C. Verwimp: shorter proof

Retracts of non-involutive solutions

Definition

Let (X, σ, τ) be a solution. We define a relation $\sim$ on X as

$$x \sim y \text{ if and only if } \sigma_x = \sigma_y \text{ and } \tau_x = \tau_y.$$

The *retract* and the *multipermutation level* are defined analogously as in the involutive case.

Theorem

Let (X, σ, τ) *be a solution. Then* $\mathrm{Ret}(X)$ *is a well-defined solution.*

2019: V. Lebed, L. Vendramin: injective case
2019: P. J., A. Pilitowska, A. Zamojska-Dzienio: general case
2022: F. Cedó, E. Jespers, Ł. Kubat, A. Van Antwerpen, C. Verwimp: shorter proof

Non-involutive 2-reductive solutions

Definition

A solution (X, σ, τ) is called 2-*reductive*, if, for all $x, y \in X$,

- $\sigma_{\sigma_x(y)} = \sigma_y$,
- $\sigma_{\tau_y(x)} = \sigma_x$,
- $\tau_{\tau_y(x)} = \tau_x$,
- $\tau_{\sigma_x(y)} = \tau_y$.

Lemma

A 2-reductive solution is of multipermutation level 2 and the group generated by σ_x and τ_x is abelian.

Non-involutive 2-reductive solutions

Definition

A solution (X, σ, τ) is called 2-*reductive*, if, for all $x, y \in X$,

- $\sigma_{\sigma_x(y)} = \sigma_y$,
- $\sigma_{\tau_y(x)} = \sigma_x$,
- $\tau_{\tau_y(x)} = \tau_x$,
- $\tau_{\sigma_x(y)} = \tau_y$.

Lemma

A 2-reductive solution is of multipermutation level 2 and the group generated by σ_x and τ_x is abelian.

Construction of non-involutive 2-reductive solutions

Theorem (P. J., A. Pilitowska)

Let us have

- *an index set I,*
- *abelian groups A_i, for $i \in I$,*
- *two matrices of constants $c_{i,j}, d_{i,j} \in A_j$, for $i,j \in I$.*

Then the set $X = \bigsqcup_{i \in I} A_i$ with operations $\sigma : X \times X \to X$ and $\tau : X \times X \to X$ defined by

$$\sigma_a(b) = b + c_{i,j} \text{ and } \tau_b(a) = a + d_{j,i}, \quad \text{for } a \in A_i \text{ and } b \in A_j,$$

is a 2-reductive solution.
Conversely, every 2-reductive solution can be obtained this way.

Inverse solution

Observation

Let (X, r) be a solution. Then (X, r^{-1}) is also a solution, called the inverse *solution.*

We denote $r^{-1} = (\hat{\sigma}, \hat{\tau})$.

Proposition (P. J., A. Pilitowska)

Let (X, σ, τ) be a 2-reductive solution. Then the inverse solution $(X, \hat{\sigma}, \hat{\tau})$ is 2-reductive as well.

Proof.

Let $\sigma_a(b) = b + c_{i,j}$ and $\tau_b(a) = a + d_{j,i}$.
Then $\hat{\sigma}_a(b) = b - d_{i,j}$ and $\hat{\tau}_b(a) = a - c_{j,i}$. □

Inverse solution

Observation

Let (X, r) be a solution. Then (X, r^{-1}) is also a solution, called the inverse *solution.*

We denote $r^{-1} = (\hat{\sigma}, \hat{\tau})$.

Proposition (P. J., A. Pilitowska)

Let (X, σ, τ) be a 2-reductive solution. Then the inverse solution $(X, \hat{\sigma}, \hat{\tau})$ is 2-reductive as well.

Proof.

Let $\sigma_a(b) = b + c_{i,j}$ and $\tau_b(a) = a + d_{j,i}$.
Then $\hat{\sigma}_a(b) = b - d_{i,j}$ and $\hat{\tau}_b(a) = a - c_{j,i}$. □

Inverse solution

Observation

Let (X, r) be a solution. Then (X, r^{-1}) is also a solution, called the inverse *solution.*

We denote $r^{-1} = (\hat{\sigma}, \hat{\tau})$.

Proposition (P. J., A. Pilitowska)

Let (X, σ, τ) be a 2-reductive solution. Then the inverse solution $(X, \hat{\sigma}, \hat{\tau})$ is 2-reductive as well.

Proof.

Let $\sigma_a(b) = b + c_{i,j}$ and $\tau_b(a) = a + d_{j,i}$.
Then $\hat{\sigma}_a(b) = b - d_{i,j}$ and $\hat{\tau}_b(a) = a - c_{j,i}$. $\square$

Skew left braces

Definition (L. Guarnieri, L. Vendramin)

A set B equipped with operations $+$ and $\circ$ is called a *skew left brace* if

- $(B, +)$ is a group;
- $(B, \circ)$ is a group;
- for all $a, b, c \in B$, we have $a \circ (b + c) = a \circ b - a + a \circ c$.

Example

Let G be a group. Then $(G, +, +_{op})$ is a skew left brace.

Skew left braces

Definition (L. Guarnieri, L. Vendramin)

A set B equipped with operations $+$ and $\circ$ is called a *skew left brace* if

- $(B, +)$ is a group;
- $(B, \circ)$ is a group;
- for all $a, b, c \in B$, we have $a \circ (b + c) = a \circ b - a + a \circ c$.

Example

Let G be a group. Then $(G, +, +_{op})$ is a skew left brace.

Solutions associated to skew left braces

Proposition (L. Guarnieri, L. Vendramin)

Let $(B, +, \circ)$ be a skew left brace. The mapping $\lambda : B \to \mathfrak{S}_B$ defined by $\lambda_a(b) = -a + a \circ b$ is a homomorphism $B \to \mathrm{Aut}(B, +)$.

Proposition (D. Bachiller)

Let $(B, +, \circ)$ be a skew left brace. The mapping $\rho : B \to \mathfrak{S}_B$ defined by $\rho_b(a) = (\lambda_a(b))^{-1} \circ a \circ b$ is an anti-homomorphism, that means $\rho_{a \circ b} = \rho_b \rho_a$.

Proposition (L. Guarnieri, L. Vendramin)

Let $(B, +, \circ)$ be a left brace. If we define $r : B^2 \to B^2$ as

$$r(a, b) = (\lambda_a(b), \rho_b(a))$$

then (B, r) is a solution.

Solutions associated to skew left braces

Proposition (L. Guarnieri, L. Vendramin)

Let $(B,+,\circ)$ *be a skew left brace. The mapping* $\lambda : B \to \mathfrak{S}_B$ *defined by* $\lambda_a(b) = -a + a \circ b$ *is a homomorphism* $B \to \mathrm{Aut}(B,+)$.

Proposition (D. Bachiller)

Let $(B,+,\circ)$ *be a skew left brace. The mapping* $\rho : B \to \mathfrak{S}_B$ *defined by* $\rho_b(a) = (\lambda_a(b))^{-1} \circ a \circ b$ *is an anti-homomorphism, that means* $\rho_{a\circ b} = \rho_b \rho_a$.

Proposition (L. Guarnieri, L. Vendramin)

Let $(B,+,\circ)$ *be a left brace. If we define* $r : B^2 \to B^2$ *as*

$$r(a,b) = (\lambda_a(b), \rho_b(a))$$

then (B,r) *is a solution.*

Solutions associated to skew left braces

Proposition (L. Guarnieri, L. Vendramin)

Let $(B,+,\circ)$ be a skew left brace. The mapping $\lambda : B \to \mathfrak{S}_B$ defined by $\lambda_a(b) = -a + a \circ b$ is a homomorphism $B \to \mathrm{Aut}(B,+)$.

Proposition (D. Bachiller)

Let $(B,+,\circ)$ be a skew left brace. The mapping $\rho : B \to \mathfrak{S}_B$ defined by $\rho_b(a) = (\lambda_a(b))^{-1} \circ a \circ b$ is an anti-homomorphism, that means $\rho_{a\circ b} = \rho_b\rho_a$.

Proposition (L. Guarnieri, L. Vendramin)

Let $(B,+,\circ)$ be a left brace. If we define $r : B^2 \to B^2$ as

$$r(a,b) = (\lambda_a(b), \rho_b(a))$$

then (B,r) is a solution.

Ideals in skew left braces

Definition

A subset I of a skew left brace $(B, +, \circ)$ is called an *ideal* if I is a normal subgroup of $(B, +)$, I is a normal subgroup of $(B, \circ)$ and $\lambda_a(I) \subseteq I$, for each $a \in B$.

Definition

The set

$$\mathrm{Soc}(B) = \{s \in B \mid a + s = s + a = s \circ a\}$$

is an ideal of B called the *socle*.

Proposition (D. Bachiller)

$\mathrm{Soc}(B) = \mathrm{Ker}\,\lambda \cap \mathrm{Ker}\,\rho$

Ideals in skew left braces

Definition

A subset I of a skew left brace $(B, +, \circ)$ is called an *ideal* if I is a normal subgroup of $(B, +)$, I is a normal subgroup of $(B, \circ)$ and $\lambda_a(I) \subseteq I$, for each $a \in B$.

Definition

The set

$$\mathrm{Soc}(B) = \{s \in B \mid a + s = s + a = s \circ a\}$$

is an ideal of B called the *socle*.

Proposition (D. Bachiller)

$\mathrm{Soc}(B) = \mathrm{Ker}\,\lambda \cap \mathrm{Ker}\,\rho$

Ideals in skew left braces

Definition

A subset I of a skew left brace $(B, +, \circ)$ is called an *ideal* if I is a normal subgroup of $(B, +)$, I is a normal subgroup of $(B, \circ)$ and $\lambda_a(I) \subseteq I$, for each $a \in B$.

Definition

The set
$$\mathrm{Soc}(B) = \{s \in B \mid a + s = s + a = s \circ a\}$$
is an ideal of B called the *socle*.

Proposition (D. Bachiller)

$\mathrm{Soc}(B) = \mathrm{Ker}\,\lambda \cap \mathrm{Ker}\,\rho$

Nilpotency of left braces

Definition

Let $(B, +, \circ)$ be a skew left brace. We define

- $B_0 = B$,
- $B_{i+1} = B_i/\mathrm{Soc}(B_i)$, for $i \geqslant 0$.

We say that B is *nilpotent* of class k if k is the least integer such that $|B_k| = 1$.

Theorem (D. Bachiller)

A skew left brace $(B, +, \circ)$ is nilpotent of class k if and only if its associated solution has multipermutation level k

Nilpotency of left braces

Definition

Let $(B, +, \circ)$ be a skew left brace. We define

- $B_0 = B$,
- $B_{i+1} = B_i/\mathrm{Soc}(B_i)$, for $i \geqslant 0$.

We say that B is *nilpotent* of class k if k is the least integer such that $|B_k| = 1$.

Theorem (D. Bachiller)

A skew left brace $(B, +, \circ)$ is nilpotent of class k if and only if its associated solution has multipermutation level k

Opposite skew left braces

Definition (A. Koch, P. J. Truman)

Let $(B, +, \circ)$ be a skew left brace. Then $(B, +_{op}, \circ)$ is a skew left brace called the *opposite* skew left brace.

Theorem (A. Koch, P. J. Truman)

The solution associated to $(B, +_{op}, \circ)$ is inverse to the solution associated to $(B, +, \circ)$.

Corollary

- $\hat{\lambda}_a(b) = (a \circ b) - a,$
- $\hat{\rho}_b(a) = (\hat{\lambda}_a(b))^{-1} \circ a \circ b.$

Opposite skew left braces

Definition (A. Koch, P. J. Truman)

Let $(B, +, \circ)$ be a skew left brace. Then $(B, +_{op}, \circ)$ is a skew left brace called the *opposite* skew left brace.

Theorem (A. Koch, P. J. Truman)

The solution associated to $(B, +_{op}, \circ)$ is inverse to the solution associated to $(B, +, \circ)$.

Corollary

- $\hat{\lambda}_a(b) = (a \circ b) - a,$
- $\hat{\rho}_b(a) = (\hat{\lambda}_a(b))^{-1} \circ a \circ b.$

Opposite skew left braces

Definition (A. Koch, P. J. Truman)

Let $(B, +, \circ)$ be a skew left brace. Then $(B, +_{op}, \circ)$ is a skew left brace called the *opposite* skew left brace.

Theorem (A. Koch, P. J. Truman)

The solution associated to $(B, +_{op}, \circ)$ *is inverse to the solution associated to* $(B, +, \circ)$.

Corollary

- $\hat{\lambda}_a(b) = (a \circ b) - a,$
- $\hat{\rho}_b(a) = (\hat{\lambda}_a(b))^{-1} \circ a \circ b.$

Bi-skew left braces

Definition (L. Childs)

A skew left brace $(B, +, \circ)$ is called a bi-skew left brace if $(B, \circ, +)$ is a skew left brace as well.

Theorem (L. Stefanello, S. Trappeniers)

Let $(B, +, \circ)$ be a skew left brace. Then B is a bi-skew left brace if and only if

$$\lambda_{\hat{\lambda}_a(b)} = \lambda_b,$$

for each $a, b \in B$.

Theorem (A. Caranti)

A skew left brace $(B, +, \circ)$ is a bi-skew left brace if and only if λ is an anti-homomorphism of $(B, +)$, i.e. $\lambda_{a+b} = \lambda_b \lambda_a$.

Bi-skew left braces

Definition (L. Childs)

A skew left brace $(B, +, \circ)$ is called a bi-skew left brace if $(B, \circ, +)$ is a skew left brace as well.

Theorem (L. Stefanello, S. Trappeniers)

Let $(B, +, \circ)$ be a skew left brace. Then B is a bi-skew left brace if and only if

$$\lambda_{\hat{\lambda}_a(b)} = \lambda_b,$$

for each $a, b \in B$.

Theorem (A. Caranti)

A skew left brace $(B, +, \circ)$ is a bi-skew left brace if and only if λ is an anti-homomorphism of $(B, +)$, i.e. $\lambda_{a+b} = \lambda_b \lambda_a$.

Bi-skew left braces

Definition (L. Childs)

A skew left brace $(B, +, \circ)$ is called a bi-skew left brace if $(B, \circ, +)$ is a skew left brace as well.

Theorem (L. Stefanello, S. Trappeniers)

Let $(B, +, \circ)$ be a skew left brace. Then B is a bi-skew left brace if and only if

$$\lambda_{\hat{\lambda}_a(b)} = \lambda_b,$$

for each $a, b \in B$.

Theorem (A. Caranti)

A skew left brace $(B, +, \circ)$ is a bi-skew left brace if and only if λ is an anti-homomorphism of $(B, +)$, i.e. $\lambda_{a+b} = \lambda_b \lambda_a$.

Distributive solutions

Theorem (P. J., A. Pilitowska)

Let (X, σ, τ) be a solution. TFAE:

- $\sigma_{\hat{\sigma}_x(y)} = \sigma_y$,
- $\sigma_{\tau_x(y)} = \sigma_y$,
- $\sigma_x\sigma_y = \sigma_{\sigma_x(y)}\sigma_x$,
- $\hat{\tau}_x = \sigma_x^{-1}$,
- $\sigma_x \in \mathrm{Aut}(X)$,

for all $x, y \in X$.

Corollary

Let $(B, +, \circ)$ be a skew left brace. TFAE:

- *B is a bi-skew left brace,*
- $\lambda_{a+b} = \lambda_b\lambda_a$,
- $\lambda_{\hat{\lambda}_a(b)} = \lambda_b$,
- $\lambda_{\rho_a(b)} = \lambda_b$,
- $\lambda_a\lambda_b = \lambda_{\lambda_a(b)}\lambda_a$,
- $\hat{\rho}_a = \lambda_a^{-1}$,
- $\lambda_a \in \mathrm{Aut}(B)$,

for all $a, b \in B$.

Distributive solutions

Theorem (P. J., A. Pilitowska)

Let (X, σ, τ) be a solution. TFAE:

- $\sigma_{\hat{\sigma}_x(y)} = \sigma_y$,
- $\sigma_{\tau_x(y)} = \sigma_y$,
- $\sigma_x\sigma_y = \sigma_{\sigma_x(y)}\sigma_x$,
- $\hat{\tau}_x = \sigma_x^{-1}$,
- $\sigma_x \in \mathrm{Aut}(X)$,

for all $x, y \in X$.

Corollary

Let $(B, +, \circ)$ be a skew left brace. TFAE:

- *B is a bi-skew left brace,*
- $\lambda_{a+b} = \lambda_b\lambda_a$,
- $\lambda_{\hat{\lambda}_a(b)} = \lambda_b$,
- $\lambda_{\rho_a(b)} = \lambda_b$,
- $\lambda_a\lambda_b = \lambda_{\lambda_a(b)}\lambda_a$,
- $\hat{\rho}_a = \lambda_a^{-1}$,
- $\lambda_a \in \mathrm{Aut}(B)$,

for all $a, b \in B$.

Equations of 2-reductivity and skew braces

Proposition (P. J., A. Pilitowska)

Let $(B, +, \circ)$ be a skew left brace. Then

- $\lambda_{\lambda_a(b)} = \lambda_b$ *if and only if* λ *is a homomorphism* $(B, +) \to \mathrm{Aut}(B, \circ)$*, that means* $\lambda_{a+b} = \lambda_a\lambda_b$*;*
- $\lambda_{\rho_a(b)} = \lambda_b$ *if and only if* λ *is an anti-homomorphism* $(B, +) \to \mathrm{Aut}(B, \circ)$*, that means* $\lambda_{a+b} = \lambda_b\lambda_a$*;*
- $\rho_{\rho_a(b)} = \rho_b$ *if and only if* ρ *is a homomorphism* $(B, +) \to \mathfrak{S}_X$*, that means* $\rho_{a+b} = \rho_a\rho_b$*;*
- $\rho_{\lambda_a(b)} = \rho_b$ *if and only if* ρ *is an anti-homomorphism* $(B, +) \to \mathrm{Aut}(B, \circ)$*, that means* $\rho_{a+b} = \rho_b\rho_a$.

Skew left braces and 2-reductivity

Theorem (P. J., A. Pilitowska)

Let $(B, +, \circ)$ be a skew left brace. TFAE

- *the solution (B, λ, ρ) is 2-reductive,*
- $\lambda_{a+b} = \lambda_{b+a} = \lambda_a \lambda_b$ *and* $\rho_{a+b} = \rho_{b+a} = \rho_a \rho_b$,
- (B, λ, ρ) *has multipermutation level at most 2,*
- $(B, +, \circ)$ *is nilpotent of degree at most 2,*
- $(B, +_{op}, \circ)$ *is nilpotent of degree at most 2.*