Biracks and their applications – Part III

Braces and biracks

Přemysl Jedlička
with Agata Pilitowska and Anna Zamojska-Dzienio

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

Będlewo 27th June 2023

Faculty of Engineering

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

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 radical ring. Let $a \circ b = a + a * b + b$. Then $(B, +, \circ)$ is a left brace.

Example

Let $(R, +, \cdot)$ be a commutative ring and let $n \in \mathrm{nil}(R)$. Let $a * b = anr$. Then $(R, +, *)$ is a commutative radical ring.

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 radical ring. Let $a \circ b = a + a * b + b$. Then $(B, +, \circ)$ is a left brace.

Example

Let $(R, +, \cdot)$ be a commutative ring and let $n \in \mathrm{nil}(R)$. Let $a * b = anr$. Then $(R, +, *)$ is a commutative radical ring.

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 radical ring. Let $a \circ b = a + a * b + b$. Then $(B, +, \circ)$ is a left brace.

Example

Let $(R, +, \cdot)$ be a commutative ring and let $n \in \mathrm{nil}(R)$. Let $a * b = anr$. Then $(R, +, *)$ is a commutative radical ring.

Two-sided braces

Definition

A left brace is called *two-sided* if $(a+b)\circ c = a\circ c + b\circ c - c$.

Example

Let $\circ$ be commutative. Then the left brace is two-sided.

Proposition (W. Rump)

Let $(B,+,\circ)$ be a two-sided brace. Let $a*b = a\circ b - a - b$. Then $(R,+,*)$ is a radical ring.
Moreover, if B is finite then

$$B = \prod_{p \text{ prime}} B_p,$$

where $B_p = \{b \in B \mid \exists m \in \mathbb{N} : p^m b = 0\}$.

Two-sided braces

Definition

A left brace is called *two-sided* if $(a+b)\circ c = a\circ c + b\circ c - c$.

Example

Let $\circ$ be commutative. Then the left brace is two-sided.

Proposition (W. Rump)

Let $(B,+,\circ)$ be a two-sided brace. Let $a*b = a\circ b - a - b$. Then $(R,+,*)$ is a radical ring.
Moreover, if B is finite then

$$B = \prod_{p \text{ prime}} B_p,$$

where $B_p = \{b \in B \mid \exists m \in \mathbb{N} : p^m b = 0\}$.

Semidirect product

Definitions

Let $(A, +_A, \circ_A)$ and $(B, +_B, \circ_B)$ are two left braces. An *action* of B on A is a homomorphism $\phi : (B, \circ_B) \to \mathrm{Aut}(A)$.

The *semidirect product* $A \rtimes_\phi B$ is defined as follows:

$$(a_1, b_1) + (a_2, b_2) = (a_1 +_A a_2, b_1 +_B b_2),$$
$$(a_1, b_1) \circ (b_2, b_2) = (a_1 \circ_A \phi(b_1)(a_2), b_1 \circ_B b_2)$$

Homomorphism λ

Proposition

Let $(B, +, \circ)$ be a left brace. The mapping $\lambda : B \to B^B$ defined by

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

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

Proof.

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

$$\lambda_a^{-1}(b) = a^{-1} \circ (a + b)$$

$$\lambda_{a \circ b}(c) = \lambda_a \lambda_b(c)$$

□

Homomorphism λ

Proposition

Let $(B,+,\circ)$ *be a left brace. The mapping* $\lambda : B \to B^B$ *defined by*

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

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

Proof.

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

□

Cohomology

Observation

Let $(B,+,\circ)$ be a left brace. The action λ turns $(B,+)$ into a left $(B,\circ)$-module such that the identity is a 1-cocycle.

On the other hand, if we have a group G, a left G-module M and a bijective 1-cocycle $\phi : G \to M$ then, by defining

$$a+b=\phi^{-1}(\phi(a)+\phi(b))$$

we obtain a left brace.

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 $a \in B$.

Observation

Ideals of left braces correspond to homomorphism pre-images of 0. On the other hand, every endomorphism is determined by its kernel.

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 $a \in B$.

Observation

Ideals of left braces correspond to homomorphism pre-images of 0*. On the other hand, every endomorphism is determined by its kernel.*

Socle

Definition

The set

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

is an ideal of B called the *socle*.

Observation

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

Observation

If $\circ$ *is commutative then* $\mathrm{Soc}(B, +, \circ) = \mathrm{Ann}(B, +, *)$.

Socle

Definition

The set

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

is an ideal of B called the *socle*.

Observation

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

Observation

If $\circ$ is commutative then $\mathrm{Soc}(B, +, \circ) = \mathrm{Ann}(B, +, *)$.

Socle

Definition

The set

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

is an ideal of B called the *socle*.

Observation

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

Observation

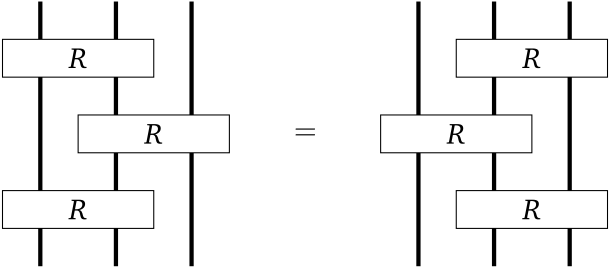
If $\circ$ *is commutative then* $\mathrm{Soc}(B, +, \circ) = \mathrm{Ann}(B, +, *)$.

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

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



Biracks

Definition

An algebra $(B, \triangleleft, \triangleright)$ is called a *birack* if

- $(X, \triangleleft)$ is a left quasigroup,
- $(X, \triangleright)$ is a right quasigroup,
- the mapping $r : (x, y) \mapsto (x \triangleleft y, x \triangleright y)$ is bijective,
- the mapping r satisfies

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

Definition

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

Biracks

Definition

An algebra $(B, \triangleleft, \triangleright)$ is called a *birack* if

- $(X, \triangleleft)$ is a left quasigroup,
- $(X, \triangleright)$ is a right quasigroup,
- the mapping $r : (x, y) \mapsto (x \triangleleft y, x \triangleright y)$ is bijective,
- the mapping r satisfies

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

Definition

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

Involutive biracks associated to left braces

Proposition

Let $(B, +, \circ)$ *be a left brace. If we define* $\triangleleft$ *and* $\triangleright$ *as*

$$a \triangleleft b = \lambda_a(b)$$
$$a \triangleright b = \lambda^{-1}_{\lambda_a(b)}(a)$$

then $(B, \triangleleft, \triangleright)$ *is an involutive birack.*

Proof.

$\lambda_{\lambda_a(b)}\lambda_{\lambda^{-1}_{\lambda_a(b)}(a))} = \lambda_{\lambda_a(b)\circ\lambda^{-1}_{\lambda_a(b)}(a)} = \lambda_{\lambda_a(b)\circ(\lambda_a(b))^{-1}\circ(\lambda_a(b)+a)} = \lambda_{(a\circ b)-a+a} = \lambda_{a\circ b} = \lambda_a\lambda_b$ □

Involutive biracks associated to left braces

Proposition

Let $(B,+,\circ)$ *be a left brace. If we define* $\triangleleft$ *and* $\triangleright$ *as*

$$a \triangleleft b = \lambda_a(b)$$
$$a \triangleright b = \lambda^{-1}_{\lambda_a(b)}(a)$$

then $(B,\triangleleft,\triangleright)$ *is an involutive birack.*

Proof.

$\lambda_{\lambda_a(b)}\lambda_{\lambda^{-1}_{\lambda_a(b)}(a))} = \lambda_{\lambda_a(b)\circ\lambda^{-1}_{\lambda_a(b)}(a)} = \lambda_{\lambda_a(b)\circ(\lambda_a(b))^{-1}\circ(\lambda_a(b)+a)} = \lambda_{(a\circ b)-a+a} = \lambda_{a\circ b} = \lambda_a\lambda_b$ □

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 birack has multipermutation level k

Proof.

$x \sim y \iff \lambda_x = \lambda_y \iff \lambda_{x \circ y^{-1}} = \mathrm{id} \iff x \circ y^{-1} \in \mathrm{Soc}(B)$ □

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 birack has multipermutation level k

Proof.

$$x \sim y \Leftrightarrow \lambda_x = \lambda_y \Leftrightarrow \lambda_{x \circ y^{-1}} = \mathrm{id} \Leftrightarrow x \circ y^{-1} \in \mathrm{Soc}(B)$$

□

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 birack has multipermutation level k

Proof.

$$x \sim y \;\Leftrightarrow\; \lambda_x = \lambda_y \;\Leftrightarrow\; \lambda_{x \circ y^{-1}} = \mathrm{id} \;\Leftrightarrow\; x \circ y^{-1} \in \mathrm{Soc}(B)$$

□

Structure group

Definition

Let $(X, \triangleleft, \triangleright)$ be a finite involutive birack. The infinite group with the presentation

$$G_X = \langle X \mid x \circ y = (x \triangleleft y) \circ (x \triangleright y) \rangle$$

is called the *structure group* of the birack X.

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

Let $(X, \triangleleft, \triangleright)$ be a finite involutive birack. Then there exists a unique free abelian group operation $+$ on the set G_X such that $(G_X, +, \circ)$ is a left brace and $\lambda_x(y) = x \triangleleft y$, for all $x, y \in X$. In particular, $(X, \triangleleft, \triangleright)$ embeds into the birack associated to G_X.

Structure group

Definition

Let $(X, \triangleleft, \triangleright)$ be a finite involutive birack. The infinite group with the presentation

$$G_X = \langle X \mid x \circ y = (x \triangleleft y) \circ (x \triangleright y) \rangle$$

is called the *structure group* of the birack X.

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

Let $(X, \triangleleft, \triangleright)$ be a finite involutive birack. Then there exists a unique free abelian group operation $+$ on the set G_X such that $(G_X, +, \circ)$ is a left brace and $\lambda_x(y) = x \triangleleft y$, for all $x, y \in X$. In particular, $(X, \triangleleft, \triangleright)$ embeds into the birack associated to G_X.

Representation of the structure group

Theorem (E. Acri, R. Lutowski, L. Vendramin)

Let X be an involutive birack of size $n \in \mathbb{N}$. Then G_X embeds into $\mathbf{GL}(n+1, \mathbb{Z})$.

Suppose $X = \{x_1, x_2, \ldots, x_n\}$.
For each $a \in G_X$, let A_a be the permutation matrix of the permutation $\lambda_a|_X$ and let $\vec{c}_a$ be such that $a = \sum (c_a)_i x_i$.
We associate to a the matrix $\begin{pmatrix} A_a & \vec{c}_a^T \\ \vec{0} & 1 \end{pmatrix} \in \mathbf{GL}(n+1, \mathbb{Z})$

Proof.
Use $\lambda_a(b) = \sum (A_a \cdot \vec{c}_b^T)_i x_i$ and $a \circ b = a + \lambda_a(b)$. □

Representation of the structure group

Theorem (E. Acri, R. Lutowski, L. Vendramin)

Let X be an involutive birack of size $n \in \mathbb{N}$. Then G_X embeds into $\mathbf{GL}(n+1, \mathbb{Z})$.

Suppose $X = \{x_1, x_2, \dots, x_n\}$.
For each $a \in G_X$, let A_a be the permutation matrix of the permutation $\lambda_a|_X$ and let $\vec{c}_a$ be such that $a = \sum (c_a)_i x_i$.

We associate to a the matrix $\begin{pmatrix} A_a & \vec{c}_a^{\,T} \\ \vec{0} & 1 \end{pmatrix} \in \mathbf{GL}(n+1, \mathbb{Z})$

Proof.

Use $\lambda_a(b) = \sum (A_a \cdot \vec{c}_b^{\,T})_i x_i$ and $a \circ b = a + \lambda_a(b)$. □

Representation of the structure group

Theorem (E. Acri, R. Lutowski, L. Vendramin)

Let X be an involutive birack of size $n \in \mathbb{N}$. Then G_X embeds into $\mathbf{GL}(n+1,\mathbb{Z})$.

Suppose $X = \{x_1, x_2, \dots, x_n\}$.
For each $a \in G_X$, let A_a be the permutation matrix of the permutation $\lambda_a|_X$ and let $\vec{c}_a$ be such that $a = \sum (c_a)_i x_i$.
We associate to a the matrix $\begin{pmatrix} A_a & \vec{c}_a^T \\ \vec{0} & 1 \end{pmatrix} \in \mathbf{GL}(n+1,\mathbb{Z})$

Proof.

Use $\lambda_a(b) = \sum (A_a \cdot \vec{c}_b^T)_i x_i$ and $a \circ b = a + \lambda_a(b)$. □

Projection to the multiplication group

Definition

Let (X, r) be an involutive birack. The group

$$\mathrm{Mlt}(X) = \langle L_x \mid x \in X \rangle = \langle L_x, \mathbf{R}_x \mid x \in X \rangle,$$

where $L_x(y) = x \triangleleft y$ and $\mathbf{R}_x(y) = y \triangleright x$, is called the *multiplication* group or the *permutation group* or the *Yang-Baxter group* of $(X, \triangleleft, \triangleright)$.

Let $\pi : G_X \to \mathrm{Mlt}(X)$ send x to L_x. This mapping extends to a homomorphism of groups since $L_x L_y = L_{x \triangleleft y} L_{x \triangleright y}$.

λ_x restricted to X is equal to L_x.

$\lambda_{x_1 \circ x_2 \circ \cdots \circ x_k}$ restricted to X is equal to $L_{x_1} L_{x_2} \cdots L_{x_k}$.

λ_a restricted to X is equal to $\pi(a)$.

$a \in \operatorname{Ker} \lambda \iff \lambda_a$ is the identity $\iff \lambda_a$ is the identity on $X \iff$ $\pi(a)$ is the identity $\iff a \in \operatorname{Ker} \pi$

Projection to the multiplication group

Definition

Let (X, r) be an involutive birack. The group

$$\mathrm{Mlt}(X) = \langle L_x \mid x \in X\rangle = \langle L_x, \mathbf{R}_x \mid x \in X\rangle,$$

where $L_x(y) = x \triangleleft y$ and $\mathbf{R}_x(y) = y \triangleright x$, is called the *multiplication group* or the *permutation group* or the *Yang-Baxter group* of $(X, \triangleleft, \triangleright)$.

Let $\pi : G_X \to \mathrm{Mlt}(X)$ send x to L_x. This mapping extends to a homomorphism of groups since $L_x L_y = L_{x \triangleleft y} L_{x \triangleright y}$.

λ_x restricted to X is equal to L_x.

$\lambda_{x_1 \circ x_2 \circ \cdots \circ x_k}$ restricted to X is equal to $L_{x_1} L_{x_2} \cdots L_{x_k}$.

λ_a restricted to X is equal to $\pi(a)$.

$a \in \operatorname{Ker} \lambda \iff \lambda_a$ is the identity $\iff \lambda_a$ is the identity on $X \iff \pi(a)$ is the identity $\iff a \in \operatorname{Ker} \pi$

Projection to the multiplication group

Definition

Let (X, r) be an involutive birack. The group

$$\mathrm{Mlt}(X) = \langle L_x \mid x \in X \rangle = \langle L_x, \mathbf{R}_x \mid x \in X \rangle,$$

where $L_x(y) = x \triangleleft y$ and $\mathbf{R}_x(y) = y \triangleright x$, is called the *multiplication group* or the *permutation group* or the *Yang-Baxter group* of $(X, \triangleleft, \triangleright)$.

Let $\pi : G_X \to \mathrm{Mlt}(X)$ send x to L_x. This mapping extends to a homomorphism of groups since $L_x L_y = L_{x \triangleleft y} L_{x \triangleright y}$.
λ_x restricted to X is equal to L_x.
$\lambda_{x_1 \circ x_2 \circ \cdots \circ x_k}$ restricted to X is equal to $L_{x_1} L_{x_2} \cdots L_{x_k}$.
λ_a restricted to X is equal to $\pi(a)$.
$a \in \operatorname{Ker} \lambda \iff \lambda_a$ is the identity $\iff \lambda_a$ is the identity on $X \iff \pi(a)$ is the identity $\iff a \in \operatorname{Ker} \pi$

Projection to the multiplication group

Definition

Let (X, r) be an involutive birack. The group

$$\mathrm{Mlt}(X) = \langle L_x \mid x \in X \rangle = \langle L_x, \mathbf{R}_x \mid x \in X \rangle,$$

where $L_x(y) = x \triangleleft y$ and $\mathbf{R}_x(y) = y \triangleright x$, is called the *multiplication group* or the *permutation group* or the *Yang-Baxter group* of $(X, \triangleleft, \triangleright)$.

Let $\pi : G_X \to \mathrm{Mlt}(X)$ send x to L_x. This mapping extends to a homomorphism of groups since $L_x L_y = L_{x \triangleleft y} L_{x \triangleright y}$.
λ_x restricted to X is equal to L_x.
$\lambda_{x_1 \circ x_2 \circ \cdots \circ x_k}$ restricted to X is equal to $L_{x_1} L_{x_2} \cdots L_{x_k}$.
λ_a restricted to X is equal to $\pi(a)$.
$a \in \operatorname{Ker} \lambda \iff \lambda_a$ is the identity $\iff \lambda_a$ is the identity on $X \iff \pi(a)$ is the identity $\iff a \in \operatorname{Ker} \pi$

Projection to the multiplication group

Definition

Let (X, r) be an involutive birack. The group

$$\mathrm{Mlt}(X) = \langle L_x \mid x \in X \rangle = \langle L_x, \mathbf{R}_x \mid x \in X \rangle,$$

where $L_x(y) = x \triangleleft y$ and $\mathbf{R}_x(y) = y \triangleright x$, is called the *multiplication group* or the *permutation group* or the *Yang-Baxter group* of $(X, \triangleleft, \triangleright)$.

Let $\pi : G_X \to \mathrm{Mlt}(X)$ send x to L_x. This mapping extends to a homomorphism of groups since $L_x L_y = L_{x \triangleleft y} L_{x \triangleright y}$.
λ_x restricted to X is equal to L_x.
$\lambda_{x_1 \circ x_2 \circ \cdots \circ x_k}$ restricted to X is equal to $L_{x_1} L_{x_2} \cdots L_{x_k}$.
λ_a restricted to X is equal to $\pi(a)$.
$a \in \operatorname{Ker} \lambda \iff \lambda_a$ is the identity $\iff \lambda_a$ is the identity on $X \iff \pi(a)$ is the identity $\iff a \in \operatorname{Ker} \pi$

Projection to the multiplication group

Definition

Let (X, r) be an involutive birack. The group

$$\mathrm{Mlt}(X) = \langle L_x \mid x \in X \rangle = \langle L_x, \mathbf{R}_x \mid x \in X \rangle,$$

where $L_x(y) = x \triangleleft y$ and $\mathbf{R}_x(y) = y \triangleright x$, is called the *multiplication group* or the *permutation group* or the *Yang-Baxter group* of $(X, \triangleleft, \triangleright)$.

Let $\pi : G_X \to \mathrm{Mlt}(X)$ send x to L_x. This mapping extends to a homomorphism of groups since $L_x L_y = L_{x \triangleleft y} L_{x \triangleright y}$.

λ_x restricted to X is equal to L_x.

$\lambda_{x_1 \circ x_2 \circ \cdots \circ x_k}$ restricted to X is equal to $L_{x_1} L_{x_2} \cdots L_{x_k}$.

λ_a restricted to X is equal to $\pi(a)$.

$a \in \operatorname{Ker} \lambda \iff \lambda_a$ is the identity $\iff \lambda_a$ is the identity on $X \iff \pi(a)$ is the identity $\iff a \in \operatorname{Ker} \pi$

Multiplication left brace

Definition

The *multiplication left brace* is the quotient left brace $G_X/\mathrm{Soc}(G_X)$.

Observation

Since $\mathrm{Soc}(G_X) = \mathrm{Ker}\,\lambda$, *the quotient can be viewed as the projection* π *of* G_X *onto* $\mathrm{Mlt}(X)$. *Hence it is usual to consider* $G_X/\mathrm{Soc}(G_X) \cong \mathrm{Mlt}(X)$.

$\pi(x) = L_x$

Since $\lambda_x(y) = L_x(y)$, we have $\pi(\lambda_x(y)) = \pi(L_x(y)) = L_{L_x(y)}$.

Since λ is a homomorphism we have $\pi(\lambda_a(y)) = L_{\pi(a)(y)}$.

Now $a + x = a \circ (a^{-1} \circ (a + x)) = a \circ \lambda_a^{-1}(x)$ and hence $\pi(a + x) = \pi(a)L_{\pi(a)^{-1}(x)}$.

Multiplication left brace

Definition

The *multiplication left brace* is the quotient left brace $G_X/\mathrm{Soc}(G_X)$.

Observation

Since $\mathrm{Soc}(G_X) = \mathrm{Ker}\,\lambda$*, the quotient can be viewed as the projection* π *of* G_X *onto* $\mathrm{Mlt}(X)$*. Hence it is usual to consider* $G_X/\mathrm{Soc}(G_X) \cong \mathrm{Mlt}(X)$.

$\pi(x) = L_x$

Since $\lambda_x(y) = L_x(y)$, we have $\pi(\lambda_x(y)) = \pi(L_x(y)) = L_{L_x(y)}$.

Since λ is a homomorphism we have $\pi(\lambda_a(y)) = L_{\pi(a)(y)}$.

Now $a + x = a \circ (a^{-1} \circ (a + x)) = a \circ \lambda_a^{-1}(x)$ and hence $\pi(a + x) = \pi(a)L_{\pi(a)^{-1}(x)}$.

Multiplication left brace

Definition

The *multiplication left brace* is the quotient left brace $G_X/\mathrm{Soc}(G_X)$.

Observation

Since $\mathrm{Soc}(G_X) = \mathrm{Ker}\,\lambda$, *the quotient can be viewed as the projection* π *of* G_X *onto* $\mathrm{Mlt}(X)$. *Hence it is usual to consider* $G_X/\mathrm{Soc}(G_X) \cong \mathrm{Mlt}(X)$.

$\pi(x) = L_x$

Since $\lambda_x(y) = L_x(y)$, we have $\pi(\lambda_x(y)) = \pi(L_x(y)) = L_{L_x(y)}$.

Since λ is a homomorphism we have $\pi(\lambda_a(y)) = L_{\pi(a)(y)}$.

Now $a + x = a \circ (a^{-1} \circ (a + x)) = a \circ \lambda_a^{-1}(x)$ and hence $\pi(a + x) = \pi(a) L_{\pi(a)^{-1}(x)}$.

Multiplication left brace

Definition

The *multiplication left brace* is the quotient left brace $G_X/\mathrm{Soc}(G_X)$.

Observation

Since $\mathrm{Soc}(G_X) = \mathrm{Ker}\,\lambda$*, the quotient can be viewed as the projection* π *of* G_X *onto* $\mathrm{Mlt}(X)$*. Hence it is usual to consider* $G_X/\mathrm{Soc}(G_X) \cong \mathrm{Mlt}(X)$.

$\pi(x) = L_x$

Since $\lambda_x(y) = L_x(y)$, we have $\pi(\lambda_x(y)) = \pi(L_x(y)) = L_{L_x(y)}$.

Since λ is a homomorphism we have $\pi(\lambda_a(y)) = L_{\pi(a)(y)}$.

Now $a + x = a \circ (a^{-1} \circ (a + x)) = a \circ \lambda_a^{-1}(x)$ and hence $\pi(a + x) = \pi(a) L_{\pi(a)^{-1}(x)}$.

Multiplication left brace

Definition

The *multiplication left brace* is the quotient left brace $G_X/\mathrm{Soc}(G_X)$.

Observation

Since $\mathrm{Soc}(G_X) = \mathrm{Ker}\,\lambda$*, the quotient can be viewed as the projection* π *of* G_X *onto* $\mathrm{Mlt}(X)$*. Hence it is usual to consider* $G_X/\mathrm{Soc}(G_X) \cong \mathrm{Mlt}(X)$.

$\pi(x) = L_x$

Since $\lambda_x(y) = L_x(y)$, we have $\pi(\lambda_x(y)) = \pi(L_x(y)) = L_{L_x(y)}$.

Since λ is a homomorphism we have $\pi(\lambda_a(y)) = L_{\pi(a)(y)}$.

Now $a + x = a \circ (a^{-1} \circ (a + x)) = a \circ \lambda_a^{-1}(x)$ and hence $\pi(a + x) = \pi(a)L_{\pi(a)^{-1}(x)}$.

Multiplication left brace

Definition

The *multiplication left brace* is the quotient left brace $G_X/\mathrm{Soc}(G_X)$.

Observation

Since $\mathrm{Soc}(G_X) = \mathrm{Ker}\,\lambda$*, the quotient can be viewed as the projection* π *of* G_X *onto* $\mathrm{Mlt}(X)$*. Hence it is usual to consider* $G_X/\mathrm{Soc}(G_X) \cong \mathrm{Mlt}(X)$.

$\pi(x) = L_x$
Since $\lambda_x(y) = L_x(y)$, we have $\pi(\lambda_x(y)) = \pi(L_x(y)) = L_{L_x(y)}$.
Since λ is a homomorphism we have $\pi(\lambda_a(y)) = L_{\pi(a)(y)}$.
Now $a + x = a \circ (a^{-1} \circ (a + x)) = a \circ \lambda_a^{-1}(x)$ and hence
$\pi(a + x) = \pi(a) L_{\pi(a)^{-1}(x)}$.

Socle vs. retract

Theorem

Let $(B, +, \circ)$ be a left brace and let $(B, \triangleleft, \triangleright)$ be its associated birack. Let X be a subset of B closed on λ that generates $(B, +)$. Then $\mathrm{Ret}(X) = \{x + \mathrm{Soc}(B) \mid x \in X\} \subseteq B/\mathrm{Soc}(B)$.

Proof.

$$x \sim y \iff \lambda_x = \lambda_y \text{ on } X \iff \lambda_x = \lambda_y \text{ on } B \iff \lambda_x \lambda_y^{-1} = \mathrm{id} \iff x \circ y^{-1} \in \operatorname{Ker} \lambda \iff x \circ y^{-1} \in \mathrm{Soc}(B)$$

$$[x]_\sim \triangleleft [y]_\sim = [\lambda_x(y)]_\sim = \lambda_x(y) + \mathrm{Soc}(B)$$

$$[x']_\sim \triangleleft [y']_\sim = [\lambda_{x'}(y')]_\sim = \lambda_{x'}(y') + \mathrm{Soc}(B) = \lambda_x(y + s) + \mathrm{Soc}(B) = \lambda_x(y) + \lambda_x(s) + \mathrm{Soc}(B) = \lambda_x(y) + \mathrm{Soc}(B)$$

□

Socle vs. retract

Theorem

Let $(B,+,\circ)$ *be a left brace and let* $(B,\triangleleft,\triangleright)$ *be its associated birack. Let* X *be a subset of* B *closed on* λ *that generates* $(B,+)$*. Then* $\mathrm{Ret}(X)=\{x+\mathrm{Soc}(B)\mid x\in X\}\subseteq B/\mathrm{Soc}(B)$.

Proof.

$x\sim y \iff \lambda_x=\lambda_y \text{ on } X \iff \lambda_x=\lambda_y \text{ on } B \iff \lambda_x\lambda_y^{-1}=\mathrm{id} \iff x\circ y^{-1}\in\operatorname{Ker}\lambda \iff x\circ y^{-1}\in\mathrm{Soc}(B)$

$[x]_\sim\triangleleft[y]_\sim=[\lambda_x(y)]_\sim=\lambda_x(y)+\mathrm{Soc}(B)$

$[x']_\sim\triangleleft[y']_\sim=[\lambda_{x'}(y')]_\sim=\lambda_{x'}(y')+\mathrm{Soc}(B)=$
$\lambda_x(y+s)+\mathrm{Soc}(B)=\lambda_x(y)+\lambda_x(s)+\mathrm{Soc}(B)=\lambda_x(y)+\mathrm{Soc}(B)$ □

Socle vs. retract

Theorem

Let $(B, +, \circ)$ be a left brace and let $(B, \triangleleft, \triangleright)$ be its associated birack. Let X be a subset of B closed on λ that generates $(B, +)$. Then $\mathrm{Ret}(X) = \{x + \mathrm{Soc}(B) \mid x \in X\} \subseteq B/\mathrm{Soc}(B)$.

Proof.

$$x \sim y \iff \lambda_x = \lambda_y \text{ on } X \iff \lambda_x = \lambda_y \text{ on } B \iff \lambda_x \lambda_y^{-1} = \mathrm{id} \iff x \circ y^{-1} \in \operatorname{Ker} \lambda \iff x \circ y^{-1} \in \mathrm{Soc}(B)$$

$$[x]_\sim \triangleleft [y]_\sim = [\lambda_x(y)]_\sim = \lambda_x(y) + \mathrm{Soc}(B)$$

$$[x']_\sim \triangleleft [y']_\sim = [\lambda_{x'}(y')]_\sim = \lambda_{x'}(y') + \mathrm{Soc}(B) = \lambda_x(y+s) + \mathrm{Soc}(B) = \lambda_x(y) + \lambda_x(s) + \mathrm{Soc}(B) = \lambda_x(y) + \mathrm{Soc}(B)$$

□

Socle vs. retract

Theorem

Let $(B,+,\circ)$ be a left brace and let $(B,\triangleleft,\triangleright)$ be its associated birack. Let X be a subset of B closed on λ that generates $(B,+)$. Then $\mathrm{Ret}(X)=\{x+\mathrm{Soc}(B)\mid x\in X\}\subseteq B/\mathrm{Soc}(B)$.

Proof.

$$x\sim y \iff \lambda_x=\lambda_y \text{ on } X \iff \lambda_x=\lambda_y \text{ on } B \iff \lambda_x\lambda_y^{-1}=\mathrm{id} \iff x\circ y^{-1}\in\operatorname{Ker}\lambda \iff x\circ y^{-1}\in\mathrm{Soc}(B)$$

$$[x]_\sim\triangleleft[y]_\sim=[\lambda_x(y)]_\sim=\lambda_x(y)+\mathrm{Soc}(B)$$

$$[x']_\sim\triangleleft[y']_\sim=[\lambda_{x'}(y')]_\sim=\lambda_{x'}(y')+\mathrm{Soc}(B)=\lambda_x(y+s)+\mathrm{Soc}(B)=\lambda_x(y)+\lambda_x(s)+\mathrm{Soc}(B)=\lambda_x(y)+\mathrm{Soc}(B)$$

□

Corollaries of the retract

Corollary

$\sim$ is a congruence for every finite involutive birack.

Proof.

Since X embeds into G_X, $\mathrm{Ret}(X)$ embeds into $\mathrm{Mlt}(X)$. □

Corollary

If X is finite and $\mathrm{Mlt}(X)$ is abelian then X is multipermutation.

Proof.

$\mathrm{Ret}(X)$ embeds into $\mathrm{Mlt}(X)$. Since $(\mathrm{Mlt}(X), \circ)$ is abelian, $(\mathrm{Mlt}(X), +, *)$ is a radical ring. All finite commutative radical rings are nilpotent. Hence $\mathrm{Ret}(X)$ is multipermutation. □

Corollaries of the retract

Corollary

$\sim$ is a congruence for every finite involutive birack.

Proof.

Since X embeds into G_X, $\mathrm{Ret}(X)$ embeds into $\mathrm{Mlt}(X)$. □

Corollary

If X is finite and $\mathrm{Mlt}(X)$ is abelian then X is multipermutation.

Proof.

$\mathrm{Ret}(X)$ embeds into $\mathrm{Mlt}(X)$. Since $(\mathrm{Mlt}(X), \circ)$ is abelian, $(\mathrm{Mlt}(X), +, *)$ is a radical ring. All finite commutative radical rings are nilpotent. Hence $\mathrm{Ret}(X)$ is multipermutation. □

Corollaries of the retract

Corollary

$\sim$ is a congruence for every finite involutive birack.

Proof.

Since X embeds into G_X, $\mathrm{Ret}(X)$ embeds into $\mathrm{Mlt}(X)$. □

Corollary

If X is finite and $\mathrm{Mlt}(X)$ is abelian then X is multipermutation.

Proof.

$\mathrm{Ret}(X)$ embeds into $\mathrm{Mlt}(X)$. Since $(\mathrm{Mlt}(X), \circ)$ is abelian, $(\mathrm{Mlt}(X), +, *)$ is a radical ring. All finite commutative radical rings are nilpotent. Hence $\mathrm{Ret}(X)$ is multipermutation. □

Corollaries of the retract

Corollary

$\sim$ is a congruence for every finite involutive birack.

Proof.

Since X embeds into G_X, $\mathrm{Ret}(X)$ embeds into $\mathrm{Mlt}(X)$. □

Corollary

If X is finite and $\mathrm{Mlt}(X)$ is abelian then X is multipermutation.

Proof.

$\mathrm{Ret}(X)$ embeds into $\mathrm{Mlt}(X)$. Since $(\mathrm{Mlt}(X), \circ)$ is abelian, $(\mathrm{Mlt}(X), +, *)$ is a radical ring. All finite commutative radical rings are nilpotent. Hence $\mathrm{Ret}(X)$ is multipermutation. □

Indecomposable involutive biracks

Definition

We say that an involutive birack $(X, \triangleleft, \triangleright)$ is *indecomposable* if the group $\mathrm{Mlt}(X)$ is transitive.

Theorem (W. Rump, reformulated by M. Castelli)

Let $(B, +, \circ)$ and let $g \in B$ be such that the orbit of g under the action λ generates the left brace B. If we define

$$a \triangleleft b = \lambda_a(g) \circ b$$

then $(B, \triangleleft, \triangleright)$ is an indecomposable involutive birack with its mutiplication left brace isomorphic to B.

Moreover, every indecomposable involutive birack can be obtained this way.

Invariants of isomorphisms

Theorem (W. Rump)

Let k be a power of prime and let $(B,+,\circ)$ be a left brace of size k with $(B,\circ)$ cyclic. Then $(B,+)$ is cyclic if and only if $k \neq 4$.

Theorem (P. J., A. P., A. Z.-D.)

A complete set of invariants for finite indecomposable involutive biracks with cyclic multiplication groups are

- $k \in \mathbb{N}$,
- $n \in \mathbb{N}$ *such that,*
  - n *divides* k,
  - *every prime* p *divides* n *whenever* p *divides* k,
  - *if 8 divides* k *then 4 divides* n,
- $g \in \{1, \ldots, \gcd(n, k/n)\}$ *coprime to* k.

Invariants of isomorphisms

Theorem (W. Rump)

Let k be a power of prime and let $(B, +, \circ)$ be a left brace of size k with $(B, \circ)$ cyclic. Then $(B, +)$ is cyclic if and only if $k \neq 4$.

Theorem (P. J., A. P., A. Z.-D.)

A complete set of invariants for finite indecomposable involutive biracks with cyclic multiplication groups are

- $k \in \mathbb{N}$,
- $n \in \mathbb{N}$ *such that,*
  - n *divides* k,
  - *every prime* p *divides* n *whenever* p *divides* k,
  - *if 8 divides* k *then 4 divides* n,
- $g \in \{1, \dots, \gcd(n, k/n)\}$ *coprime to* k.

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

Biracks 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

$$a \lhd b = \lambda_a(b), \qquad a \rhd b = \rho_b(a)$$

then $(B,\lhd,\rhd)$ is a birack.

Biracks 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*

$$a \triangleleft b = \lambda_a(b), \qquad a \triangleright b = \rho_b(a)$$

then $(B,\triangleleft,\triangleright)$ *is a birack.*

Biracks 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*

$$a \triangleleft b = \lambda_a(b), \qquad a \triangleright b = \rho_b(a)$$

then $(B, \triangleleft, \triangleright)$ *is a birack.*

Holomorph

Definition

Let G be a group. The *holomorph* of a group is the group $G \rtimes \mathrm{Aut}(G)$ with the operation

$$(g, \alpha) \cdot (h, \beta) = (g\alpha(h), \alpha\beta).$$

A subgroup $H \leqslant \mathrm{Hol}(G)$ is called *regular* if, for each $g \in G$, there exists a unique $\phi_g \in \mathrm{Aut}(G)$ such that $(g, \phi_g) \in H$.

Theorem (L. Guarnieri, L. Vendramin)

There is a 1-1 correspondence between skew left braces and regular subgroups of holomorphs.

Proof.

$b, \lambda_b \leftrightsquigarrow (b, \phi_b)$ □

Holomorph

Definition

Let G be a group. The *holomorph* of a group is the group $G \rtimes \mathrm{Aut}(G)$ with the operation

$$(g, \alpha) \cdot (h, \beta) = (g\alpha(h), \alpha\beta).$$

A subgroup $H \leqslant \mathrm{Hol}(G)$ is called *regular* if, for each $g \in G$, there exists a unique $\phi_g \in \mathrm{Aut}(G)$ such that $(g, \phi_g) \in H$.

Theorem (L. Guarnieri, L. Vendramin)

There is a 1-1 correspondence between skew left braces and regular subgroups of holomorphs.

Proof.

$b, \lambda_b \leftrightsquigarrow (b, \phi_b)$ □

Holomorph

Definition

Let G be a group. The *holomorph* of a group is the group $G \rtimes \mathrm{Aut}(G)$ with the operation

$$(g, \alpha) \cdot (h, \beta) = (g\alpha(h), \alpha\beta).$$

A subgroup $H \leqslant \mathrm{Hol}(G)$ is called *regular* if, for each $g \in G$, there exists a unique $\phi_g \in \mathrm{Aut}(G)$ such that $(g, \phi_g) \in H$.

Theorem (L. Guarnieri, L. Vendramin)

There is a 1-1 correspondence between skew left braces and regular subgroups of holomorphs.

Proof.

$b, \lambda_b \leftrightsquigarrow (b, \phi_b)$ □

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

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

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

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

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

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

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 *socle-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 socle-nilpotent of class k if and only if its associated birack 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 *socle-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 socle-nilpotent of class k if and only if its associated birack has multipermutation level k.

Central nilpotency

Definition (I. Colazzo, F. Catino, P. Stefanelli)

The *annihilator* or the *center* of a skew left brace is the ideal

$$\{c \in B \mid \forall a \in B \quad c + a = a + c = c \circ a = a \circ c\}$$

or simply $Z(B,+) \cap Z(B,\circ) \cap \operatorname{Ker}\lambda$.

Definitions (M. Bonatto, P. J.)

Upper central series:

$$Z_0(B) = 0, \quad Z_n = \{c \in B \mid \forall a \in B \quad a * c, c * a, [a,c]_+ \in Z_{n-1}(B)\},$$

Lower central series:

$$\Gamma_0(I) = I, \quad \Gamma_n(I) = \langle \Gamma_{n-1}(I) * B, B * \Gamma_{n-1}(I), [\Gamma_{n-1}(I), B]_+ \rangle_+,$$

where $x * y = -x + (x \circ y) - y$.

Central nilpotency

Definition (I. Colazzo, F. Catino, P. Stefanelli)

The *annihilator* or the *center* of a skew left brace is the ideal

$$\{c \in B \mid \forall a \in B \quad c + a = a + c = c \circ a = a \circ c\}$$

or simply $Z(B,+) \cap Z(B,\circ) \cap \operatorname{Ker}\lambda$.

Definitions (M. Bonatto, P. J.)

Upper central series:

$$Z_0(B) = 0, \quad Z_n = \{c \in B \mid \forall a \in B \quad a * c, c * a, [a,c]_+ \in Z_{n-1}(B)\},$$

Lower central series:

$$\Gamma_0(I) = I, \quad \Gamma_n(I) = \langle \Gamma_{n-1}(I) * B, B * \Gamma_{n-1}(I), [\Gamma_{n-1}(I), B]_+ \rangle_+,$$

where $x * y = -x + (x \circ y) - y$.

Commutator in skew braces

Theorem (D. Bourn, A. Facchini, M. Pompili)

The commutator of two ideals I and J in a skew brace $(B, +, \circ)$ is the smallest ideal generated by $[I, J]_+$, $[I, J]_\circ$ and $I * J$.

Corollary

$$Z_n(B)/Z_{n-1}(B) = Z(B/Z_{n-1}(B))$$

$$\Gamma_n(I) = [\Gamma_{n-1}(I), B]$$

Commutator in skew braces

Theorem (D. Bourn, A. Facchini, M. Pompili)

The commutator of two ideals I and J in a skew brace $(B, +, \circ)$ is the smallest ideal generated by $[I, J]_+$, $[I, J]_\circ$ and $I * J$.

Corollary

$$Z_n(B)/Z_{n-1}(B) = Z(B/Z_{n-1}(B))$$
$$\Gamma_n(I) = [\Gamma_{n-1}(I), B]$$

Opposite skew left braces

Proposition

Let $(B, \triangleleft, \triangleright)$ be a birack and let $r(x,y) = (x \triangleleft y, x \triangleright y)$. Then $r^{-1} : (x,y) \mapsto (x \hat{\triangleleft} y, x \hat{\triangleright} y)$ is a birack.

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

Corollary

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

Opposite skew left braces

Proposition

Let $(B, \triangleleft, \triangleright)$ be a birack and let $r(x,y) = (x \triangleleft y, x \triangleright y)$. Then $r^{-1} : (x,y) \mapsto (x \,\hat{\triangleleft}\, y, x \,\hat{\triangleright}\, y)$ is a birack.

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

Corollary

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

Opposite skew left braces

Proposition

Let $(B, \triangleleft, \triangleright)$ *be a birack and let* $r(x,y) = (x \triangleleft y, x \triangleright y)$. *Then* $r^{-1} : (x,y) \mapsto (x \mathbin{\hat{\triangleleft}} y, x \mathbin{\hat{\triangleright}} y)$ *is a birack.*

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

Corollary

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

Opposite skew left braces

Proposition

Let $(B, \triangleleft, \triangleright)$ *be a birack and let* $r(x,y) = (x \triangleleft y, x \triangleright y)$. *Then* $r^{-1} : (x,y) \mapsto (x \hat{\triangleleft} y, x \hat{\triangleright} y)$ *is a birack.*

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

Corollary

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

Structure group

Definition

Let $(X, \triangleleft, \triangleright)$ be a finite birack. The infinite group with the presentation

$$G_X = \langle X \mid x \circ y = (x \triangleleft y) \circ (x \triangleright y) \rangle$$

is called the *structure group* of the birack X.

Theorem

Let $(X, \triangleleft, \triangleright)$ be a birack. Let

$$A_X = \langle X \mid x + y = y + (y \triangleleft (y \setminus_{\triangleleft} x)) \rangle .$$

Then there exists a bijection $\phi : A_X \to G_X$ such that $\phi(x) = x$ and

$$\phi(a) \circ \phi(b + c) = \phi(\phi^{-1}(\phi(a) \circ \phi(b)) - a + \phi^{-1}(\phi(a) \circ \phi(c))).$$

Structure group

Definition

Let $(X, \triangleleft, \triangleright)$ be a finite birack. The infinite group with the presentation

$$G_X = \langle X \mid x \circ y = (x \triangleleft y) \circ (x \triangleright y) \rangle$$

is called the *structure group* of the birack X.

Theorem

Let $(X, \triangleleft, \triangleright)$ be a birack. Let

$$A_X = \langle X \mid x + y = y + (y \triangleleft (y \backslash_{\triangleleft} x)) \rangle .$$

Then there exists a bijection $\phi : A_X \to G_X$ such that $\phi(x) = x$ and

$$\phi(a) \circ \phi(b + c) = \phi(\phi^{-1}(\phi(a) \circ \phi(b)) - a + \phi^{-1}(\phi(a) \circ \phi(c))).$$

Injective biracks

Theorem

Let $(X, \triangleleft, \triangleright)$ *be a birack and let* G_X *be its structure group. If we define*

$$\iota : (X, \triangleleft, \triangleright) \to (G_X, \triangleleft, \triangleright), \qquad x \mapsto x,$$

then ι *is a homomorphism of biracks.*

Corollary

Suppose $\iota(x) = \iota(y)$ *then* $x \sim y$.

Definition

We say that a birack is *injective* if ι is injective.

Observation

Every involutive birack is injective.

Injective biracks

Theorem

Let $(X, \triangleleft, \triangleright)$ be a birack and let G_X be its structure group. If we define

$$\iota : (X, \triangleleft, \triangleright) \to (G_X, \triangleleft, \triangleright), \qquad x \mapsto x,$$

then ι is a homomorphism of biracks.

Corollary

Suppose $\iota(x) = \iota(y)$ then $x \sim y$.

Definition

We say that a birack is *injective* if ι is injective.

Observation

Every involutive birack is injective.

Injective biracks

Theorem

Let $(X, \lhd, \rhd)$ be a birack and let G_X be its structure group. If we define

$$\iota : (X, \lhd, \rhd) \to (G_X, \lhd, \rhd), \qquad x \mapsto x,$$

then ι is a homomorphism of biracks.

Corollary

Suppose $\iota(x) = \iota(y)$ then $x \sim y$.

Definition

We say that a birack is *injective* if ι is injective.

Observation

Every involutive birack is injective.

Injective biracks

Theorem

Let $(X, \triangleleft, \triangleright)$ be a birack and let G_X be its structure group. If we define

$$\iota : (X, \triangleleft, \triangleright) \to (G_X, \triangleleft, \triangleright), \qquad x \mapsto x,$$

then ι is a homomorphism of biracks.

Corollary

Suppose $\iota(x) = \iota(y)$ then $x \sim y$.

Definition

We say that a birack is *injective* if ι is injective.

Observation

Every involutive birack is injective.

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 (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. $\lambda_{a+b} = \lambda_b \lambda_a$.

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 $a, b \in B$.

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 (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. $\lambda_{a+b} = \lambda_b \lambda_a$.

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 $a, b \in B$.

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 (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. $\lambda_{a+b} = \lambda_b \lambda_a$.

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 $a, b \in B$.

Distributive biracks

Theorem (P. J., A. Pilitowska)

Let (X,σ,τ) be a birack. TFAE:

- $L_{\hat{L}_x(y)} = L_y$,
- $L_{\mathbf{R}_x(y)} = L_y$,
- $L_xL_y = L_{L_x(y)}L_x$,
- $\hat{L}_x = L_x^{-1}$,
- $L_x \in \mathrm{Aut}(X)$,

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 biracks

Theorem (P. J., A. Pilitowska)

Let (X, σ, τ) *be a birack. TFAE:*

- $L_{\hat{L}_x(y)} = L_y$,
- $L_{\mathbf{R}_x(y)} = L_y$,
- $L_x L_y = L_{L_x(y)} L_x$,
- $\hat{L}_x = L_x^{-1}$,
- $L_x \in \mathrm{Aut}(X)$,

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

Proposition (P. J., A. Pilitowska)

Let $(X, \triangleleft, \triangleright)$ *be* 2*-reductive. Then* G_X *is socle-nilpotent of degree at most* 2*.*

Skew left braces and 2-reductivity

Theorem (P. J., A. Pilitowska)

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

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

Proposition (P. J., A. Pilitowska)

Let $(X, \triangleleft, \triangleright)$ be 2-reductive. Then G_X is socle-nilpotent of degree at most 2.