Skew braces and solutions of the YBE

Ilaria Colazzo

May 25, 2021

Hopf Algebras and Galois Module Theory

Overview

Yang-Baxter equation

Skew braces

A construction technique for skew braces: The Ideal Extension by a trivial brace

Skew braces with non-trivial annihilator

Skew braces and regular subgroups of the Holomorph

The Yang-Baxter equation

The Yang-Baxter equation is a fundamental tool in many fields such as:

- statistical mechanics
- quantum group theory
- low-dimensional topology
- knot theory
- quantum computation

The Yang-Baxter equation

- k – a field
- V – a vector sapace over k

A solution (of the YBE) is a linear map $R\colon V\otimes V\to V\otimes V$ such that

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

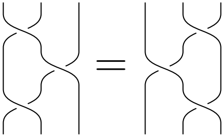
Set-theoretic solutions of the YBE

Problem (Drinfeld,'92)

Study set-theoretic solutions of the YBE.

A set-theoretic solution (of the YBE) is a pair (X, r) where X is a non-empty set and $r: X \times X \to X \times X$ is a map such that

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



Reidemeister move of type III

(X, r) – a set-theoretic solution of the YBE
Write

$$r(x, y) = (\lambda_x(y), \rho_y(x))$$

where $\lambda_x, \rho_x : X \to X$.

- r is left (resp. right) non-degenerate if λ_x (resp. ρ_x) is bijective, for any $x \in X$.
- non-degenerate if it is both left and right non-degenerate
- involutive if $r^2(x, y) = (x, y)$.

(X, r) – a set-theoretic solution of the YBE
Write

$$r(x, y) = \big(\lambda_x(y), \rho_y(x) \big)$$

where $\lambda_x, \rho_x : X \to X$.

- r is left (resp. right) non-degenerate if λ_x (resp. ρ_x) is bijective, for any $x \in X$.
- non-degenerate if it is both left and right non-degenerate
- involutive if $r^2(x, y) = (x, y)$.

(X, r) – a set-theoretic solution of the YBE
Write

$$r(x, y) = \left(\lambda_x(y),\ \rho_y(x)\right)$$

where $\lambda_x, \rho_x : X \to X$.

- r is left (resp. right) non-degenerate if λ_x (resp. ρ_x) is bijective, for any $x \in X$.
- non-degenerate if it is both left and right non-degenerate
- involutive if $r^2(x, y) = (x, y)$.

(X, r) – a set-theoretic solution of the YBE
Write

$$r(x, y) = (\lambda_x(y), \rho_y(x))$$

where $\lambda_x, \rho_x : X \to X$.

- r is left (resp. right) non-degenerate if λ_x (resp. ρ_x) is bijective, for any $x \in X$.
- non-degenerate if it is both left and right non-degenerate
- involutive if $r^2(x, y) = (x, y)$.

(X, r) – a set-theoretic solution of the YBE
Write

$$r(x, y) = (\lambda_x(y), \rho_y(x))$$

where $\lambda_x, \rho_x : X \to X$.

- r is left (resp. right) non-degenerate if λ_x (resp. ρ_x) is bijective, for any $x \in X$.
- non-degenerate if it is both left and right non-degenerate
- involutive if $r^2(x, y) = (x, y)$.

Briefly, the state-of-the-art

- Involutive non-degenerate solutions

  ['99] Etingof, Schedler & Soloviev
  ['99] Gateva-Ivanova & Van den Bergh
  (Ring and group theoretical tools)
  ['07] Rump
  ['14] Cedó, Jespers & Okninski
  (Braces)

- Bijective non-degenerate solutions

  ['00] Lu, Yan & Zhu
  ['00] Soloviev
  (Ring and group theoretical tools)
  ['17] Guarnienri & Vendramin
  (Skew braces)

Briefly, the state-of-the-art

- Involutive non-degenerate solutions

  ['99] Etingof, Schedler & Soloviev
  ['99] Gateva-Ivanova & Van den Bergh
  (Ring and group theoretical tools)
  ['07] Rump
  ['14] Cedó, Jespers & Okninski
  (Braces)

- Bijective non-degenerate solutions

  ['00] Lu, Yan & Zhu
  ['00] Soloviev
  (Ring and group theoretical tools)
  ['17] Guarnienri & Vendramin
  (Skew braces)

Briefly, the state-of-the-art

- Involutive non-degenerate solutions

  ['99] Etingof, Schedler & Soloviev
  ['99] Gateva-Ivanova & Van den Bergh
  (Ring and group theoretical tools)
  ['07] Rump
  ['14] Cedó, Jespers & Okninski
  (Braces)

- Bijective non-degenerate solutions

  ['00] Lu, Yan & Zhu
  ['00] Soloviev
  (Ring and group theoretical tools)
  ['17] Guarnienri & Vendramin
  (Skew braces)

Briefly, the state-of-the-art

- Involutive non-degenerate solutions
  - ['99] Etingof, Schedler & Soloviev
  - ['99] Gateva-Ivanova & Van den Bergh
    (Ring and group theoretical tools)
  - ['07] Rump
  - ['14] Cedó, Jespers & Okninski
    (Braces)
- Bijective non-degenerate solutions
  - ['00] Lu, Yan & Zhu
  - ['00] Soloviev
    (Ring and group theoretical tools)
  - ['17] Guarnienri & Vendramin
    (Skew braces)

Briefly, the state-of-the-art

- Involutive non-degenerate solutions
  ['99] Etingof, Schedler & Soloviev
  ['99] Gateva-Ivanova & Van den Bergh
  (Ring and group theoretical tools)
  ['07] Rump
  ['14] Cedó, Jespers & Okninski
  (Braces)
- Bijective non-degenerate solutions
  ['00] Lu, Yan & Zhu
  ['00] Soloviev
  (Ring and group theoretical tools)
  ['17] Guarnienri & Vendramin
  (Skew braces)

Briefly, the state-of-the-art

- Involutive non-degenerate solutions
  - ['99] Etingof, Schedler & Soloviev
  - ['99] Gateva-Ivanova & Van den Bergh
    (Ring and group theoretical tools)
  - ['07] Rump
  - ['14] Cedó, Jespers & Okninski
    (Braces)
- Bijective non-degenerate solutions
  - ['00] Lu, Yan & Zhu
  - ['00] Soloviev
    (Ring and group theoretical tools)
  - ['17] Guarnienri & Vendramin
    (Skew braces)

Briefly, the state-of-the-art

- Not necessarly bijective solutions

['17] Lebed
(idempotent solutions)

idempotent solutions allow a unified treatment of different algebraic structures (such as free monoids, free commutative monoids, factorizable monoids, and distributive lattices)

['20] Cvetko-Vah & Verwimp
(cubic solutions and skew lattices)

['17] Catino, C. & Stefanelli
(left non-degenerate solutions and left cancellative semi-braces)

['19] Jespers & Van Antwerpen
(semi-braces)

Briefly, the state-of-the-art

- Not necessarly bijective solutions

['17] Lebed
(idempotent solutions)

idempotent solutions allow a unified treatment of different algebraic structures (such as free monoids, free commutative monoids, factorizable monoids, and distributive lattices)

['20] Cvetko-Vah & Verwimp
(cubic solutions and skew lattices)

['17] Catino, C. & Stefanelli
(left non-degenerate solutions and left cancellative semi-braces)

['19] Jespers & Van Antwerpen
(semi-braces)

Briefly, the state-of-the-art

- Not necessarly bijective solutions

['17] Lebed
(idempotent solutions)

idempotent solutions allow a unified treatment of different algebraic structures (such as free monoids, free commutative monoids, factorizable monoids, and distributive lattices)

['20] Cvetko-Vah & Verwimp
(cubic solutions and skew lattices)

['17] Catino, C. & Stefanelli
(left non-degenerate solutions and left cancellative semi-braces)

['19] Jespers & Van Antwerpen
(semi-braces)

Briefly, the state-of-the-art

- Not necessarly bijective solutions

  ['17] Lebed
  (idempotent solutions)

  idempotent solutions allow a unified treatment of different algebraic structures (such as free monoids, free commutative monoids, factorizable monoids, and distributive lattices)

  ['20] Cvetko-Vah & Verwimp
  (cubic solutions and skew lattices)

  ['17] Catino, C. & Stefanelli
  (left non-degenerate solutions and left cancellative semi-braces)

  ['19] Jespers & Van Antwerpen
  (semi-braces)

Examples

- The flip map $r(x, y) = (y, x)$.
- $\sigma, \tau : X \to X$ maps.

$$r(x, y) = (\sigma(y), \tau(x)) \text{ solution } \iff \sigma\tau = \tau\sigma.$$

  r is non-degenerate if σ and ρ are bijective.
- X a group

$$r(x, y) = \left(y, y^{-1}xy\right)$$

  is a solution.
- Generally

  X – a set
  $\triangleleft$ – binary operation of X

$$r(x, y) = (y, x \triangleleft y) \text{ solution } \iff \triangleleft \text{ self-distributive}$$

Examples

- The flip map $r(x, y) = (y, x)$.
- $\sigma, \tau : X \to X$ maps.

$$r(x, y) = (\sigma(y), \tau(x)) \text{ solution } \iff \sigma\tau = \tau\sigma.$$

  r is non-degenerate if σ and ρ are bijective.

- X a group

$$r(x, y) = (y, y^{-1}xy)$$

  is a solution.

- Generally

  X – a set
  $\triangleleft$ – binary operation of X

$$r(x, y) = (y, x \triangleleft y) \text{ solution } \iff \triangleleft \text{ self-distributive}$$

Examples

- The flip map $r(x,y) = (y,x)$.
- $\sigma, \tau : X \to X$ maps.

$$r(x,y) = (\sigma(y), \tau(x)) \text{ solution } \iff \sigma\tau = \tau\sigma.$$

  r is non-degenerate if σ and ρ are bijective.
- X a group

$$r(x,y) = \left(y, y^{-1}xy\right)$$

  is a solution.
- Generally

  X – a set
  $\triangleleft$ – binary operation of X

$$r(x,y) = (y, x \triangleleft y) \text{ solution } \iff \triangleleft \text{ self-distributive}$$

Examples

- The flip map $r(x, y) = (y, x)$.
- $\sigma, \tau : X \to X$ maps.

  $$r(x, y) = (\sigma(y), \tau(x)) \text{ solution } \iff \sigma\tau = \tau\sigma.$$

  r is non-degenerate if σ and ρ are bijective.
- X a group

  $$r(x, y) = \left(y, y^{-1}xy\right)$$

  is a solution.
- Generally

  X – a set
  $\triangleleft$ – binary operation of X

  $$r(x, y) = (y, x \triangleleft y) \text{ solution } \iff \triangleleft \text{ self-distributive}$$

Examples

- The flip map $r(x,y) = (y,x)$.
- $\sigma, \tau : X \to X$ maps.

$$r(x,y) = (\sigma(y), \tau(x)) \text{ solution } \iff \sigma\tau = \tau\sigma.$$

  r is non-degenerate if σ and ρ are bijective.

- X a group

$$r(x,y) = \left(y, y^{-1}xy\right)$$

  is a solution.

- Generally

  X – a set
  $\triangleleft$ – binary operation of X

$$r(x,y) = (y, x \triangleleft y) \text{ solution } \iff \triangleleft \text{ self-distributive}$$

$$(x \triangleleft y) \triangleleft z = (x \triangleleft z) \triangleleft (y \triangleleft z)$$

Radical rings

- $(R, +, \cdot)$ – a ring
- Define $x \circ y = x + xy + y$.
- $(R, \circ)$ is a monoid with neutral element 0.
- R is a radical ring if $(R, \circ)$ is a group.

Theorem (Rump, '08)

- R – a radical ring.
- Then $r : R \times R \to R \times R$,

$$r(a, b) = \left(-a + a \circ b, \left(a^{-} + b\right)^{-} \circ b\right)$$

is an involutive non-degenerate solution.

Here, x^{-} denotes the inverse of x in $(R, \circ)$.

Do we need a radical ring to produce a set-theoretical solution as in Rump construction?

Skew braces

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

- $(B, +)$ and $(B, \circ)$ are groups
- for any $a, b, c \in B$ it holds

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

A skew brace with $(B, +)$ abelian is called a brace (Rump, '07).

Skew braces and solutions

Theorem (Guarnieri & Vendramin, '17)

- B a skew brace.
- Then $r: B \times B \to B \times B$,

$$r(a,b) = \left(-a + a \circ b, \left(a^{-} + b\right)^{-} \circ b\right)$$

is an bijective non-degenerate solution.

r is involutive$r^2 = \mathrm{id} \iff (B,+)$ is abelian.

Examples

- Radical rings
- Trivial skew braces

  $(G, +)$ – a group
  Define $a \circ b = a + b$.
  Then $(G, +, \circ)$ is a skew brace.
- Let $(G, +)$ be a group with an exact factorization $G = A + B$.

  A, B subgroups of G
  $A \cap B = \{0\}$
  Define $x \circ y = a + y + b$,
  where $x = a + b,\ a \in A,\ b \in B$.

Examples

- Radical rings
- Trivial skew braces

  $(G, +)$ – a group
  Define $a \circ b = a + b$.
  Then $(G, +, \circ)$ is a skew brace.
- Let $(G, +)$ be a group with an exact factorization $G = A + B$.

  A, B subgroups of G
  $A \cap B = \{0\}$
  Define $x \circ y = a + y + b$,
  where $x = a + b$, $a \in A$, $b \in B$.

Examples

- Radical rings
- Trivial skew braces

  $(G, +)$ – a group
  Define $a \circ b = a + b$.
  Then $(G, +, \circ)$ is a skew brace.
- Let $(G, +)$ be a group with an exact factorization $G = A + B$.

  A, B subgroups of G
  $A \cap B = \{0\}$
  Define $x \circ y = a + y + b$,
  where $x = a + b,\ a \in A,\ b \in B$.

Solutions & skew braces

Theorem

- All finite involutive non-degenerate solutions can be described from the description of all finite braces. (Bachiller, Cedó, Jespers, '16)
- All finite bijective non-degenerate solution can be described from the description of all finite skew braces. (Bachiller, '18)

Solutions & skew braces

Theorem

- All finite involutive non-degenerate solutions can be described from the description of all finite braces. (Bachiller, Cedó, Jespers, '16)
- All finite bijective non-degenerate solution can be described from the description of all finite skew braces. (Bachiller, '18)

Solutions & skew braces

Theorem

- All finite involutive non-degenerate solutions can be described from the description of all finite braces. (Bachiller, Cedó, Jespers, '16)
- All finite bijective non-degenerate solution can be described from the description of all finite skew braces. (Bachiller, '18)

The permutation group

- (X, r) - bijective non-degenerate solution
- Write $r(x, y) = (\lambda_x(y), \rho_y(x))$
- Define the permutation group

$$\mathcal{G}(X, r) = \text{gr}\left((\lambda_x, \rho_x^{-1}) : x \in X\right) \subseteq \text{Sym}(X) \times \text{Sym}(X)$$

Then the permutation group is a skew brace.

In addition

- If (X, r), (Y, s) are isomorphic solution $\mathcal{G}(X, r) \cong \mathcal{G}(Y, s)$
- If B is a skew brace, then it is possible to reconstruct all bijective non-degenerate solution (X, r) such that $\mathcal{G}(X, r) \cong B$.

The permutation group

- (X, r) - bijective non-degenerate solution
- Write $r(x, y) = (\lambda_x(y), \rho_y(x))$
- Define the permutation group

$$\mathcal{G}(X, r) = \text{gr}\left((\lambda_x, \rho_x^{-1}) : x \in X \right) \subseteq \text{Sym}(X) \times \text{Sym}(X)$$

Then the permutation group is a skew brace.

In addition

- If (X, r), (Y, s) are isomorphic solution $\mathcal{G}(X, r) \cong \mathcal{G}(Y, s)$
- If B is a skew brace, then it is possible to reconstruct all bijective non-degenerate solution (X, r) such that $\mathcal{G}(X, r) \cong B$.

The permutation group

- (X, r) - bijective non-degenerate solution
- Write $r(x, y) = (\lambda_x(y), \rho_y(x))$
- Define the permutation group

$$\mathcal{G}(X, r) = \text{gr}\left(\left(\lambda_x, \rho_x^{-1}\right) : x \in X\right) \subseteq \text{Sym}(X) \times \text{Sym}(X)$$

Then the permutation group is a skew brace.

In addition

- If (X, r), (Y, s) are isomorphic solution $\mathcal{G}(X, r) \cong \mathcal{G}(Y, s)$
- If B is a skew brace, then it is possible to reconstruct all bijective non-degenerate solution (X, r) such that $\mathcal{G}(X, r) \cong B$.

The permutation group

- (X, r) - bijective non-degenerate solution
- Write $r(x, y) = (\lambda_x(y), \rho_y(x))$
- Define the permutation group

$$\mathcal{G}(X, r) = \operatorname{gr}\left(\left(\lambda_x, \rho_x^{-1}\right) : x \in X\right) \subseteq \operatorname{Sym}(X) \times \operatorname{Sym}(X)$$

Then the permutation group is a skew brace.

In addition

- If (X, r), (Y, s) are isomorphic solution $\mathcal{G}(X, r) \cong \mathcal{G}(Y, s)$
- If B is a skew brace, then it is possible to reconstruct all bijective non-degenerate solution (X, r) such that $\mathcal{G}(X, r) \cong B$.

The idea: Extension of groups

New methods to construct skew braces.

An idea: Extension of groups

- H, I – groups
- determine all groups B such that

  I is a normal subgroup of B
  B/I is isomorphic to H

The idea: Extension of groups

New methods to construct skew braces.

An idea: Extension of groups

- H, I – groups
- determine all groups B such that

  I is a normal subgroup of B
  B/I is isomorphic to H

Normal subgroups $\longrightarrow$ Ideals

- B – skew brace
- $I \subseteq B$

I is an ideal of B if

- I is a normal subgroup of $(B, +)$ and $(B, \circ)$
- $\lambda_a(I) \subseteq I$

where for any $a \in A$, $\lambda_a : B \to B$, $b \mapsto -a + a \circ b$.

Normal subgroups $\longrightarrow$ Ideals

- B – skew brace
- $I \subseteq B$

I is an ideal of B if

- I is a normal subgroup of $(B, +)$ and $(B, \circ)$
- $\lambda_a(I) \subseteq I$

  where for any $a \in A$, $\lambda_a : B \to B$, $b \mapsto -a + a \circ b$.

The extension

The extensions method:

- I, H skew braces
- determine all possible skew braces B such that
  - I is an ideal of B
  - $B/I \cong H$

The extension problem for skew brace is still open.

We give a construction technique when I is a trivial brace, i.e.

- $(I, +)$ is abelian
- $a + b = a \circ b$

The extension

The extensions method:

- I, H skew braces
- determine all possible skew braces B such that
  - I is an ideal of B
  - $B/I \cong H$

The extension problem for skew brace is still open.

We give a construction technique when I is a trivial brace, i.e.

- $(I, +)$ is abelian
- $a + b = a \circ b$

The extension

The extensions method:

- I, H skew braces
- determine all possible skew braces B such that
  - I is an ideal of B
  - $B/I \cong H$

The extension problem for skew brace is still open.

We give a construction technique when I is a trivial brace, i.e.

- $(I, +)$ is abelian
- $a + b = a \circ b$

2-cocycles

- $(B, \circ)$ – a group with identity 0
- $(I, +)$ – abelian group
- $\sigma : B \to \mathrm{Aut}\,(I, +)$ – a right action

$\theta : B \times B \to I$ is a 2-cocycle form $(B, \circ)$ with values in $(I, +)$ wrt σ if

$$\sigma_c\,(\theta\,(a, b)) + \theta\,(a \circ b, c) = \theta\,(a, b \circ c) + \theta\,(b, c)$$
$$\theta\,(b, 0) = \theta\,(0, b) = 0$$

$\tau : B \times B \to I$ is a 2-cocycle form $(B, \circ)$ with values in $(I, +)$ if τ is a 2-cocycle wrt the trivial action σ (i.e. $\sigma_b = \mathrm{id}$).

An extension system

- $(B,+,\circ)$ – a skew brace
- $(I,+,\circ)$ – a trivial brace (i.e. $(I,+)$ abelian and $a+b=a\circ b$)
- $\nu:(B,\circ)\to \mathrm{Aut}(I,+)$ – a left action
- $\tau : B\times B\to I$ – a 2-cocycle form $(B,+)$ with values in $(I,+)$
- $\sigma:(B,\circ)\to \mathrm{Aut}(I,+)$ – a right action
- $\theta : B\times B\to I$ – a 2-cocycle form $(B,\circ)$ with values in $(I,+)$ wrt σ

$(B,I,\nu,\tau,\theta,\sigma)$ is a extension system of B by I (via ν, τ, θ and σ).

A compatible extension system

An extension system $(B, I, \nu, \tau, \theta, \sigma)$ is compatible if

$$\nu_{a+b}\sigma_{a+b}(i) + i = \nu_a\sigma_a(i) + \nu_b\sigma_b(i)$$

$$\begin{aligned}&\nu_{a\circ(b+c)}(\theta(a, b+c)) + \nu_a(\tau(b, c)) \\ &\quad = \nu_{a\circ b}(\theta(a, b)) + \nu_{a\circ c}(\theta(a, c)) - \tau(a, -a + b\circ c) + \tau(a\circ b, -a + b\circ c)\end{aligned}$$

Ideal extensions for skew braces by a trivial brace

- $(B, I, \nu, \tau, \theta, \sigma)$ – a compatible extension system

Define on $B \times I$

$$(a, i) + (b, j) = (a + b, i + j + \tau(a, b))$$
$$(a, i) \circ (b, j) = (a \circ b, \nu_{a \circ b}(\sigma_b \nu_{a^-}(i)) + \nu_a(j) + \nu_{a \circ b}(\theta(a, b))).$$

Then $(B \times I, +, \circ)$ is a skew brace, the ideal extension of B by I.

- $\{0\} \times I \cong I$
- $\{0\} \times I$ is an ideal on $B \times I$
- $(B \times I)/(\{0\} \times I) \cong B$
- $\{0\} \times I \subseteq \mathrm{Z}(B \times I, +)$

- B – a skew brace
- I – a central trivial ideal of B
- Put $\bar{B} = B/I$

Then there exists a compatible extension system of $\bar{B}$ by I such that B is isomorphic to the ideal extension of $\bar{B}$ by I.

i.e.

- $I \subseteq \mathrm{Z}(B,+)$
- I is a trivial brace

- B – a skew brace
- I – a central trivial ideal of B
- Put $\bar{B} = B/I$

Then there exists a compatible extension system of $\bar{B}$ by I such that B is isomorphic to the ideal extension of $\bar{B}$ by I.

i.e.

- $I \subseteq \mathrm{Z}(B, +)$
- I is a trivial brace

Example

- R – a radical ring
- I the trivial brace with additive group $(R, +)$
- $\alpha : R \to R$ - an homomoprphism of the additive group $(R, +)$
- define
  - $\tau(a, b) = \alpha(a)b$
  - $\theta(a, b) = 0$
  - $\sigma_b = \nu_b = \mathrm{id}$

Then $(R, I, \nu, \tau, \theta, \sigma)$ is a compatible extension system.

$$(a, i) + (b, j) = (a + b, i + j + \alpha(a)b)$$
$$(a, i) \circ (b, j) = (a \circ b, i + j)$$

$$(R \times I, +, \circ) \text{ is a brace} \iff \alpha(a)b = \alpha(b)a$$
$$\iff \tau(a, b) = \tau(b, a)$$

Ideal extensions for braces by a trivial brace

- $(B, +)$, $(I, +)$ – abelian groups
- $\tau : B \times B \to I$ – a 2-cocycle

τ is symmetric if

$$\tau(a, b) = \tau(b, a)$$

- B – a brace
- I – a trivial brace
- $(B, I, \nu, \tau, \theta, \sigma)$ - a compatible extension system with τ symmetric

then the ideal extension of B by I is a brace.

Ideal extensions for braces by a trivial brace

- $(B, +)$, $(I, +)$ – abelian groups
- $\tau : B \times B \to I$ – a 2-cocycle

τ is symmetric if

$$\tau(a, b) = \tau(b, a)$$

- B – a brace
- I – a trivial brace
- $(B, I, \nu, \tau, \theta, \sigma)$ - a compatible extension system with τ symmetric

then the ideal extension of B by I is a brace.

Skew braces with non-trivial annihilator

Examples of central trivial ideals

B – skew brace

- the socle

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

- the annihilator

$$\mathrm{Ann}(B) = \mathrm{Soc}(B) \cap \mathrm{Z}(B, \circ)$$

Hochschild compatible extension system

- $(B, +, \circ)$ – skew brace
- $(I, +, \circ)$ – an trivial brace

A Hochschild compatible extension system of B with values in I is

- compatible extension system $(B, I, \nu, \tau, \theta, \sigma)$
- ν, σ trivial actions.

The "compatibility conditions"

$$\nu_{a+b}\sigma_{a+b}(i) + i = \nu_a\sigma_a(i) + \nu_b\sigma_b(i) \quad \longleftarrow \quad \text{trivially holds}$$

$$\nu_{a\circ(b+c)}(\theta(a, b + c)) + \nu_a(\tau(b, c)) \\ = \nu_{a\circ b}(\theta(a, b)) + \nu_{a\circ c}(\theta(a, c)) - \tau(a, -a + b \circ c) + \tau(a \circ b, -a + b \circ c)$$

Hochschild compatible extension system

- $(B, +, \circ)$ – skew brace
- $(I, +, \circ)$ – an trivial brace

A Hochschild compatible extension system of B with values in I is

- compatible extension system $(B, I, \nu, \tau, \theta, \sigma)$
- ν, σ trivial actions.

The "compatibility conditions"

$$\nu_{a+b}\sigma_{a+b}(i) + i = \nu_a\sigma_a(i) + \nu_b\sigma_b(i) \qquad \longleftarrow \text{ trivially holds}$$

$$\nu_{a\circ(b+c)}(\theta(a, b+c)) + \nu_a(\tau(b, c))$$
$$= \nu_{a\circ b}(\theta(a, b)) + \nu_{a\circ c}(\theta(a, c)) - \tau(a, -a + b \circ c) + \tau(a \circ b, -a + b \circ c)$$

Hochschild compatible extension system

- $(B, +, \circ)$ – skew brace
- $(I, +, \circ)$ – an trivial brace

A Hochschild compatible extension system of B with values in I is

- compatible extension system $(B, I, \nu, \tau, \theta, \sigma)$
- ν, σ trivial actions.

The "compatibility conditions"

$$\nu_{a+b}\sigma_{a+b}(i) + i = \nu_a\sigma_a(i) + \nu_b\sigma_b(i) \quad \longleftarrow \quad \text{trivially holds}$$

$$\begin{aligned}&\nu_{a\circ(b+c)}(\theta(a, b+c)) + \nu_a(\tau(b,c))\\ &\quad = \nu_{a\circ b}(\theta(a,b)) + \nu_{a\circ c}(\theta(a,c)) - \tau(a, -a+b\circ c) + \tau(a\circ b, -a+b\circ c)\end{aligned}$$

Hochschild compatible extension system

- $(B, +, \circ)$ – skew brace
- $(I, +, \circ)$ – an trivial brace

A Hochschild compatible extension system of B with values in I is

- compatible extension system $(B, I, \nu, \tau, \theta, \sigma)$
- ν, σ trivial actions.

The "compatibility conditions"

$$\cancel{i + i = i + i}$$

$$\nu_{a\circ(b+c)}(\theta(a, b + c)) + \nu_a(\tau(b, c))$$
$$= \nu_{a\circ b}(\theta(a, b)) + \nu_{a\circ c}(\theta(a, c)) - \tau(a, -a + b \circ c) + \tau(a \circ b, -a + b \circ c)$$

Hochschild compatible extension system

- $(B, +, \circ)$ – skew brace
- $(I, +, \circ)$ – an trivial brace

A Hochschild compatible extension system of B with values in I is

- compatible extension system $(B, I, \nu, \tau, \theta, \sigma)$
- ν, σ trivial actions.

The "compatibility conditions"

$$\cancel{i + i = i + i}$$

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

- (B, I, τ, θ) – a Hochschild compatible extension system

Define on $B \times I$

$$(a,i) + (b,j) = (a+b, i+j+\tau(a,b))$$
$$(a,i) \circ (b,j) = (a \circ b, i+j+\theta(a,b)).$$

Then $(B \times I, +, \circ)$ is a skew brace, the Hochshild product of B by I.
Recall that for a ideal extension we have:

$$(a,i) + (b,j) = (a+b, i+j+\tau(a,b))$$
$$(a,i) \circ (b,j) = (a \circ b, \nu_{a \circ b}(\sigma_b \nu_{a^-}(i)) + \nu_a(j) + \nu_{a \circ b}(\theta(a,b))).$$

- (B, I, τ, θ) – a Hochschild compatible extension system

Define on $B \times I$

$$(a, i) + (b, j) = (a + b, i + j + \tau(a, b))$$
$$(a, i) \circ (b, j) = (a \circ b, i + j + \theta(a, b)).$$

Then $(B \times I, +, \circ)$ is a skew brace, the Hochshild product of B by I.
Recall that for a ideal extension we have:

$$(a, i) + (b, j) = (a + b, i + j + \tau(a, b))$$
$$(a, i) \circ (b, j) = (a \circ b, \nu_{a \circ b}(\sigma_b \nu_{a^-}(i)) + \nu_a(j) + \nu_{a \circ b}(\theta(a, b))).$$

Skew brace with non-trivial annihilator

- B skew brace
- $\operatorname{Ann}(B) \neq 0$
- Put
  - $I = \operatorname{Ann}(B)$
  - $\bar{B} = B/I$

Then

- there exists a Hochschild compatible extension system $(\bar{B}, I, \tau, \theta)$
- B is isomorphic to the Hochschild product of $\bar{B}$ by I

Sketch of the proof

- $\pi : B \to \bar{B}$ the projection map
- $s : \bar{B} \to B$ a map such that $s(\bar{0}) = 0$ and $\pi(s(\bar{b})) = \bar{b}$
- $\tau : \bar{B} \times \bar{B} \to I$ defined by

$$\left(\bar{a}, \bar{b}\right) = s\left(\bar{a}\right) + s\left(\bar{b}\right) - s\left(\bar{a} + \bar{b}\right)$$

  is a 2-cocycle form $\left(\bar{B}, +\right)$ with values in $(I, +)$
- $\theta : \bar{B} \times \bar{B} \to I$ defined by

$$\theta\left(\bar{a}, \bar{b}\right) = \left(s\left(\bar{a} \circ \bar{b}\right)\right)^{-} \circ s\left(\bar{a}\right) \circ s\left(\bar{b}\right)$$

  is a 2-cocycle form $\left(\bar{B}, \circ\right)$ with values in $(I, +)$

Then

- $(\bar{B}, I, \tau, \theta)$ is a Hochschild compatible extension system
- B is isomorphic to the Hochschild product of $\bar{B}$ by I

Holomorph of a group

- $(B, +)$ – a group

The holomorph of B is the group $\operatorname{Hol}(B, +) := B \times \operatorname{Aut}(B)$ with the product

$$(a, \alpha)(b, \beta) := (a + \alpha(b), \ \alpha\beta)$$

- $pr_1 : \operatorname{Hol}(B) \to B, (a, \alpha) \mapsto a$ be the first projection

Any $N \leq \operatorname{Hol}(B)$ acts on B
for all $(a, \alpha) \in N$ and $x \in B$ via

$$(a, \alpha) \cdot x = pr_1((a, \alpha)(x, \mathrm{id}_B)) = a + \alpha(x).$$

Holomorph of a group

- $(B, +)$ – a group

The holomorph of B is the group $\mathrm{Hol}\,(B, +) := B \times \mathrm{Aut}\,(B)$ with the product

$$(a, \alpha)\,(b, \beta) := (a + \alpha\,(b)\,,\ \alpha\beta)$$

- $\mathrm{pr}_1 : \mathrm{Hol}\,(B) \to B, (a, \alpha) \mapsto a$ be the first projection

Any $N \leq \mathrm{Hol}\,(B)$ acts on B
for all $(a, \alpha) \in N$ and $x \in B$ via

$$(a, \alpha) \cdot x = \mathrm{pr}_1\,((a, \alpha)\,(x, \mathrm{id}_B)) = a + \alpha\,(x)\,.$$

Regular subgroups

- B – a group
- $\mathrm{Hol}\,(B,+)$ – the holomorph of B
- $N \leq \mathrm{Hol}\,(B)$

N is regular if for all $a, b \in B$ there exists a unique $(x, \chi) \in N$ s.t.

$$(x, \chi) \cdot a = b.$$

E.g. $N = \{(a, \mathrm{id}) \mid a \in B\}$ is a regular subgroup.

Regular subgroups

- B – a group
- $\mathrm{Hol}\,(B,+)$ – the holomorph of B
- $N \leq \mathrm{Hol}\,(B)$

N is regular if for all $a, b \in B$ there exists a unique $(x, \chi) \in N$ s.t.

$$(x, \chi) \cdot a = b.$$

E.g. $N = \{(a, \mathrm{id}) \mid a \in B\}$ is a regular subgroup.

Skew braces and regular subgroups of $\mathrm{Hol}\,(B,+)$

- $(B,+)$ – a group
- $\mathcal{SB}$ – all skew braces with additive group $(B,+)$
- $\mathcal{R}$ – all regular subgroups of $\mathrm{Hol}\,(B,+)$

It holds that

- If $B^\circ = (B,+,\circ) \in \mathcal{SB}$, then $N_{B^\circ} := \{\,(a,\lambda_a) \mid a \in B\} \in \mathcal{R}$.
- The map $f\colon \mathcal{SB} \to \mathcal{R}$, $B^\circ \mapsto N_{B^\circ}$ is a bijection.

Moreover

isomorphic skew left braces	$\longleftrightarrow$	Regular subgroups of $\mathrm{Hol}\,(B)$ conjugated under the action of $\mathrm{Aut}\,(B)$.

Thanks for your attention!