BRACES

Between regular subgroups and solutions of the Yang-Baxter equation

Ilaria Colazzo

ilaria.colazzo@vub.ac.be

A4C2019 – 1st workshop in Algebra for Cryptography

October 11, 2019

VRIJE UNIVERSITEIT BRUSSEL

OVERVIEW

1. Basic definition
2. Braces and regular subgroups
3. Constructions of braces over a field
4. Extension of the Catino-Rizzo correspondence
5. Yang-Baxter equation

FINITE PRIMITIVE PERMUTATION GROUPS

CONTAINING A REGULAR SUBGROUP

- 1900. Primitive permutation group containing a cyclic group of prime-power is 2-transitive or has prime degree [Burnside]

Extensions

1933
to general cyclic group
[Schur]

1935
to abelian group which contain a regular elementary abelian 2-group
[Wielandt]

FINITE PRIMITIVE PERMUTATION GROUPS

CONTAINING A REGULAR SUBGROUP

- 1900. Primitive permutation group containing a cyclic group of prime-power is 2-transitive or has prime degree [Burnside]

Extensions

1933
to general cyclic group [Schur]

1935
to abelian group which contain a regular elementary abelian 2-group [Wielandt]

FINITE PRIMITIVE PERMUTATION GROUPS

CONTAINING A REGULAR SUBGROUP

- 1900. Primitive permutation group containing a cyclic group of prime-power is 2-transitive or has prime degree [Burnside]

Extensions

1933
to general cyclic group [Schur]

1935
to abelian group which contain a regular elementary abelian 2-group [Wielandt]

- 1979. Finite simple primitive groups with a cyclic regular subgroup

  (by classification of finite group) [Fit]
- 1982. Insolvable primitive permutation groups with a cyclic regular subgroup

  [Gorenstein]
- 2000. A non-abelian regular subgroup of particular affine group

  ↑ [Hegedűs]

  In AGL, there are regular abelian subgroups other than the translation group
- 2003. Classify finite primitive permutation groups with an abelian subgroup

  [Cai Heng Li]

- 1979. Finite simple primitive groups with a cyclic regular subgroup

  (by classification of finite group) [Fit]

- 1982. Insolvable primitive permutation groups with a cyclic regular subgroup

  [Gorenstein]

- 2000. A non-abelian regular subgroup of particular affine group

  [Hegedűs]

  In AGL, there are regular abelian subgroups other than the translation group

- 2003. Classify finite primitive permutation groups with an abelian subgroup

  [Cai Heng Li]

- 1979. Finite simple primitive groups with a cyclic regular subgroup

  (by classification of finite group) [Fit]

- 1982. Insolvable primitive permutation groups with a cyclic regular subgroup

  [Gorenstein]

- 2000. A non-abelian regular subgroup of particular affine group

  [Hegedűs]

  ↑

  In AGL, there are regular abelian subgroups other than the translation group

- 2003. Classify finite primitive permutation groups with an abelian subgroup

  [Cai Heng Li]

- 1979. Finite simple primitive groups with a cyclic regular subgroup

  (by classification of finite group) [Fit]

- 1982. Insolvable primitive permutation groups with a cyclic regular subgroup

  [Gorenstein]

- 2000. A non-abelian regular subgroup of particular affine group

  ↑ [Hegedűs]

  In AGL, there are regular abelian subgroups other than the translation group

- 2003. Classify finite primitive permutation groups with an abelian subgroup

  [Cai Heng Li]

- 1979. Finite simple primitive groups with a cyclic regular subgroup

  (by classification of finite group) [Fit]
- 1982. Insolvable primitive permutation groups with a cyclic regular subgroup

  [Gorenstein]
- 2000. A non-abelian regular subgroup of particular affine group

  ↑ [Hegedűs]

  In AGL, there are regular abelian subgroups other than the translation group
- 2003. Classify finite primitive permutation groups with an abelian subgroup

  [Cai Heng Li]

- 2006. Description of all abelian regular subgroups of an affine group

  $\uparrow$ [Caranti, Della Volta, Sala]

  via commutative algebras
- 2009. Problem of determining all regular subgroups of the affine group

  [Liebeck, Praeger and Saxl]
- 2009. Description of all regular subgroups of an affine group

  $\uparrow$ [Catino, Rizzo]

  via *F*-braces

- 2006. Description of all abelian regular subgroups of an affine group

  ↑ [Caranti, Della Volta, Sala]

  via commutative algebras
- 2009. Problem of determining all regular subgroups of the affine group

  [Liebeck, Praeger and Saxl]
- 2009. Description of all regular subgroups of an affine group

  ↑ [Catino, Rizzo]

  via *F*-braces

- 2006. Description of all abelian regular subgroups of an affine group

  ↑ [Caranti, Della Volta, Sala]

  via commutative algebras
- 2009. Problem of determining all regular subgroups of the affine group

  [Liebeck, Praeger and Saxl]
- 2009. Description of all regular subgroups of an affine group

  ↑ [Catino, Rizzo]

  via F-braces

- 2006. Description of all abelian regular subgroups of an affine group

  $\uparrow$ [Caranti, Della Volta, Sala]

  via commutative algebras
- 2009. Problem of determining all regular subgroups of the affine group

  [Liebeck, Praeger and Saxl]
- 2009. Description of all regular subgroups of an affine group

  $\uparrow$ [Catino, Rizzo]

  via *F*-braces

PRIMITIVE GROUP

X a set $\qquad G \leq \mathrm{Sym}(X) \qquad x \in G$

$$x^G := \{\pi(x) \mid \pi \in G\} \qquad\qquad G_x := \{\pi \mid \pi \in G, \pi(x) = x\}$$

$\uparrow$ orbit of x $\qquad$ $\uparrow$ stabilizer subgroup of x

- G is transitive on X if there exists a unique orbit

$$\Updownarrow$$

$$\forall x, y \in X \quad \exists \pi \in G \text{ s.t. } \pi(x) = y$$

- G is primitive if G is transitive and there is no partition of X preserved by G except for the trivial partitions

$\downarrow$ the partition with a single part, and the partition into singletons

E.g. $\mathrm{Sym}(n)$ is primitive for any $n \in \mathbb{N}$.

PRIMITIVE GROUP

X a set $\quad G \leq \mathrm{Sym}(X) \quad x \in G$

$$x^G := \{\pi(x) \mid \pi \in G\} \qquad G_x := \{\pi \mid \pi \in G, \pi(x) = x\}$$

orbit of x — stabilizer subgroup of x

- G is transitive on X if there exists a unique orbit

$$\Updownarrow$$

$$\forall x, y \in X \quad \exists \pi \in G \text{ s.t. } \pi(x) = y$$

- G is primitive if G is transitive and there is no partition of X preserved by G except for the trivial partitions

$$\downarrow$$

the partition with a single part, and the partition into singletons

E.g. $\mathrm{Sym}(n)$ is primitive for any $n \in \mathbb{N}$.

PRIMITIVE GROUP

X a set $\quad G \leq \mathrm{Sym}(X) \quad x \in G$

$$x^G := \{\pi(x) \mid \pi \in G\} \qquad G_x := \{\pi \mid \pi \in G, \pi(x) = x\}$$

orbit of x $\qquad$ stabilizer subgroup of x

- G is transitive on X if there exists a unique orbit

  $\Updownarrow$

  $\forall x, y \in X \quad \exists \pi \in G$ s.t. $\pi(x) = y$
- G is primitive if G is transitive and there is no partition of X preserved by G except for the trivial partitions

  $\downarrow$

  the partition with a single part, and the partition into singletons

E.g. $\mathrm{Sym}(n)$ is primitive for any $n \in \mathbb{N}$.

PRIMITIVE GROUP

X a set $\qquad G \leq \mathrm{Sym}(X) \qquad x \in G$

$$x^G := \{\pi(x) \mid \pi \in G\} \qquad G_x := \{\pi \mid \pi \in G, \pi(x) = x\}$$

$\uparrow$ orbit of x $\qquad$ $\uparrow$ stabilizer subgroup of x

- G is transitive on X if there exists a unique orbit

  $\Updownarrow$

  $\forall x, y \in X \quad \exists \pi \in G$ s.t. $\pi(x) = y$
- G is primitive if G is transitive and there is no partition of X preserved by G except for the trivial partitions

  $\downarrow$

  the partition with a single part, and the partition into singletons

E.g. $\mathrm{Sym}(n)$ is primitive for any $n \in \mathbb{N}$.

PRIMITIVE GROUP

X a set $\qquad G \leq \mathrm{Sym}(X) \qquad x \in G$

$$x^G := \{\pi(x) \mid \pi \in G\} \qquad\qquad G_x := \{\pi \mid \pi \in G, \pi(x) = x\}$$

$\uparrow$ orbit of x $\qquad\qquad$ $\uparrow$ stabilizer subgroup of x

- G is transitive on X if there exists a unique orbit

$$\Updownarrow$$

$$\forall x, y \in X \quad \exists \pi \in G \text{ s.t. } \pi(x) = y$$

- G is primitive if G is transitive and there is no partition of X preserved by G except for the $\underline{\text{trivial partitions}}$

$\downarrow$

the partition with a single part, and the partition into singletons

E.g. $\mathrm{Sym}(n)$ is primitive for any $n \in \mathbb{N}$.

THE AFFINE GROUP OF A VECTOR SPACE

If V is a vector space over a field F the group

$$\mathrm{AGL}(V) := \langle \underbrace{\mathrm{GL}(V)}_{\text{linear group of } V}, \underbrace{\mathrm{T}(V)}_{\text{group of translation of } V} \rangle$$

It is easy to see that

- $T(V) \trianglelefteq AGL(V)$
- $GL(V) \cap T(V) = 1$ $\iff$ $AGL(V) = GL(V) \ltimes T(V)$
- $AGL(V) = GL(V)T(V)$

$\mathrm{AGL}(V)$ can be identified with the set of all pairs (a, α) with $a \in V$ and $\alpha \in \mathrm{GL}(V)$ with respect to the product

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

THE AFFINE GROUP OF A VECTOR SPACE

If V is a vector space over a field F the group

$$\mathrm{AGL}(V) := \langle \underbrace{\mathrm{GL}(V)}_{\text{linear group of } V}, \underbrace{\mathrm{T}(V)}_{\text{group of translation of } V} \rangle$$

It is easy to see that

- $T(V) \trianglelefteq AGL(V)$
- $GL(V) \cap T(V) = 1$ $\qquad \Longleftrightarrow \qquad AGL(V) = GL(V) \ltimes T(V)$
- $AGL(V) = GL(V)T(V)$

$\mathrm{AGL}(V)$ can be identified with the set of all pairs (a, α) with $a \in V$ and $\alpha \in \mathrm{GL}(V)$ with respect to the product

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

THE AFFINE GROUP OF A VECTOR SPACE

If V is a vector space over a field F the group

$$\mathrm{AGL}(V) := \langle \underbrace{\mathrm{GL}(V)}_{\text{linear group of } V}, \underbrace{\mathrm{T}(V)}_{\text{group of translation of } V} \rangle$$

It is easy to see that

- $T(V) \trianglelefteq AGL(V)$
- $GL(V) \cap T(V) = 1$ $\qquad \Longleftrightarrow \qquad AGL(V) = GL(V) \ltimes T(V)$
- $AGL(V) = GL(V)T(V)$

$\mathrm{AGL}(V)$ can be identified with the set of all pairs (a, α) with $a \in V$ and $\alpha \in \mathrm{GL}(V)$ with respect to the product

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

THE AFFINE GROUP OF A VECTOR SPACE

If V is a vector space over a field F the group

$$\mathrm{AGL}(V) := \langle \underbrace{\mathrm{GL}(V)}_{\text{linear group of } V}, \underbrace{\mathrm{T}(V)}_{\text{group of translation of } V} \rangle$$

It is easy to see that

- $T(V) \trianglelefteq AGL(V)$
- $GL(V) \cap T(V) = 1$ $\iff$ $AGL(V) = GL(V) \ltimes T(V)$
- $AGL(V) = GL(V)T(V)$

AGL(V) can be identified with the set of all pairs (a, α) with $a \in V$ and $\alpha \in \mathrm{GL}(V)$ with respect to the product

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

THE AFFINE GROUP OF A VECTOR SPACE

If V is a vector space over a field F the group

$$\mathrm{AGL}(V) := \langle \underbrace{\mathrm{GL}(V)}_{\text{linear group of } V}, \underbrace{\mathrm{T}(V)}_{\text{group of translation of } V} \rangle$$

It is easy to see that

- $T(V) \trianglelefteq AGL(V)$
- $GL(V) \cap T(V) = 1$ $\quad\Longleftrightarrow\quad AGL(V) = GL(V) \ltimes T(V)$
- $AGL(V) = GL(V)T(V)$

$\mathrm{AGL}(V)$ can be identified with the set of all pairs (a, α) with $a \in V$ and $\alpha \in \mathrm{GL}(V)$ with respect to the product

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

REGULAR SUBGROUP OF $AGL(V)$

$G \leq AGL(V)$ is regular if, for all $x, y \in V$, there exists a unique $\pi \in G$ such that $\pi(x) = y$.

$G \leq \mathrm{AGL}(V)$ regular $\iff$ $\exists \phi : V \to \mathrm{GL}(V), a \mapsto \phi_a$ s.t. $\phi_a \phi_b = \phi_{a+\phi_a(b)}$ and $G = \{(a, \phi_a) \mid a \in V\}$

E.g. The translation group $T(V) = \{(a, \mathrm{id}) \mid a \in V\}$ is an abelian regular subgroups of $AGL(V)$.

If T is a regular subgroup of $\mathrm{AGL}(V)$ then its conjugate by an element of $\mathrm{GL}(V)$ is still a regular subgroup.

REGULAR SUBGROUP OF $AGL(V)$

$G \leq AGL(V)$ is regular if, for all $x, y \in V$, there exists a unique $\pi \in G$ such that $\pi(x) = y$.

$$G \leq \mathrm{AGL}(V) \text{ regular} \iff \begin{array}{l} \exists \phi : V \to \mathrm{GL}(V), a \mapsto \phi_a \text{ s.t.} \\ \phi_a \phi_b = \phi_{a+\phi_a(b)} \text{ and} \\ G = \{(a, \phi_a) \mid a \in V\} \end{array}$$

E.g. The translation group $T(V) = \{(a, \mathrm{id}) \mid a \in V\}$ is an abelian regular subgroups of $AGL(V)$.

If T is a regular subgroup of $\mathrm{AGL}(V)$ then its conjugate by an element of $\mathrm{GL}(V)$ is still a regular subgroup.

EMBEDDING OF $AGL(N, F)$ INTO $GL(N+1, F)$

- V an n-dimensional vector ($n \in \mathbb{N}$) space over F
- fix a basis of V
- define the group monomorphism

$$\theta : \mathrm{AGL}(n, F) \longrightarrow GL(n+1, F), \quad (a, \alpha) \mapsto \begin{pmatrix} 1 & a \\ 0 & \alpha \end{pmatrix}$$

$\mathrm{AGL}(n, F)$ acts on the right on the set of affine vectors $\Omega := \{\, (1, v) \mid v \in F^n \}$.

EMBEDDING OF $AGL(N, F)$ INTO $GL(N+1, F)$

If T is a regular subgroup of $\mathrm{AGL}(n, F)$ then there exists $\phi : V \to \mathrm{GL}(V)$ s.t.

$$T = \{ (a, \phi_a) \mid a \in V \} .$$

Hence, if we consider $\mathrm{AGL}(n, F) \hookrightarrow \mathrm{GL}(n+1, F)$, for every $a \in F^n$ there is a unique element of T that has $(1, a)$ as first row:

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & \phi_a \end{pmatrix} \middle| \; a \in F^n \right\} .$$

REGULAR SUBGROUPS OF $AGL(2, F)$

Let F be a field and σ an endomorphism of the additive group of F. Then

$$T := \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & \sigma(x) \\ 0 & 0 & 1 \end{pmatrix} \middle| \; x, y \in F \right\}$$

is a regular subgroup of the affine group $AGL(2, F)$.

In particular, T is abelian if and only if σ is linear, i.e., $\sigma(xy)\sigma = x\sigma(y)$.

REGULAR SUBGROUPS OF $AGL(2, F)$

Let F be a field and σ an endomorphism of the additive group of F. Then

$$T := \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & \sigma(x) \\ 0 & 0 & 1 \end{pmatrix} \middle| \; x, y \in F \right\}$$

is a regular subgroup of the affine group $AGL(2, F)$.

In particular, T is abelian if and only if σ is linear, i.e., $\sigma(xy)\sigma = x\sigma(y)$.

BRACES OVER A FIELD

Let F be a field, $(B, +)$ a vector space over F and $\circ$ an operation over B such that $(B, \circ)$ is a group. We say that $(B, +, \circ)$ is an F-brace (or a brace over the field F) if the following relations hold

$$a \circ (b + c) + a = a \circ b + a \circ c$$
$$\mu(a \circ b) = a \circ (\mu b) + (\mu - 1)a.$$

E.g. Let $(B, +)$ be a vector space over F. Define $a \circ b = a + b$, then $(B, +, \circ)$ is an F-brace.

If B is a radical algebra over F and we consider the adjoint operation $a \circ b := ab + a + b$. Then $(B, +, \circ)$ is an F-brace.

Remark

An algebra B is radical if B with respect to the adjoint operation $a \circ b$ is a group.

F-BRACES AND REGULAR SUBGROUPS

CATINO, RIZZO (2019)

- B a vector space over a field F
- $\mathcal{FB}$ the class of F-braces with underlying vector space B
- $\mathcal{R}$ the set of all regular subgroups of $\mathrm{AGL}(B)$ the affine group of B

It holds that

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

Moreover

isomorphic F-braces $\quad\longleftrightarrow\quad$ regular subgroups of $\mathrm{AGL}(B)$ conjugated under the action of $\mathrm{GL}(B)$.

COMMUTATIVE ALGEBRAS AND REGULAR SUBGROUPS

CARANTI, DELLA VOLTA, SALA (2006)

Remark

If B is a commutative F-brace then B is a commutative radical algebra with respect to the multiplication defined by $ab = a \circ b - a - b$.

Hence, as direct consequence of the previous result, we have

- B a vector space over a field F
- $\mathcal{RA}$ the class of commutative radical algebras with underlying vector space B
- $\mathcal{AR}$ the set of all abelian regular subgroups of $\mathrm{AGL}(B)$ the affine group of B

It holds that

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

F-BRACES AND REGULAR SUBGROUPS

F. CATINO, R. RIZZO (2009) - PROOF

Proof (sketch)

$B^\circ = (B, +, \circ)$ an F-brace. For any $x \in B$, define the map

$$\lambda_x : B \longrightarrow B, \quad y \longmapsto -x + x \circ y.$$

- $(x, \lambda_x) \in \mathrm{AGL}\,(B)$.
- Note that $(x, \lambda_x)\,(y, \lambda_y) = (x + \lambda_x\,(y)\,, \lambda_x \lambda_y) = (x \circ y, \lambda_{x \circ y})$.
- The map $f : B \to AGL(B), x \mapsto (x, \lambda_x)$ is a group monomorphism from $(B, \circ)$ into $\mathrm{AGL}(B)$ and $f\,(B) = N_{B^\circ}$.

Hence, N_{B° is a regular subgroup of $AGL(V)$.

F-BRACES AND REGULAR SUBGROUPS

Conversely, if T is a regular subgroup of $\mathrm{AGL}(B)$, then

$$T = \{(x, \lambda_x) \mid x \in B\}.$$

Define the following operation on B

$$\forall x, y \in V, \quad x \circ y := x + \lambda_x(y)$$

Therefore $V^\circ = (V, +, \circ)$ is an F-brace and $N_{B^\circ} = T$.
Then

- $V^\circ, V^* \in \mathcal{FB}$
- $\varphi : V^\bullet \to V^*$ be an isomorphism, in particular $\varphi \in GL(B)$
- $N_{B^\circ} = \{(x, \lambda_x^\circ) \mid x \in B\}$ and $N_{B^*} = \{(x, \lambda_x^*) \mid x \in B\}$.

It follows that $(0, \varphi)(x, \lambda_x^\circ)\left(0, \varphi^{-1}\right) = \left(\varphi(x), \varphi\lambda^\circ\varphi^{-1}\right) = \left(\varphi(x), \lambda_{\varphi x}^*\right)$.

F-BRACES AND REGULAR SUBGROUPS

Finally,

- $N_1 := \left\{ \left(a, \phi_a^{(1)}\right) \middle| a \in V \right\}, N_2 := \left\{ \left(a, \phi_a^{(2)}\right) \middle| a \in V \right\}$ be regular subgroups of $\mathrm{AGL}(V)$
- $\varphi \in \mathrm{GL}(V)$ such that $(0, \varphi) N_1 \left(0, \varphi^{-1}\right) = N_2$
- Set $a \circ b := a + \phi_a^{(1)}(b)$ and $a * b := a + \phi_a^{(2)}(b)$

Then φ is an isomorphism from $(V, +, \circ)$ into $(V, +, *)$, i.e., the left semi-braces corresponding to N_1 and N_2 respectively are isomorphic.

THE INTERSECTION WITH THE TRANSLATION GROUP

- F a field
- $\mathrm{T}(V)$ the translation group of V
- $V^\circ = (V, +, \circ)$ a left F-brace
- $N_{V^\circ} = f(V^\circ) \leq \mathrm{AGL}(V)$ regular associated with V°

Then

$$\mathrm{T}(V) \cap N_{V^\circ} = \{(a, \mathrm{id}_V) \mid a \in V,\ \forall b \in V \quad a + b = a \circ b\}.$$

Proof

$$T(V) := \{(a, \mathrm{id}_V) \mid a \in V\}$$
$$\Downarrow$$
$$a \in T(V) \cap N_{V^\circ} \iff \lambda_a = \mathrm{id}_B \iff \forall b \in V\ a \circ b = a + b$$

Remark

In braces terms, the set

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

is an extensively study substructure know as socle

F-BRACES WITH NON-TRIVIAL ANNIHILATOR

CATINO, I.C., STEFANELLI (2015)

- F a field
- V an F-brace

The F-annihilator of V is the set

$$\mathrm{Ann}_F(V) := \{a \mid a \in V \text{ s.t. } (\mu a) \circ b = (\mu a) + b = b \circ (\mu a) \ \ \forall b \in B\ \forall \mu \in F\}$$

Remark

- $\mathrm{Ann}_F(V)$ is an ideal and a subspace of V
- $\bar{V} := V/\mathrm{Ann}_F(V)$ is a left F-brace

If $(T, +)$ is a vector space over F, a map $\theta : V \times V \to T$ such that

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

is called 2-cocycle of left F-brace V with values in T.

F-BRACE WITH NON-TRIVIAL ANNIHILATOR

- F a field
- T an F-space
- V an F-brace
- $\theta : V \times V \to T$ a 2-cocycle of V with values in T

Define

$$\begin{aligned} \mu(a, v) &:= (\mu a, \mu v) \\ (a, v) + (b, w) &:= (a + b, v + w) \\ (a, v) \circ (b, w) &:= (a \circ b, v + w + \theta(a, b)), \end{aligned}$$

Then $(V \times T, +, \circ)$ is a left F-brace, called a Hochschild product of the F-brace V by T (via θ).

F-BRACE WITH NON-TRIVIAL ANNIHILATOR

Conversely

- F a field
- V an F-brace with $\mathrm{Ann}_F(V) \neq \{0\}$
- $T := \mathrm{Ann}_F(B)$

Then there exists a 2-cocycle θ of the F-brace $\bar{V} := V/T$ with values in T s.t. V is isomorphic to the Hochschild product of $\bar{V}$ by V (via θ).

Proof (sketch)

Set

- $T := \mathrm{Ann}_F(V)$
- $\bar{V} := V/\mathrm{Ann}_F(V)$
- $\pi : B \to \bar{B}$ the projection map

Choose a linear map $s : \bar{V} \to V$ s.t. $\pi(s(\bar{b})) = \bar{b}$.

The map $\theta : \bar{V} \times \bar{V} \to T$ defined by

$$\theta(\bar{b}_1, \bar{b}_2) := -s(\bar{b}_1 \circ \bar{b}_2) + s(\bar{b}_1) \circ s(\bar{b}_2),$$

is a 2-cocycle. Consider the F-brace Hochschild product of V by T (via θ). Finally, $\psi : \bar{V} \times T \to V$, defined by $\psi(\bar{b}, i) = s(\bar{b}) + i$, is an isomorphism from the Hochschild product of $\bar{V}$ by T (via θ) into V.

F-BRACE WITH NON-TRIVIAL ANNIHILATOR

AN EXAMPLE

- N the zero 1-dimensional algebra over F
- (e_1) a basis of N
- $\tau \in \operatorname{End}(F,+)$

The map $\theta : N \times N \to F$ such that

$$\theta(x_1e_1, y_1e_1) := \tau(x_1)\, y_1$$

is a 2-cocycle of the left F-brace N, but it is a 2-cocycle of the F-algebra N if and only if τ is linear.

Conversely, if θ a 2-cocycle on N, as left F-brace then there exists $\tau \in \operatorname{End}(F,+)$ such that

$$\theta(x_1e_1, y_1e_1) = \tau(x_1)\, y_1.$$

$\Longrightarrow$ θ are the unique 2-cocycles of a 1-dimensional zero algebra

F-BRACE WITH NON-TRIVIAL ANNIHILATOR

AN EXAMPLE

Hence, all regular subgroups of $\mathrm{AGL}\left(F^2\right)$ with non trivial intersection with the translation group are given by

$$\left\{ \left(\begin{array}{ccc} 1 & x & y \\ 0 & 1 & \tau(x) \\ 0 & 0 & 1 \end{array} \right) \middle| \; x, y \in F \right\},$$

for every τ automorphism of $(F, +)$.

HEGEDŰS' SUBGROUPS

- p a prime
- If $p = 2$, assume $n = 3$, or $n \geq 5$
- If p is odd, assume $n \geq 3$ odd

Then the affine group $AGL(n, \mathbb{F}_p)$ has a regular subgroup which contains no translations other than the identity.

Proof (sketch)

- $\mathfrak{q} : \mathbb{F}_p^{n-1} \to \mathbb{F}_p$ a non-degenerate quadratic form
- $\mathfrak{b} : \mathbb{F}_p^{n-1} \times \mathbb{F}_p^{n-1} \to \mathbb{F}_p$ the symmetric bilinear form associated to $\mathfrak{q}$
- X the matrix associated to $\mathfrak{b}$ with respect to a fixed basis (i.e., $\mathfrak{q}(x+y) = \mathfrak{q}(v) + \mathfrak{q}(w) + vXw^T$)
- A an orthogonal non-singular $(n-1) \times (n-1)$-matrix (i.e., $XA^T = A^{-1}X$) of order p such that $\mathfrak{q}(v) = \mathfrak{q}(vA)$

HEGEDŰS' SUBGROUPS

- p a prime
- If $p = 2$, assume $n = 3$, or $n \geq 5$
- If p is odd, assume $n \geq 3$ odd

Then the affine group $AGL(n, \mathbb{F}_p)$ has a regular subgroup which contains no translations other than the identity.

Proof (sketch)

- $\mathfrak{q} : \mathbb{F}_p^{n-1} \to \mathbb{F}_p$ a non-degenerate quadratic form
- $\mathfrak{b} : \mathbb{F}_p^{n-1} \times \mathbb{F}_p^{n-1} \to \mathbb{F}_p$ the symmetric bilinear form associated to $\mathfrak{q}$
- X the matrix associated to $\mathfrak{b}$ with respect to a fixed basis (i.e., $\mathfrak{q}(x + y) = \mathfrak{q}(v) + \mathfrak{q}(w) + vXw^T$)
- A an orthogonal non-singular $(n-1) \times (n-1)$-matrix (i.e., $XA^T = A^{-1}X$) of order p such that $\mathfrak{q}(v) = \mathfrak{q}(vA)$

HEGEDŰS' SUBGROUPS

Then the set

$$H := \left\{ \begin{pmatrix} 1 & \mathfrak{q}(v) & v \\ 0 & 1 & 0 \\ 0^T & A^m X v^T & A^m \end{pmatrix} \,\middle|\, m \in \mathbb{F}_p, v \in \mathbb{F}_p^{n-1} \right\}$$

is a regular subgroup of the affine group $AGL(n, p)$ that has trivial intersection with the translation group.

In particular, this group is not abelian. In fact, if V is a finite dimensional vector space and T is an abelian regular subgroup of the affine group $AGL(V)$, then T has nontrivial intersection with the translation group.

THE ASYMMETRIC PRODUCT OF ZERO F-BRACES

CATINO, I.C., STEFANELLI (2016)

- F a field of characteristic p
- H, N zero F-braces (i.e., s.t. $a \circ b = a + b$)
- $\beta : N \to \operatorname{Aut}(H)$ a group homomorphism from $(H, \circ)$ into $\operatorname{Aut}(H, +, \circ)$
- $\mathfrak{b} : H \times H \to N$ a bilinear and symmetric map (if $p \neq 2$)
- $\mathfrak{q}$ a quadratic form and $\mathfrak{b}$ its polar form (if $p = 2$)

that satisfy

$$\mathfrak{b}(h_1, h_2) = ({}^n h_1, {}^n h_2) \qquad \text{(if } p \neq 2\text{)}$$

$$\mathfrak{q}({}^n h) = \mathfrak{q}(h) \qquad \text{(if } p = 2\text{)}$$

THE ASYMMETRIC PRODUCT OF ZERO F-BRACES

The sum, the multiplication, and the scalar multiplication

$$
\begin{aligned}
(h_1, n_1) + (h_2, n_2) &:= (h_1 + h_2, \mathfrak{b}(h_1, h_2) + n_1 + n_2) \\
(h_1, n_1) \circ (h_2, n_2) &:= (h_1 \circ {}^{n_1}h_2, n_1 \circ n_2) \\
\mu (h, n) &:= \left(\mu h, \frac{\mu(\mu - 1)}{2} \mathfrak{b}(h, h) + \mu n\right) && \text{(if } p \neq 2\text{)} \\
\mu (h, n) &:= (\mu h, \mu(\mu + 1) \mathfrak{q}(h) + \mu n) && \text{(if } p = 2\text{)}
\end{aligned}
$$

define a structure of F-brace over $H \times N$ called the Asymmetric Product H by N and denoted by $H \rtimes_\circ N$.

THE INTERSECTION WITH THE TRANSLATION GROUP

We check the intersection of the regular subgroup associated to $V := H \rtimes_\circ N$ with the translation group $\mathrm{T}(V)$ via the socle:

$$N_V \cap \mathrm{T}(V) = \{(a, \mathrm{id}_V) \mid a \in \mathrm{Soc}(V)\}.$$

Then

$$(h, n) \in \mathrm{Soc}(H \rtimes_\circ N) \iff h \in \mathrm{rad}\,\mathfrak{b} \text{ and } \beta(n) = id_H$$

where $\mathrm{rad}\,\mathfrak{b} = \{h \mid h \in H, \forall k \in H\ \mathfrak{b}(h, k) = 0\}$.

GENERALIZATION OF HEGEDŰS' SUBGROUPS

p a prime, $m \in \mathbb{N}$. If one of the following conditions hold

- p odd, $m = 1$ and $n \geq 3$;
- p odd, $m > 1$ and $n \geq 4$;
- $p = 2$, $m = 1$ and $n = 3$ or $n \geq 5$;
- $p = 2$, $m > 1$ and $n = 4, n = 6$ or $n \geq 8$,

then the affine group $\mathrm{AGL}(n+1, p^m)$ contains a regular subgroup having trivial intersection with the translation group.

GENERALIZATION OF HEGEDŰS' SUBGROUPS

Proof (sketch)

$m = 1$, $n \geq 3$ and p odd or $n \geq 2$, n even and $p = 2$ $\Longrightarrow$ $\exists \mathfrak{q} : \mathbb{F}_p^n \to \mathbb{F}_p$ s.t. its polar form $\mathfrak{b}$ is non-degenerate

$p \mid |O(V, \mathfrak{q})|$ $\Longrightarrow$ $\exists A \in O(V, \mathfrak{q})$ of order p

Define

$$\beta : \mathbb{F}_p \to \mathbb{F}_p^n m \qquad \text{s.t. } \beta(1) = A.$$

Consider $\mathbb{F}_p^n \rtimes_\circ \mathbb{F}_p$ its multiplicative group is a regular subgroup of $\mathrm{AGL}(n+1, \mathbb{F}_p)$ and since β is faithful and $\mathfrak{b}$ is non-degenerate its intersection with the translation group is trivial.

GENERALIZATION OF HEGEDŰS' SUBGROUPS

$m > 1$ $n \geq 4$ and p odd or $n \geq 4$, n even and $p = 2$	$\Longrightarrow$	$\exists \mathfrak{q} : \mathbb{F}_{p^m}^n \to \mathbb{F}_{p^m}$ an isotropic s.t. its polar form $\mathfrak{b}$ is non-degenerate

$\exists A_1, \dots A_m \in O(V, \mathfrak{q})$ of order p that pairwise commute
Define the group homomorphism

$$\beta : \mathbb{F}_{p^m} = \bigoplus_{i=1}^{m} \langle \omega_i \rangle \longrightarrow \mathrm{GL}(n, \mathbb{F}_{p^m})$$

s.t. $\beta(\omega_i) = A_i$.
The multiplicative group of the left $\mathbb{F}_{p^m}$-brace $\mathbb{F}_{p^m} \rtimes_\circ \mathbb{F}_{p^m}^n$ is a regular subgroup of the affine group. Since β is faithful and $\mathfrak{b}$ is non-degenerate this subgroup has trivial intersection with the translation group.

GENERALIZATION OF HEGEDŰS' SUBGROUPS

$p = 2 \quad m = 1$ and $n \geq 5$
or $m > 1$ $n \geq 9$, n odd

Consider the direct product of two left $\mathbb{F}_{2^m}$-braces:

- $B_1 := \mathbb{F}_{2^m}^{n_1} \rtimes_\circ \mathbb{F}_{2^m}$
- $B_2 := \mathbb{F}_{2^m}^{n_2} \rtimes_\circ \mathbb{F}_{2^m}$

where n_1, n_2 are even $n_1, n_2 \geq 4$ such that $n_1 + 1 + n_2 + 1 = n + 1$.
The multiplicative group of the $\mathbb{F}_{2^m}$-brace direct product is the direct product of the multiplicative groups of B_1 and B_2.
Since

$$\mathrm{Soc}\,(B_1 \times B_2) = \mathrm{Soc}\,(B_1) \times \mathrm{Soc}\,(B_2)$$

the intersection of the multiplicative group of $B_1 \times B_2$ with the translation group is trivial.

SKEW BRACES

GUARNIERI, VENDRAMIN (2017)

- B a set with two operations $+$ and $\circ$
- $(B, +)$ and $(B, \circ)$ groups

$(B, +, \circ)$ is a skew brace if the following relation holds

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

In particular, if $(B, +)$ is an abelian group, $(B, +, \circ)$ is called a brace.

E.g. $(B, +)$ a group, define $a \circ b := a + b$, $(B, +, \circ)$ is a skew brace.

$(B, +)$ a group, define $a \circ b := b + a$, $(B, +, \circ)$ is a skew brace.

Every F-brace is a skew brace

An additive exactly factorizable group B (i.e., $B = A + C$ for disjoint subgroups A and C) is a skew brace with $x \circ y = a + y + c$, where $x = a + C$, $a \in A$ and $b \in B$.

HOLOMORPH OF A GROUP

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

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

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

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

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

- 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.

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

SKEW BRACES AND REGULAR SUBGROUPS OF $\mathrm{Hol}(B)$

- $(B,+)$ a group
- $\mathcal{SB}$ be the class of skew left braces with additive group $(B,+)$
- $\mathcal{R}$ the set of all regular subgroups of $\mathrm{Hol}(B)$ the holomorph of $(B,+)$

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 $f : \mathcal{SB} \to \mathcal{R}, B^\circ \mapsto N_{B^\circ}$ is a bijection.

Moreover

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

SOLUTIONS OF 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.

SET-THEORETICAL SOLUTIONS

[V. Drinfel'd, 1992] set-theoretical solutions or braided sets.

Given X a set, a map $r : X \times X \to X \times X$ is a set-theoretical solution if

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

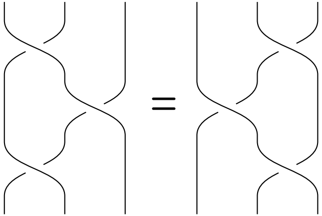
Reidemeister move of type III

SET-THEORETICAL SOLUTIONS

[V. Drinfel'd, 1992] set-theoretical solutions or braided sets.

Given X a set, a map $r : X \times X \to X \times X$ is a set-theoretical solution if

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



Reidemeister move of type III

SOLUTIONS OF THE YANG-BAXTER EQUATION

If X is a set, $r : X \times X \to X \times X$ is a solution and $a, b \in X$, then we denote

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

where λ_a, ρ_b are maps from X into itself.

We say that r is

- left (resp. right) non-degenerate if λ_a (resp. ρ_a) is bijective, for every $a \in X$;
- non-degenerate if it is both left and right non-degenerate
- involutive if $r^2(a, b) = (a, b)$, for all $a, b \in X$.

E.g. The flip: $r(x, y) = (y, x)$.

If X is a set and $\sigma, \tau : X \to X$ are bijection s.t. $\sigma\tau = \tau\sigma$ then $r(x, y) = (\sigma(y), \tau(x))$ is a solution.

SOLUTIONS OF THE YANG-BAXTER EQUATION

If X is a set, $r : X \times X \to X \times X$ is a solution and $a, b \in X$, then we denote

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

where λ_a, ρ_b are maps from X into itself.

We say that r is

- left (resp. right) non-degenerate if λ_a (resp. ρ_a) is bijective, for every $a \in X$;
- non-degenerate if it is both left and right non-degenerate
- involutive if $r^2(a, b) = (a, b)$, for all $a, b \in X$.

E.g. The flip: $r(x, y) = (y, x)$.

If X is a set and $\sigma, \tau : X \to X$ are bijection s.t. $\sigma\tau = \tau\sigma$ then $r(x, y) = (\sigma(y), \tau(x))$ is a solution.

SOLUTIONS OF THE YANG-BAXTER EQUATION

If X is a set, $r : X \times X \to X \times X$ is a solution and $a, b \in X$, then we denote

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

where λ_a, ρ_b are maps from X into itself.

We say that r is

- left (resp. right) non-degenerate if λ_a (resp. ρ_a) is bijective, for every $a \in X$;
- non-degenerate if it is both left and right non-degenerate
- involutive if $r^2(a, b) = (a, b)$, for all $a, b \in X$.

E.g. The flip: $r(x, y) = (y, x)$.

If X is a set and $\sigma, \tau : X \to X$ are bijection s.t. $\sigma\tau = \tau\sigma$ then $r(x, y) = (\sigma(y), \tau(x))$ is a solution.

SOLUTIONS OF THE YANG-BAXTER EQUATION

If X is a set, $r : X \times X \to X \times X$ is a solution and $a, b \in X$, then we denote

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

where λ_a, ρ_b are maps from X into itself.

We say that r is

- left (resp. right) non-degenerate if λ_a (resp. ρ_a) is bijective, for every $a \in X$;
- non-degenerate if it is both left and right non-degenerate
- involutive if $r^2(a, b) = (a, b)$, for all $a, b \in X$.

E.g. The flip: $r(x, y) = (y, x)$.

If X is a set and $\sigma, \tau : X \to X$ are bijection s.t. $\sigma\tau = \tau\sigma$ then $r(x, y) = (\sigma(y), \tau(x))$ is a solution.

SOLUTIONS OF THE YANG-BAXTER EQUATION

If X is a set, $r : X \times X \to X \times X$ is a solution and $a, b \in X$, then we denote

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

where λ_a, ρ_b are maps from X into itself.

We say that r is

- left (resp. right) non-degenerate if λ_a (resp. ρ_a) is bijective, for every $a \in X$;
- non-degenerate if it is both left and right non-degenerate
- involutive if $r^2(a, b) = (a, b)$, for all $a, b \in X$.

E.g. The flip: $r(x, y) = (y, x)$.

If X is a set and $\sigma, \tau : X \to X$ are bijection s.t. $\sigma\tau = \tau\sigma$ then $r(x, y) = (\sigma(y), \tau(x))$ is a solution.

SOLUTIONS OF THE YANG-BAXTER EQUATION

If X is a set, $r : X \times X \to X \times X$ is a solution and $a, b \in X$, then we denote

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

where λ_a, ρ_b are maps from X into itself.

We say that r is

- left (resp. right) non-degenerate if λ_a (resp. ρ_a) is bijective, for every $a \in X$;
- non-degenerate if it is both left and right non-degenerate
- involutive if $r^2(a, b) = (a, b)$, for all $a, b \in X$.

E.g. The flip: $r(x, y) = (y, x)$.

If X is a set and $\sigma, \tau : X \to X$ are bijection s.t. $\sigma\tau = \tau\sigma$ then $r(x, y) = (\sigma(y), \tau(x))$ is a solution.

SOLUTIONS OF THE YANG-BAXTER EQUATION

If X is a set, $r : X \times X \to X \times X$ is a solution and $a, b \in X$, then we denote

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

where λ_a, ρ_b are maps from X into itself.

We say that r is

- left (resp. right) non-degenerate if λ_a (resp. ρ_a) is bijective, for every $a \in X$;
- non-degenerate if it is both left and right non-degenerate
- involutive if $r^2(a, b) = (a, b)$, for all $a, b \in X$.

E.g. The flip: $r(x, y) = (y, x)$.

If X is a set and $\sigma, \tau : X \to X$ are bijection s.t. $\sigma\tau = \tau\sigma$ then $r(x, y) = (\sigma(y), \tau(x))$ is a solution.

BRIEFLY, THE STATE-OF-THE-ART

- Involutive non-degenerate solutions

1999

[Etingof, Schedler & Soloviev]
[Gateva-Ivanova & Van den Bergh]

2007. [Rump]
2014. [Cedò, Jespers & Okninski]

(via braces)

- bijective non-degenerate solutions

2000

[Lu, Yan & Zhu]
[Soloviev]

2017

[Guarnienri & Vendramin]

(via skew braces)

BRIEFLY, THE STATE-OF-THE-ART

- Involutive non-degenerate solutions

1999

[Etingof, Schedler & Soloviev]
[Gateva-Ivanova & Van den Bergh]

2007. [Rump]
2014. [Cedò, Jespers & Okninski]

(via braces)

- bijective non-degenerate solutions

2000

[Lu, Yan & Zhu]
[Soloviev]

2017

[Guarnienri & Vendramin]

(via skew braces)

BRIEFLY, THE STATE-OF-THE-ART

- Involutive non-degenerate solutions

1999

[Etingof, Schedler & Soloviev]
[Gateva-Ivanova & Van den Bergh]

2007. [Rump]
2014. [Cedò, Jespers & Okninski]

(via braces)

- bijective non-degenerate solutions

2000

[Lu, Yan & Zhu]
[Soloviev]

2017

[Guarnienri & Vendramin]

(via skew braces)

BRIEFLY, THE STATE-OF-THE-ART

- Involutive non-degenerate solutions

1999

[Etingof, Schedler & Soloviev]
[Gateva-Ivanova & Van den Bergh]

2007. [Rump]
2014. [Cedò, Jespers & Okninski]

(via braces)

- bijective non-degenerate solutions

2000

[Lu, Yan & Zhu]
[Soloviev]

2017

[Guarnienri & Vendramin]

(via skew braces)

BRIEFLY, THE STATE-OF-THE-ART

- Involutive non-degenerate solutions

1999

[Etingof, Schedler & Soloviev]
[Gateva-Ivanova & Van den Bergh]

2007. [Rump]
2014. [Cedò, Jespers & Okninski]

(via braces)

- bijective non-degenerate solutions

2000

[Lu, Yan & Zhu]
[Soloviev]

2017

[Guarnienri & Vendramin]

(via skew braces)

BRIEFLY, THE STATE-OF-THE-ART

- Involutive non-degenerate solutions

1999

[Etingof, Schedler & Soloviev]
[Gateva-Ivanova & Van den Bergh]

2007. [Rump]
2014. [Cedò, Jespers & Okninski]

(via braces)

- bijective non-degenerate solutions

2000

[Lu, Yan & Zhu]
[Soloviev]

2017

[Guarnienri & Vendramin]

(via skew braces)

BRIEFLY, THE STATE-OF-THE-ART

- Involutive non-degenerate solutions

1999

[Etingof, Schedler & Soloviev]
[Gateva-Ivanova & Van den Bergh]

2007. [Rump]
2014. [Cedò, Jespers & Okninski]

(via braces)

- bijective non-degenerate solutions

2000

[Lu, Yan & Zhu]
[Soloviev]

2017

[Guarnienri & Vendramin]

(via skew braces)

BRIEFLY, THE STATE-OF-THE-ART

- Involutive non-degenerate solutions

1999

[Etingof, Schedler & Soloviev]
[Gateva-Ivanova & Van den Bergh]

2007. [Rump]
2014. [Cedò, Jespers & Okninski]

(via braces)

- bijective non-degenerate solutions

2000

[Lu, Yan & Zhu]
[Soloviev]

2017

[Guarnienri & Vendramin]

(via skew braces)

SOLUTION ASSOCIATED WITH A SKEW BRACES

GUARNIERI, VENDRAMIN (2017)

$(B, +, \circ)$ a skew brace.
The map $r : B \times B \to B \times B$ defined by

$$r_B(a, b) := \left(-a + a \circ b, (a^- + b)^- \circ b\right)$$

where a^- denotes the inverse of a in $(B, \circ)$, is a non-degenerate solution to the Yang-Baxter equation. Moreover

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

SKEW BRACE ASSOCIATED WITH A SOLUTION

SMOKTUNOWICZ, VENDRAMIN (2018)

(X, r) a non-degenerate solution.
Define the structure group $\rightsquigarrow$ Etingof, Schedler & Soloviev

$$G(X, r) = \langle X \mid xy = uv \text{ whenever } r(x, y) = (u, v) \rangle .$$

Then there exists a unique skew brace structure over $G(X, r)$ such that its associated solution $r_{G(X,r)}$ satisfies

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

where $\iota : X \to G(X, r)$ is the canonical map.

SKEW BRACE ASSOCIATED WITH A SOLUTION

SMOKTUNOWICZ, VENDRAMIN (2018)

(X, r) a non-degenerate solution.
Define the structure group $\leftsquigarrow$ Etingof, Schedler & Soloviev

$$G(X, r) = \langle X \mid xy = uv \text{ whenever } r(x, y) = (u, v) \rangle .$$

Then there exists a unique skew brace structure over $G(X, r)$ such that its associated solution $r_{G(X,r)}$ satisfies

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

where $\iota : X \to G(X, r)$ is the canonical map.

SKEW BRACE ASSOCIATED WITH A SOLUTION

SMOKTUNOWICZ, VENDRAMIN (2018)

(X, r) a non-degenerate solution.
Define the structure group ⇜ Etingof, Schedler & Soloviev

$$G(X, r) = \langle X \mid xy = uv \text{ whenever } r(x, y) = (u, v) \rangle .$$

Then there exists a unique skew brace structure over $G(X, r)$ such that its associated solution $r_{G(X,r)}$ satisfies

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

where $\iota : X \to G(X, r)$ is the canonical map.

Grazie per l'attenzione!