... the Yang-Baxter equation, and Hopf Galois structures

Lorenzo Stefanello, Andrea Caranti

May 25, 2021

Outline

- Introduction

Outline

- Introduction
- The Yang-Baxter equation

Outline

- Introduction
- The Yang-Baxter equation
- Hopf Galois structures

Introduction

Notation and convention

Let $(G, \cdot)$ be a group, and $g \in G$.

Notation and convention

Let $(G, \cdot)$ be a group, and $g \in G$.

- If $\psi \in \mathrm{End}(G, \cdot)$, we write ${}^{\psi}g$ for the image of g under ψ.

Notation and convention

Let $(G, \cdot)$ be a group, and $g \in G$.

- If $\psi \in \mathrm{End}(G, \cdot)$, we write ${}^{\psi}g$ for the image of g under ψ.
- We denote by λ the left regular representation, and by ρ the right regular representation.

Notation and convention

Let $(G, \cdot)$ be a group, and $g \in G$.

- If $\psi \in \mathrm{End}(G, \cdot)$, we write ${}^{\psi}g$ for the image of g under ψ.
- We denote by λ the left regular representation, and by ρ the right regular representation.
- We write $\iota \colon (G, \cdot) \to \mathrm{Aut}(G, \cdot)$ for the homomorphism that sends $g \in G$ to the conjugation-by-g automorphism.

Notation and convention

Let $(G, \cdot)$ be a group, and $g \in G$.

- If $\psi \in \mathrm{End}(G, \cdot)$, we write ${}^{\psi}g$ for the image of g under ψ.
- We denote by λ the left regular representation, and by ρ the right regular representation.
- We write $\iota\colon (G, \cdot) \to \mathrm{Aut}(G, \cdot)$ for the homomorphism that sends $g \in G$ to the conjugation-by-g automorphism.
- If $\psi \in \mathrm{End}(G, \cdot)$, we write $[g, \psi] := g \cdot {}^{\psi}g^{-1}$, and $[G, \psi] = \langle [g, \psi] : g \in G \rangle$.

Notation and convention

Let $(G, \cdot)$ be a group, and $g \in G$.

- If $\psi \in \mathrm{End}(G, \cdot)$, we write ${}^{\psi}g$ for the image of g under ψ.
- We denote by λ the left regular representation, and by ρ the right regular representation.
- We write $\iota \colon (G, \cdot) \to \mathrm{Aut}(G, \cdot)$ for the homomorphism that sends $g \in G$ to the conjugation-by-g automorphism.
- If $\psi \in \mathrm{End}(G, \cdot)$, we write $[g, \psi] := g \cdot {}^{\psi}g^{-1}$, and $[G, \psi] = \langle [g, \psi] : g \in G \rangle$.
- If $(G, \cdot, \circ)$ is a skew brace, we denote by g^{-1} the inverse of g with respect to $\cdot$, and by $\overline{g}$ the inverse of g with respect to $\circ$.

Theorem ([Guarnieri and Vendramin, 2017])

Let $(G, \cdot)$ *be a group. The following data are equivalent.*

Gamma functions

Theorem ([Guarnieri and Vendramin, 2017])

Let $(G, \cdot)$ be a group. The following data are equivalent.

- *An operation $\circ$ such that $(G, \cdot, \circ)$ is a skew brace.*

Gamma functions

Theorem ([Guarnieri and Vendramin, 2017])

Let $(G, \cdot)$ be a group. The following data are equivalent.

- *An operation $\circ$ such that $(G, \cdot, \circ)$ is a skew brace.*
- *A regular subgroup $N \leq \mathrm{Perm}(G)$ which normalises $\lambda(G)$.*

Gamma functions

Theorem ([Guarnieri and Vendramin, 2017])

Let $(G, \cdot)$ be a group. The following data are equivalent.

- *An operation $\circ$ such that $(G, \cdot, \circ)$ is a skew brace.*
- *A regular subgroup $N \leq \mathrm{Perm}(G)$ which normalises $\lambda(G)$.*
- *A function $\gamma \colon G \to \mathrm{Aut}(G, \cdot)$ such that, for every $g, h \in G$,*

$$\gamma(g \cdot {}^{\gamma(g)}h) = \gamma(g)\gamma(h).$$

Gamma functions

Theorem ([Guarnieri and Vendramin, 2017])

Let $(G, \cdot)$ be a group. The following data are equivalent.

- *An operation $\circ$ such that $(G, \cdot, \circ)$ is a skew brace.*
- *A regular subgroup $N \leq \mathrm{Perm}(G)$ which normalises $\lambda(G)$.*
- *A function $\gamma \colon G \to \mathrm{Aut}(G, \cdot)$ such that, for every $g, h \in G$,*

$$\gamma(g \cdot {}^{\gamma(g)}h) = \gamma(g)\gamma(h).$$

The function γ is called *gamma function*.

Gamma functions

Theorem ([Guarnieri and Vendramin, 2017])

Let $(G, \cdot)$ be a group. The following data are equivalent.

- *An operation $\circ$ such that $(G, \cdot, \circ)$ is a skew brace.*
- *A regular subgroup $N \leq \mathrm{Perm}(G)$ which normalises $\lambda(G)$.*
- *A function $\gamma\colon G \to \mathrm{Aut}(G, \cdot)$ such that, for every $g, h \in G$,*

$$\gamma(g \cdot {}^{\gamma(g)}h) = \gamma(g)\gamma(h).$$

The function γ is called *gamma function*. Explicitly,

Gamma functions

Theorem ([Guarnieri and Vendramin, 2017])

Let $(G, \cdot)$ be a group. The following data are equivalent.

- *An operation $\circ$ such that $(G, \cdot, \circ)$ is a skew brace.*
- *A regular subgroup $N \leq \mathrm{Perm}(G)$ which normalises $\lambda(G)$.*
- *A function $\gamma \colon G \to \mathrm{Aut}(G, \cdot)$ such that, for every $g, h \in G$,*

$$\gamma(g \cdot {}^{\gamma(g)}h) = \gamma(g)\gamma(h).$$

The function γ is called *gamma function*. Explicitly,

$${}^{\gamma(g)}h = g^{-1} \cdot (g \circ h),$$

Theorem ([Guarnieri and Vendramin, 2017])

Let $(G, \cdot)$ be a group. The following data are equivalent.

- *An operation $\circ$ such that $(G, \cdot, \circ)$ is a skew brace.*
- *A regular subgroup $N \leq \mathrm{Perm}(G)$ which normalises $\lambda(G)$.*
- *A function $\gamma \colon G \to \mathrm{Aut}(G, \cdot)$ such that, for every $g, h \in G$,*

$$\gamma(g \cdot {}^{\gamma(g)}h) = \gamma(g)\gamma(h).$$

The function γ is called *gamma function*. Explicitly,

$$\begin{aligned} {}^{\gamma(g)}h &= g^{-1} \cdot (g \circ h), \\ N &= \{\lambda(g)\gamma(g) : g \in G\}. \end{aligned}$$

Bi-gamma functions

Theorem ([Childs, 2019], [Caranti, 2020])

Let $(G, \cdot)$ be a group. The following data are equivalent.

Theorem ([Childs, 2019], [Caranti, 2020])

Let $(G, \cdot)$ be a group. The following data are equivalent.

- *An operation $\circ$ such that $(G, \cdot, \circ)$ is a bi-skew brace.*

Theorem ([Childs, 2019], [Caranti, 2020])

Let $(G, \cdot)$ be a group. The following data are equivalent.

- *An operation $\circ$ such that $(G, \cdot, \circ)$ is a bi-skew brace.*
- *A regular subgroup $N \leq \mathrm{Perm}(G)$ which normalises, and is normalised by, $\lambda(G)$.*

Theorem ([Childs, 2019], [Caranti, 2020])

Let $(G, \cdot)$ be a group. The following data are equivalent.

- *An operation $\circ$ such that $(G, \cdot, \circ)$ is a bi-skew brace.*
- *A regular subgroup $N \leq \mathrm{Perm}(G)$ which normalises, and is normalised by, $\lambda(G)$.*
- *An antihomomorphism $\gamma \colon (G, \cdot) \to \mathrm{Aut}(G, \cdot)$ such that, for every $g, h \in G$,*

$$\gamma(g \cdot {}^{\gamma(g)}h) = \gamma(g)\gamma(h).$$

Bi-gamma functions

Theorem ([Childs, 2019], [Caranti, 2020])

Let $(G, \cdot)$ be a group. The following data are equivalent.

- *An operation $\circ$ such that $(G, \cdot, \circ)$ is a bi-skew brace.*
- *A regular subgroup $N \leq \mathrm{Perm}(G)$ which normalises, and is normalised by, $\lambda(G)$.*
- *An antihomomorphism $\gamma \colon (G, \cdot) \to \mathrm{Aut}(G, \cdot)$ such that, for every $g, h \in G$,*

$$\gamma(g \cdot {}^{\gamma(g)}h) = \gamma(g)\gamma(h).$$

The function γ is called *bi-gamma function*.

Our setting: $\varepsilon = -1$

Let $(G, \cdot)$ be a group, and $\psi \in \mathrm{End}(G, \cdot)$.

Our setting: $\varepsilon = -1$

Let $(G, \cdot)$ be a group, and $\psi \in \mathrm{End}(G, \cdot)$.

Theorem ([Caranti and LS, 2021])

The following are equivalent.

Our setting: $\varepsilon = -1$

Let $(G, \cdot)$ be a group, and $\psi \in \mathrm{End}(G, \cdot)$.

Theorem ([Caranti and LS, 2021])

The following are equivalent.

- ψ *satisfies* ${}^{\psi}[[G, \psi], G] \leq Z(G, \cdot)$.

Our setting: $\varepsilon = -1$

Let $(G, \cdot)$ be a group, and $\psi \in \mathrm{End}(G, \cdot)$.

Theorem ([Caranti and LS, 2021])

The following are equivalent.

- ψ *satisfies* ${}^{\psi}[[G, \psi], G] \leq Z(G, \cdot)$.
- $(G, \cdot, \circ)$ *is a bi-skew brace, for* $g \circ h = g \cdot {}^{\psi}g^{-1} \cdot h \cdot {}^{\psi}g$.

Our setting: $\varepsilon = -1$

Let $(G, \cdot)$ be a group, and $\psi \in \mathrm{End}(G, \cdot)$.

Theorem ([Caranti and LS, 2021])

The following are equivalent.

- ψ *satisfies* ${}^{\psi}[[G, \psi], G] \leq Z(G, \cdot)$.
- $(G, \cdot, \circ)$ *is a bi-skew brace, for* $g \circ h = g \cdot {}^{\psi}g^{-1} \cdot h \cdot {}^{\psi}g$.
- *The function* γ *define by* $\gamma(g) = \iota({}^{\psi}g^{-1})$ *is a bi-gamma function for* $(G, \cdot)$.

Our setting: $\varepsilon = -1$

Let $(G, \cdot)$ be a group, and $\psi \in \mathrm{End}(G, \cdot)$.

Theorem ([Caranti and LS, 2021])

The following are equivalent.

- *ψ satisfies ${}^{\psi}[[G, \psi], G] \leq Z(G, \cdot)$.*
- *$(G, \cdot, \circ)$ is a bi-skew brace, for $g \circ h = g \cdot {}^{\psi}g^{-1} \cdot h \cdot {}^{\psi}g$.*
- *The function γ define by $\gamma(g) = \iota({}^{\psi}g^{-1})$ is a bi-gamma function for $(G, \cdot)$.*

If any of these holds, then $N = \{\lambda(g)\iota({}^{\psi}g^{-1}) : g \in G\}$ is a regular subgroup of $\mathrm{Perm}(G)$ which normalises, and is normalised by, $\lambda(G)$.

Our setting: $\varepsilon = -1$

Let $(G, \cdot)$ be a group, and $\psi \in \operatorname{End}(G, \cdot)$.

Theorem ([Caranti and LS, 2021])

The following are equivalent.

- ψ *satisfies* ${}^{\psi}[[G, \psi], G] \leq Z(G, \cdot)$.
- $(G, \cdot, \circ)$ *is a bi-skew brace, for* $g \circ h = g \cdot {}^{\psi}g^{-1} \cdot h \cdot {}^{\psi}g$.
- *The function* γ *define by* $\gamma(g) = \iota({}^{\psi}g^{-1})$ *is a bi-gamma function for* $(G, \cdot)$.

If any of these holds, then $N = \{\lambda(g)\iota({}^{\psi}g^{-1}) : g \in G\}$ is a regular subgroup of $\operatorname{Perm}(G)$ which normalises, and is normalised by, $\lambda(G)$.

This result generalises [Koch, 2020], where the map ψ is abelian.

The Yang-Baxter equation

Definition ([Drinfel'd, 1992])

A *set-theoretic solution* of the Yang-Baxter equation is a couple (X, r), where $X \neq \emptyset$ is a set, and

Main definitions

Definition ([Drinfel'd, 1992])

A *set-theoretic solution* of the Yang-Baxter equation is a couple (X, r), where $X \neq \emptyset$ is a set, and

$$\begin{aligned} r\colon X \times X &\to X \times X \\ (x, y) &\mapsto (\sigma_x(y), \tau_y(x)) \end{aligned}$$

is a bijective map satisfying

Definition ([Drinfel'd, 1992])

A *set-theoretic solution* of the Yang-Baxter equation is a couple (X, r), where $X \neq \emptyset$ is a set, and

$$\begin{aligned} r\colon X \times X &\to X \times X \\ (x, y) &\mapsto (\sigma_x(y), \tau_y(x)) \end{aligned}$$

is a bijective map satisfying

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

Main definitions

Definition ([Drinfel'd, 1992])

A *set-theoretic solution* of the Yang-Baxter equation is a couple (X, r), where $X \neq \emptyset$ is a set, and

$$\begin{aligned} r\colon X \times X &\to X \times X \\ (x, y) &\mapsto (\sigma_x(y), \tau_y(x)) \end{aligned}$$

is a bijective map satisfying

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

We say that (X, r) is *non-degenerate* if, for every $x \in X$, σ_x and τ_x are bijective,

Main definitions

Definition ([Drinfel'd, 1992])

A *set-theoretic solution* of the Yang-Baxter equation is a couple (X, r), where $X \neq \emptyset$ is a set, and

$$\begin{aligned} r \colon X \times X &\to X \times X \\ (x, y) &\mapsto (\sigma_x(y), \tau_y(x)) \end{aligned}$$

is a bijective map satisfying

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

We say that (X, r) is *non-degenerate* if, for every $x \in X$, σ_x and τ_x are bijective, and *involutive* if $r^2 = \mathrm{id}_{X \times X}$.

Main definitions

Definition ([Drinfel'd, 1992])

A *set-theoretic solution* of the Yang-Baxter equation is a couple (X, r), where $X \neq \emptyset$ is a set, and

$$\begin{aligned} r\colon X \times X &\to X \times X \\ (x, y) &\mapsto (\sigma_x(y), \tau_y(x)) \end{aligned}$$

is a bijective map satisfying

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

We say that (X, r) is *non-degenerate* if, for every $x \in X$, σ_x and τ_x are bijective, and *involutive* if $r^2 = \mathrm{id}_{X \times X}$. For us, a *solution* is a non-degenerate set-theoretic solution of the Yang-Baxter equation.

Theorem ([Rump, 2007], [Guarnieri and Vendramin, 2017])

Let $(G, \cdot, \circ)$ be a skew brace.

Theorem ([Rump, 2007], [Guarnieri and Vendramin, 2017])

Let $(G, \cdot, \circ)$ be a skew brace. Then

$$r\colon (g, h) \mapsto (g^{-1} \cdot (g \circ h), \overline{g^{-1} \cdot (g \circ h)} \circ g \circ h)$$

is a solution for G.

Theorem ([Rump, 2007], [Guarnieri and Vendramin, 2017])

Let $(G, \cdot, \circ)$ be a skew brace. Then

$$r\colon (g, h) \mapsto (g^{-1} \cdot (g \circ h), \overline{g^{-1} \cdot (g \circ h)} \circ g \circ h)$$

is a solution for G.

The solution (G, r) is involutive if and only if $(G, \cdot, \circ)$ is a brace, that is, if $(G, \cdot)$ is abelian.

Definition ([Rump, 2019], [Koch and Truman, 2020a])

Let $(G, \cdot, \circ)$ be a skew brace. The *opposite skew brace* is $(G, \cdot', \circ)$, where, for every $g, h \in G$, $g \cdot' h = h \cdot g$.

Opposite skew brace, bi-skew braces and solutions

Definition ([Rump, 2019], [Koch and Truman, 2020a])

Let $(G, \cdot, \circ)$ be a skew brace. The *opposite skew brace* is $(G, \cdot', \circ)$, where, for every $g, h \in G$, $g \cdot' h = h \cdot g$.

Given a bi-skew brace $(G, \cdot, \circ)$, we find (up to) four solutions for G:

Opposite skew brace, bi-skew braces and solutions

Definition ([Rump, 2019], [Koch and Truman, 2020a])

Let $(G, \cdot, \circ)$ be a skew brace. The *opposite skew brace* is $(G, \cdot', \circ)$, where, for every $g, h \in G$, $g \cdot' h = h \cdot g$.

Given a bi-skew brace $(G, \cdot, \circ)$, we find (up to) four solutions for G:

$$(G, \cdot, \circ) \rightsquigarrow (g, h) \mapsto (g^{-1} \cdot (g \circ h), \overline{g^{-1} \cdot (g \circ h)} \circ g \circ h),$$

Definition ([Rump, 2019], [Koch and Truman, 2020a])

Let $(G, \cdot, \circ)$ be a skew brace. The *opposite skew brace* is $(G, \cdot', \circ)$, where, for every $g, h \in G$, $g \cdot' h = h \cdot g$.

Given a bi-skew brace $(G, \cdot, \circ)$, we find (up to) four solutions for G:

$$(G, \cdot, \circ) \rightsquigarrow (g, h) \mapsto (g^{-1} \cdot (g \circ h), \overline{g^{-1} \cdot (g \circ h)} \circ g \circ h),$$
$$(G, \cdot', \circ) \rightsquigarrow (g, h) \mapsto ((g \circ h) \cdot g^{-1}, \overline{(g \circ h) \cdot g^{-1}} \circ g \circ h),$$

Definition ([Rump, 2019], [Koch and Truman, 2020a])

Let $(G, \cdot, \circ)$ be a skew brace. The *opposite skew brace* is $(G, \cdot', \circ)$, where, for every $g, h \in G$, $g \cdot' h = h \cdot g$.

Given a bi-skew brace $(G, \cdot, \circ)$, we find (up to) four solutions for G:

$$
\begin{aligned}
(G, \cdot, \circ) &\rightsquigarrow (g, h) \mapsto (g^{-1} \cdot (g \circ h), \overline{g^{-1} \cdot (g \circ h)} \circ g \circ h),\\
(G, \cdot', \circ) &\rightsquigarrow (g, h) \mapsto ((g \circ h) \cdot g^{-1}, \overline{(g \circ h) \cdot g^{-1}} \circ g \circ h),\\
(G, \circ, \cdot) &\rightsquigarrow (g, h) \mapsto (\overline{g} \circ (g \cdot h), (\overline{g} \circ (g \cdot h))^{-1} \cdot g \cdot h),
\end{aligned}
$$

Opposite skew brace, bi-skew braces and solutions

Definition ([Rump, 2019], [Koch and Truman, 2020a])

Let $(G, \cdot, \circ)$ be a skew brace. The *opposite skew brace* is $(G, \cdot', \circ)$, where, for every $g, h \in G$, $g \cdot' h = h \cdot g$.

Given a bi-skew brace $(G, \cdot, \circ)$, we find (up to) four solutions for G:

$$\begin{aligned}
(G, \cdot, \circ) &\rightsquigarrow (g, h) \mapsto (g^{-1} \cdot (g \circ h), \overline{g^{-1} \cdot (g \circ h)} \circ g \circ h), \\
(G, \cdot', \circ) &\rightsquigarrow (g, h) \mapsto ((g \circ h) \cdot g^{-1}, \overline{(g \circ h) \cdot g^{-1}} \circ g \circ h), \\
(G, \circ, \cdot) &\rightsquigarrow (g, h) \mapsto (\overline{g} \circ (g \cdot h), (\overline{g} \circ (g \cdot h))^{-1} \cdot g \cdot h), \\
(G, \circ', \cdot) &\rightsquigarrow (g, h) \mapsto ((g \cdot h) \circ \overline{g}, ((g \cdot h) \circ \overline{g})^{-1} \cdot g \cdot h).
\end{aligned}$$

Yang-Baxter and (bi)-gamma functions

We may rewrite the solutions so that they depend only on $\cdot$ and γ.

Yang-Baxter and (bi)-gamma functions

We may rewrite the solutions so that they depend only on $\cdot$ and γ.

Theorem ([Caranti and LS, 2021])

Let $(G, \cdot)$ be a group, and γ be a gamma function.

Yang-Baxter and (bi)-gamma functions

We may rewrite the solutions so that they depend only on $\cdot$ and γ.

Theorem ([Caranti and LS, 2021])

Let $(G, \cdot)$ be a group, and γ be a gamma function.
The we get (up to) two solutions:

Yang-Baxter and (bi)-gamma functions

We may rewrite the solutions so that they depend only on $\cdot$ and γ.

Theorem ([Caranti and LS, 2021])

Let $(G, \cdot)$ be a group, and γ be a gamma function.
The we get (up to) two solutions:

$$(g, h) \mapsto ({}^{\gamma(g)}h, {}^{\gamma({}^{\gamma(g)}h)^{-1}}({}^{\gamma(g)}h^{-1} \cdot g \cdot {}^{\gamma(g)}h)),$$

Yang-Baxter and (bi)-gamma functions

We may rewrite the solutions so that they depend only on $\cdot$ and γ.

Theorem ([Caranti and LS, 2021])

Let $(G, \cdot)$ be a group, and γ be a gamma function.
The we get (up to) two solutions:

$$(g, h) \mapsto ({}^{\gamma(g)}h, {}^{\gamma({}^{\gamma(g)}h)^{-1}}({}^{\gamma(g)}h^{-1} \cdot g \cdot {}^{\gamma(g)}h)),$$

$$(g, h) \mapsto ({}^{\iota(g)\gamma(g)}h, {}^{\gamma({}^{\iota(g)\gamma(g)}h)^{-1}}g).$$

Yang-Baxter and (bi)-gamma functions

We may rewrite the solutions so that they depend only on $\cdot$ and γ.

Theorem ([Caranti and LS, 2021])

Let $(G, \cdot)$ be a group, and γ be a gamma function.
The we get (up to) two solutions:

$$(g, h) \mapsto ({}^{\gamma(g)}h, {}^{\gamma({}^{\gamma(g)}h)^{-1}}({}^{\gamma(g)}h^{-1} \cdot g \cdot {}^{\gamma(g)}h)),$$
$$(g, h) \mapsto ({}^{\iota(g)\gamma(g)}h, {}^{\gamma({}^{\iota(g)\gamma(g)}h)^{-1}}g).$$

If in addition γ is a bi-gamma function, then we get (up to) other two solutions:

We may rewrite the solutions so that they depend only on $\cdot$ and γ.

Theorem ([Caranti and LS, 2021])

Let $(G, \cdot)$ be a group, and γ be a gamma function.
The we get (up to) two solutions:

$$(g, h) \mapsto ({}^{\gamma(g)}h, {}^{\gamma({}^{\gamma(g)}h)^{-1}}({}^{\gamma(g)}h^{-1} \cdot g \cdot {}^{\gamma(g)}h)),$$
$$(g, h) \mapsto ({}^{\iota(g)\gamma(g)}h, {}^{\gamma({}^{\iota(g)\gamma(g)}h)^{-1}}g).$$

If in addition γ is a bi-gamma function, then we get (up to) other two solutions:

$$(g, h) \mapsto ({}^{\gamma(g^{-1})}h, {}^{\gamma(g^{-1})}h^{-1} \cdot g \cdot h),$$

We may rewrite the solutions so that they depend only on $\cdot$ and γ.

Theorem ([Caranti and LS, 2021])

Let $(G, \cdot)$ be a group, and γ be a gamma function.
The we get (up to) two solutions:

$$(g, h) \mapsto ({}^{\gamma(g)}h, {}^{\gamma({}^{\gamma(g)}h)^{-1}}({}^{\gamma(g)}h^{-1} \cdot g \cdot {}^{\gamma(g)}h)),$$
$$(g, h) \mapsto ({}^{\iota(g)\gamma(g)}h, {}^{\gamma({}^{\iota(g)\gamma(g)}h)^{-1}}g).$$

If in addition γ is a bi-gamma function, then we get (up to) other two solutions:

$$(g, h) \mapsto ({}^{\gamma(g^{-1})}h, {}^{\gamma(g^{-1})}h^{-1} \cdot g \cdot h),$$
$$(g, h) \mapsto (g \cdot h \cdot {}^{\gamma(h)}g^{-1}, {}^{\gamma(h)}g^{-1}).$$

Yang-Baxter in our setting

Theorem ([Caranti and LS, 2021])

Let $(G, \cdot)$ *be a group, and* $\psi \in \mathrm{End}(G, \cdot)$.

Yang-Baxter in our setting

Theorem ([Caranti and LS, 2021])

Let $(G, \cdot)$ *be a group, and* $\psi \in \mathrm{End}(G, \cdot)$*. If* ${}^{\psi}[[G, \psi], G] \le Z(G, \cdot)$*, then we get (up to) four solutions:*

Yang-Baxter in our setting

Theorem ([Caranti and LS, 2021])

Let $(G, \cdot)$ *be a group, and* $\psi \in \mathrm{End}(G, \cdot)$*. If* ${}^{\psi}[[G, \psi], G] \leq Z(G, \cdot)$*, then we get (up to) four solutions:*

$$(g, h) \mapsto ({}^{\psi}g^{-1} \cdot h \cdot {}^{\psi}g, {}^{\psi}(g^{-1} \cdot h) \cdot h^{-1} \cdot {}^{\psi}g \cdot g \cdot {}^{\psi}g^{-1} \cdot h \cdot {}^{\psi}(h^{-1} \cdot g)),$$

Yang-Baxter in our setting

Theorem ([Caranti and LS, 2021])

Let $(G, \cdot)$ *be a group, and* $\psi \in \mathrm{End}(G, \cdot)$*. If* ${}^{\psi}[[G, \psi], G] \leq Z(G, \cdot)$*, then we get (up to) four solutions:*

$$(g, h) \mapsto ({}^{\psi}g^{-1} \cdot h \cdot {}^{\psi}g, {}^{\psi}(g^{-1} \cdot h) \cdot h^{-1} \cdot {}^{\psi}g \cdot g \cdot {}^{\psi}g^{-1} \cdot h \cdot {}^{\psi}(h^{-1} \cdot g)),$$

$$(g, h) \mapsto (g \cdot {}^{\psi}g^{-1} \cdot h \cdot {}^{\psi}g \cdot g^{-1}, {}^{\psi}h \cdot g \cdot {}^{\psi}h^{-1}),$$

Yang-Baxter in our setting

Theorem ([Caranti and LS, 2021])

Let $(G, \cdot)$ *be a group, and* $\psi \in \mathrm{End}(G, \cdot)$. *If* ${}^{\psi}[[G, \psi], G] \leq Z(G, \cdot)$, *then we get (up to) four solutions:*

$$(g, h) \mapsto ({}^{\psi}g^{-1} \cdot h \cdot {}^{\psi}g, {}^{\psi}(g^{-1} \cdot h) \cdot h^{-1} \cdot {}^{\psi}g \cdot g \cdot {}^{\psi}g^{-1} \cdot h \cdot {}^{\psi}(h^{-1} \cdot g)),$$
$$(g, h) \mapsto (g \cdot {}^{\psi}g^{-1} \cdot h \cdot {}^{\psi}g \cdot g^{-1}, {}^{\psi}h \cdot g \cdot {}^{\psi}h^{-1}),$$
$$(g, h) \mapsto ({}^{\psi}g \cdot h \cdot {}^{\psi}g^{-1}, {}^{\psi}g \cdot h^{-1} \cdot {}^{\psi}g^{-1} \cdot g \cdot h),$$

Yang-Baxter in our setting

Theorem ([Caranti and LS, 2021])

Let $(G, \cdot)$ be a group, and $\psi \in \mathrm{End}(G, \cdot)$. If ${}^{\psi}[[G, \psi], G] \leq Z(G, \cdot)$, then we get (up to) four solutions:

$$(g, h) \mapsto ({}^{\psi}g^{-1} \cdot h \cdot {}^{\psi}g, {}^{\psi}(g^{-1} \cdot h) \cdot h^{-1} \cdot {}^{\psi}g \cdot g \cdot {}^{\psi}g^{-1} \cdot h \cdot {}^{\psi}(h^{-1} \cdot g)),$$
$$(g, h) \mapsto (g \cdot {}^{\psi}g^{-1} \cdot h \cdot {}^{\psi}g \cdot g^{-1}, {}^{\psi}h \cdot g \cdot {}^{\psi}h^{-1}),$$
$$(g, h) \mapsto ({}^{\psi}g \cdot h \cdot {}^{\psi}g^{-1}, {}^{\psi}g \cdot h^{-1} \cdot {}^{\psi}g^{-1} \cdot g \cdot h),$$
$$(g, h) \mapsto (g \cdot h \cdot {}^{\psi}h^{-1} \cdot g^{-1} \cdot {}^{\psi}h, {}^{\psi}h^{-1} \cdot g \cdot {}^{\psi}h).$$

Yang-Baxter in our setting

Theorem ([Caranti and LS, 2021])

Let $(G, \cdot)$ *be a group, and* $\psi \in \mathrm{End}(G, \cdot)$*. If* ${}^{\psi}[[G, \psi], G] \leq Z(G, \cdot)$*, then we get (up to) four solutions:*

$$(g, h) \mapsto ({}^{\psi}g^{-1} \cdot h \cdot {}^{\psi}g, {}^{\psi}(g^{-1} \cdot h) \cdot h^{-1} \cdot {}^{\psi}g \cdot g \cdot {}^{\psi}g^{-1} \cdot h \cdot {}^{\psi}(h^{-1} \cdot g)),$$
$$(g, h) \mapsto (g \cdot {}^{\psi}g^{-1} \cdot h \cdot {}^{\psi}g \cdot g^{-1}, {}^{\psi}h \cdot g \cdot {}^{\psi}h^{-1}),$$
$$(g, h) \mapsto ({}^{\psi}g \cdot h \cdot {}^{\psi}g^{-1}, {}^{\psi}g \cdot h^{-1} \cdot {}^{\psi}g^{-1} \cdot g \cdot h),$$
$$(g, h) \mapsto (g \cdot h \cdot {}^{\psi}h^{-1} \cdot g^{-1} \cdot {}^{\psi}h, {}^{\psi}h^{-1} \cdot g \cdot {}^{\psi}h).$$

These coincide with the solutions found in [Koch, 2020], where ψ is abelian.

Hopf Galois structures

Main definition and results

Fix a finite Galois extension L/K with Galois group $(G, \cdot)$.

Main definition and results

Fix a finite Galois extension L/K with Galois group $(G, \cdot)$.

Definition

A Hopf Galois structure on L/K consists of a cocommutative K-Hopf algebra H, together with an action of H on L satisfying certain technical properties.

Main definition and results

Fix a finite Galois extension L/K with Galois group $(G, \cdot)$.

Definition

A Hopf Galois structure on L/K consists of a cocommutative K-Hopf algebra H, together with an action of H on L satisfying certain technical properties.

Theorem ([Greither and Pareigis, 1987])

The Hopf Galois structures on L/K are in bijective correspondence with the regular subgroups of $\mathrm{Perm}(G)$ *normalised by* $\lambda(G)$.

Fix a finite Galois extension L/K with Galois group $(G, \cdot)$.

Definition

A Hopf Galois structure on L/K consists of a cocommutative K-Hopf algebra H, together with an action of H on L satisfying certain technical properties.

Theorem ([Greither and Pareigis, 1987])

The Hopf Galois structures on L/K are in bijective correspondence with the regular subgroups of $\mathrm{Perm}(G)$ *normalised by* $\lambda(G)$.

The K-Hopf algebra $L[N]^G$ corresponds to the subgroup N.

Main definition and results

Fix a finite Galois extension L/K with Galois group $(G, \cdot)$.

Definition

A Hopf Galois structure on L/K consists of a cocommutative K-Hopf algebra H, together with an action of H on L satisfying certain technical properties.

Theorem ([Greither and Pareigis, 1987])

The Hopf Galois structures on L/K are in bijective correspondence with the regular subgroups of $\mathrm{Perm}(G)$ *normalised by* $\lambda(G)$.

The K-Hopf algebra $L[N]^G$ corresponds to the subgroup N.

Moreover, the K-sub-Hopf algebras of $L[N]^G$ are in bijective correspondence with the subgroups of N normalised by $\lambda(G)$.

Hopf Galois and gamma functions

We would like to use gamma functions to analyse Hopf Galois structures.

Hopf Galois and gamma functions

We would like to use gamma functions to analyse Hopf Galois structures. Notice that a gamma function for $(G, \cdot)$ yields a regular subgroup which normalises $\lambda(G)$,

Hopf Galois and gamma functions

We would like to use gamma functions to analyse Hopf Galois structures. Notice that a gamma function for $(G, \cdot)$ yields a regular subgroup which normalises $\lambda(G)$, while we need a regular subgroup normalised by $\lambda(G)$.

We would like to use gamma functions to analyse Hopf Galois structures. Notice that a gamma function for $(G, \cdot)$ yields a regular subgroup which normalises $\lambda(G)$, while we need a regular subgroup normalised by $\lambda(G)$.

Fact

If γ is a bi-gamma function for $(G, \cdot)$, then

Hopf Galois and gamma functions

We would like to use gamma functions to analyse Hopf Galois structures. Notice that a gamma function for $(G, \cdot)$ yields a regular subgroup which normalises $\lambda(G)$, while we need a regular subgroup normalised by $\lambda(G)$.

Fact

If γ is a bi-gamma function for $(G, \cdot)$, then

$$N = \{\lambda(g)\gamma(g) : g \in G\}$$

Hopf Galois and gamma functions

We would like to use gamma functions to analyse Hopf Galois structures. Notice that a gamma function for $(G, \cdot)$ yields a regular subgroup which normalises $\lambda(G)$, while we need a regular subgroup normalised by $\lambda(G)$.

Fact

If γ is a bi-gamma function for $(G, \cdot)$, then

$$N = \{\lambda(g)\gamma(g) : g \in G\}$$

is a regular subgroup of $\mathrm{Perm}(G)$ *which normalises, and is normalised by,* $\lambda(G)$.

Hopf Galois and gamma functions

We would like to use gamma functions to analyse Hopf Galois structures. Notice that a gamma function for $(G, \cdot)$ yields a regular subgroup which normalises $\lambda(G)$, while we need a regular subgroup normalised by $\lambda(G)$.

Fact

If γ is a bi-gamma function for $(G, \cdot)$, then

$$N = \{\lambda(g)\gamma(g) : g \in G\}$$

is a regular subgroup of $\mathrm{Perm}(G)$ *which normalises, and is normalised by, $\lambda(G)$. In particular, $L[N]^G$ gives a Hopf Galois structure on L/K.*

Hopf Galois structures in our setting

Let L/K be a finite Galois extension with Galois group $(G, \cdot)$, Let L/K be a finite Galois extension with Galois group $(G, \cdot)$, and $\psi \in \mathrm{End}(G, \cdot)$ such that ${}^{\psi}[[G, \psi], G] \leq Z(G, \cdot)$.

Let L/K be a finite Galois extension with Galois group $(G, \cdot)$, and $\psi \in \mathrm{End}(G, \cdot)$ such that ${}^{\psi}[[G, \psi], G] \leq Z(G, \cdot)$.
Then γ, defined by $\gamma(g) = \iota({}^{\psi}g^{-1})$, is a bi-gamma function,

Hopf Galois structures in our setting

Let L/K be a finite Galois extension with Galois group $(G, \cdot)$, and $\psi \in \mathrm{End}(G, \cdot)$ such that ${}^{\psi}[[G, \psi], G] \leq Z(G, \cdot)$.
Then γ, defined by $\gamma(g) = \iota({}^{\psi}g^{-1})$, is a bi-gamma function, and so $L[N]^G$ gives a Hopf Galois structure on L/K, where

$$N = \{\lambda(g)\iota({}^{\psi}g^{-1}) : g \in G\}.$$

Hopf Galois structures in our setting

Let L/K be a finite Galois extension with Galois group $(G, \cdot)$, and $\psi \in \mathrm{End}(G, \cdot)$ such that ${}^{\psi}[[G, \psi], G] \leq Z(G, \cdot)$.
Then γ, defined by $\gamma(g) = \iota({}^{\psi}g^{-1})$, is a bi-gamma function, and so $L[N]^G$ gives a Hopf Galois structure on L/K, where

$$N = \{\lambda(g)\iota({}^{\psi}g^{-1}) : g \in G\}.$$

Question

Can we determine the type of N?

Five subgroups of N

As in [Koch, 2020], we can always find (up to) five subgroups of N normalised by $\lambda(G)$, and these correspond to five K-sub-Hopf algebras of $L[N]^G$.

Five subgroups of N

As in [Koch, 2020], we can always find (up to) five subgroups of N normalised by $\lambda(G)$, and these correspond to five K-sub-Hopf algebras of $L[N]^G$.

For example, the λ-points and ρ-points, introduced in [Koch and Truman, 2020b]:

Five subgroups of N

As in [Koch, 2020], we can always find (up to) five subgroups of N normalised by $\lambda(G)$, and these correspond to five K-sub-Hopf algebras of $L[N]^G$.

For example, the λ-points and ρ-points, introduced in [Koch and Truman, 2020b]:

$$\Lambda_N = N \cap \lambda(G)$$

Five subgroups of N

As in [Koch, 2020], we can always find (up to) five subgroups of N normalised by $\lambda(G)$, and these correspond to five K-sub-Hopf algebras of $L[N]^G$.

For example, the λ-points and ρ-points, introduced in [Koch and Truman, 2020b]:

$$\Lambda_N = N \cap \lambda(G) = \{\lambda(g) : g \in \ker(\gamma)\}$$

Five subgroups of N

As in [Koch, 2020], we can always find (up to) five subgroups of N normalised by $\lambda(G)$, and these correspond to five K-sub-Hopf algebras of $L[N]^G$.

For example, the λ-points and ρ-points, introduced in [Koch and Truman, 2020b]:

$$\begin{aligned}\Lambda_N = N \cap \lambda(G) &= \{\lambda(g) : g \in \ker(\gamma)\} \\ &= \{\lambda(g) : g \text{ satisfies } {}^{\psi}g \in Z(G,\cdot)\},\end{aligned}$$

Five subgroups of N

As in [Koch, 2020], we can always find (up to) five subgroups of N normalised by $\lambda(G)$, and these correspond to five K-sub-Hopf algebras of $L[N]^G$.

For example, the λ-points and ρ-points, introduced in [Koch and Truman, 2020b]:

$$\begin{aligned} \Lambda_N &= N \cap \lambda(G) = \{\lambda(g) : g \in \ker(\gamma)\} \\ &= \{\lambda(g) : g \text{ satisfies } {}^{\psi}g \in Z(G, \cdot)\}, \\ P_N &= N \cap \rho(G) \end{aligned}$$

Five subgroups of N

As in [Koch, 2020], we can always find (up to) five subgroups of N normalised by $\lambda(G)$, and these correspond to five K-sub-Hopf algebras of $L[N]^G$.

For example, the λ-points and ρ-points, introduced in [Koch and Truman, 2020b]:

$$\begin{aligned} \Lambda_N &= N \cap \lambda(G) = \{\lambda(g) : g \in \ker(\gamma)\} \\ &= \{\lambda(g) : g \text{ satisfies } {}^{\psi}g \in Z(G, \cdot)\}, \\ P_N &= N \cap \rho(G) = \{\rho(g) : g \text{ satisfies } \gamma(g) = \iota(g^{-1})\} \end{aligned}$$

Five subgroups of N

As in [Koch, 2020], we can always find (up to) five subgroups of N normalised by $\lambda(G)$, and these correspond to five K-sub-Hopf algebras of $L[N]^G$.

For example, the λ-points and ρ-points, introduced in [Koch and Truman, 2020b]:

$$\begin{aligned}
\Lambda_N &= N \cap \lambda(G) = \{\lambda(g) : g \in \ker(\gamma)\} \\
&= \{\lambda(g) : g \text{ satisfies } {}^{\psi}g \in Z(G, \cdot)\}, \\
P_N &= N \cap \rho(G) = \{\rho(g) : g \text{ satisfies } \gamma(g) = \iota(g^{-1})\} \\
&= \{\rho(g) : g \text{ satisfies } g \cdot {}^{\psi}g^{-1} \in Z(G, \cdot)\}.
\end{aligned}$$

Five subgroups of N

As in [Koch, 2020], we can always find (up to) five subgroups of N normalised by $\lambda(G)$, and these correspond to five K-sub-Hopf algebras of $L[N]^G$.

For example, the λ-points and ρ-points, introduced in [Koch and Truman, 2020b]:

$$\begin{aligned}\Lambda_N &= N \cap \lambda(G) = \{\lambda(g) : g \in \ker(\gamma)\} \\ &= \{\lambda(g) : g \text{ satisfies } {}^{\psi}g \in Z(G,\cdot)\}, \\ P_N &= N \cap \rho(G) = \{\rho(g) : g \text{ satisfies } \gamma(g) = \iota(g^{-1})\} \\ &= \{\rho(g) : g \text{ satisfies } g \cdot {}^{\psi}g^{-1} \in Z(G,\cdot)\}.\end{aligned}$$

Some of the five subgroups may coincide, but we can find examples in which they are all distinct.

When we can be explicit

- If ψ is a fixed point free abelian endomorphism, then $N \cong (G, \cdot)$ ([Childs, 2013], [Koch, 2020]).

When we can be explicit

- If ψ is a fixed point free abelian endomorphism, then $N \cong (G, \cdot)$ ([Childs, 2013], [Koch, 2020]).
- If ψ is different from zero and idempotent, then for every $n \geq 1$, $\psi^n = \psi$,

When we can be explicit

- If ψ is a fixed point free abelian endomorphism, then $N \cong (G, \cdot)$ ([Childs, 2013], [Koch, 2020]).
- If ψ is different from zero and idempotent, then for every $n \geq 1$, $\psi^n = \psi$, and ${}^{\psi}G = \{g \in G : {}^{\psi}g = g\}$.

When we can be explicit

- If ψ is a fixed point free abelian endomorphism, then $N \cong (G, \cdot)$ ([Childs, 2013], [Koch, 2020]).
- If ψ is different from zero and idempotent, then for every $n \geq 1$, $\psi^n = \psi$, and ${}^{\psi}G = \{g \in G : {}^{\psi}g = g\}$. We can use a version of the Fitting's Lemma for groups ([Caranti, 1985]) to deduce that $N \cong (\ker(\psi), \cdot) \times ({}^{\psi}G, \cdot)$.

Bibliography I

Caranti, A. (1985).
Finite p-groups of exponent p^2 in which each element commutes with its endomorphic images.
J. Algebra, 97(1):1–13.

Caranti, A. (2020).
Bi-skew braces and regular subgroups of the holomorph.
J. Algebra, 562:647–665.

Caranti, A. and LS (2021).
From endomorphisms to bi-skew braces, regular subgroups, normalising graphs, the Yang-Baxter equation, and Hopf Galois structures.
https://arxiv.org/abs/2104.01582.

Bibliography II

Childs, L. N. (2013).
Fixed-point free endomorphisms and Hopf Galois structures.
Proc. Amer. Math. Soc., 141(4):1255–1265.

Childs, L. N. (2019).
Bi-skew braces and Hopf Galois structures.
New York J. Math., 25:574–588.

Drinfel'd, V. G. (1992).
On some unsolved problems in quantum group theory.
In *Quantum groups (Leningrad, 1990)*, volume 1510 of *Lecture Notes in Math.*, pages 1–8. Springer, Berlin.

Greither, C. and Pareigis, B. (1987).
Hopf Galois theory for separable field extensions.
J. Algebra, 106(1):239–258.

Bibliography III

Guarnieri, L. and Vendramin, L. (2017).
Skew braces and the Yang-Baxter equation.
Math. Comp., 86(307):2519–2534.

Koch, A. (2020).
Abelian maps, bi-skew braces, and opposite pairs of Hopf-Galois structures.
https://arxiv.org/abs/2007.08967.

Koch, A. and Truman, P. J. (2020a).
Opposite skew left braces and applications.
J. Algebra, 546:218–235.

Koch, A. and Truman, P. J. (2020b).
Skew left braces and isomorphism problems for Hopf-Galois structures on Galois extensions.
https://arxiv.org/abs/2005.05809.

Bibliography IV

Rump, W. (2007).
Braces, radical rings, and the quantum Yang-Baxter equation.
J. Algebra, 307(1):153–170.

Rump, W. (2019).
A covering theory for non-involutive set-theoretic solutions to the Yang-Baxter equation.
J. Algebra, 520:136–170.