Skew bracoids and Hopf-Galois structures

Paul Truman

Keele University, UK

Hopf algebras and Galois module theory

30th May, 2023

Overview

- Joint work with Isabel Martin-Lyons

Aim

Last year we explored generalizing the definition of skew braces to give objects corresponding to Hopf-Galois structures on separable, but non-normal, extensions. This talk surveys developments in this theory.

- A route for constructing a skew brace from a Hopf-Galois structure on a Galois extension.
- Generalizing to skew bracoids
- Characterizations and γ-functions
- Ideals and quotients
- Hopf-Galois structures and the Hopf-Galois correspondence

The names they are a-changing

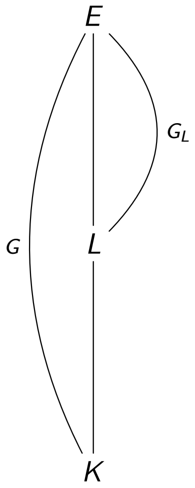
- ~~Weak skew braces~~
- ~~Near skew braces~~
- ~~Neo-skew braces~~
- Skew bracoids

What else is new?

- Better tools for relating / comparing skew bracoids.
- Development of substructures / ideals / quotients.
- Improved formulations of homomorphisms / isomorphisms: up as far as First Isomorphism Theorem. (Not this talk)
- Tighter correspondence between skew bracoids and HGS on separable extensions: after Stefanello-Trappeniers.

Greither-Pareigis theory for non-normal extensions

- Let L/K be a separable extension of fields with Galois closure E.
- Write $G = \mathrm{Gal}(E/K)$ and $G_L = \mathrm{Gal}(E/L)$.
- Let $X = G/G_L$ and define $\lambda : G \to \mathrm{Perm}(X)$ by $\lambda(g)[\overline{h}] = \overline{gh}$.
- Then G acts on $\mathrm{Perm}(X)$ by conjugation via λ.
- There is a bijection between G-stable regular subgroups of $\mathrm{Perm}(X)$ and Hopf-Galois structures on L/K.



The S-T route from a HGS to a skew brace

- Let L/K be a Galois extension with Galois group $G = (G, \cdot)$.
- Suppose that N is a regular G-stable subgroup of $\mathrm{Perm}(G)$.
- The map $N \to G$ defined by $\eta \mapsto \eta^{-1}[e_G]$ is a bijection.
- Transport the structure of N^{opp} to G via

$$\eta^{-1}[e_G] \star \mu^{-1}[e_G] = (\eta\mu)^{-1}[e_G].$$

- Then $(G, \star)$ is a group isomorphic to N and

$$g \cdot (h_1 \star h_2) = (g \cdot h_1) \star g^{-1} \star (g \cdot h_2),$$

so $(G, \star, \cdot)$ is a skew brace.

Mimicking the route in the non-normal case

- Now let L/K be separable, but non-normal, with Galois closure E.
- Suppose that N is a regular G-stable subgroup of $\mathrm{Perm}(X)$.
- The map $N \to X$ defined by $\eta \mapsto \eta^{-1}[\overline{e_G}]$ is a bijection.
- Transport the structure of N^{opp} to X via

$$\eta^{-1}[\overline{e_G}] \star \mu^{-1}[\overline{e_G}] = (\eta\mu)^{-1}[\overline{e_G}].$$

- Then $(X, \star)$ is a group isomorphic to N and

$$g \odot (\overline{x_1} \star \overline{x_2}) = (g \odot \overline{x_1}) \star \overline{g}^{-1} \star (g \odot \overline{x_2}),$$

where $\odot$ denotes left translation of cosets.

Skew bracoids

Definition

A *skew bracoid* is a 5-tuple $(G, \cdot, N, \star, \odot)$ where $(G, \cdot)$ and $(N, \star)$ are groups and $\odot$ is a transitive action of $(G, \cdot)$ on N such that

$$g \odot (\eta \star \mu) = (g \odot \eta) \star (g \odot e_N)^{-1} \star (g \odot \mu) \qquad (*)$$

for all $g \in G$ and $\eta, \mu \in N$.

- Where possible, we write simply $(G, N, \odot)$, or even (G, N).
- For now, we always assume G, N are finite. Then $|G| = |S||N|$, where $S = \mathrm{Stab}_G(e_N)$.
- Every skew brace is a skew bracoid, with $\odot$ and $\cdot$ coinciding.
- If $|N| = |G|$ then (G, N) is essentially a skew brace.

An example

Example

- Let $(G, \star, \cdot)$ be a skew brace and let H be a strong left ideal.
- H is a normal subgroup of $(G, \star)$, so $(G/H, \star)$ is a group.
- H is a subgroup of $(G, \cdot)$, so $(G, \cdot)$ acts by left translation on the coset space G/H. Write $\odot$ for this action.
- Then $(G, \cdot, G/H, \star, \odot)$ is a skew bracoid.

Question

Does every skew bracoid occur in this way?

Some characterizations

Theorem

Let $(G, \cdot), (N, \star)$ be finite groups. The following are equivalent:

1. *A transitive action $\odot$ of G on N such that $(G, \cdot, N, \star, \odot)$ is a skew bracoid;*
2. *a transitive subgroup A of $\mathrm{Hol}(N)$ isomorphic to a quotient of G;*
3. *a homomorphism $\gamma : G \to \mathrm{Aut}(N)$ and a surjective 1-cocycle $\pi : G \twoheadrightarrow N$.*

- The implication (1) $\to$ (2) uses the permutation representation $\lambda_\odot : G \to \mathrm{Perm}(N)$.
- The implication (2) $\to$ (3) gives rise to the γ-function of a skew bracoid.

Equivalence

Definition

Two skew bracoids (G, N) and (G', N') are called *equivalent* if $N = N'$ and $\lambda_{\odot}(G) = \lambda_{\odot'}(G') \subseteq \mathrm{Hol}(N)$.

- The analogous notion for skew braces is "equal".

Proposition

Let $(N, \star)$ be a group. There is a bijective correspondence between transitive subgroups of $\mathrm{Hol}(N)$ and equivalence classes of skew bracoids (G, N).

Reduction

Definition

A skew bracoid (G, N) is called *reduced* if $\lambda_{\odot} : G \to \mathrm{Hol}(N)$ is injective.

Proposition

Let (G, N) be a skew bracoid.

- Let $\overline{G} = G/\ker(\lambda_{\odot})$. Then $(\overline{G}, N)$ is a reduced skew bracoid, which will be called the *reduced form* of (G, N).
- Every skew bracoid is equivalent to its reduced form.

Example

If $(G, \cdot, G/H, \star, \odot)$ is a skew bracoid arising as a quotient of a skew brace by a strong left ideal then $\ker(\lambda_{\odot})$ is the normal core of H in $(G, \cdot)$, so $(G, G/H)$ is reduced if and only if H is core-free.

γ-functions

Proposition

Let (G, N) be a skew bracoid. Define $\gamma : G \to \text{Perm}(N)$ by

$$^{\gamma(g)}\eta = (g \odot e_N)^{-1} \star (g \odot \eta) \text{ for all } g \in G \text{ and } \eta \in N.$$

Then

- γ is a group homomorphism;
- $\gamma(G) \subseteq \text{Aut}(N)$.

- Caranti begins with a group $(G, \star)$ and uses $\gamma : G \to \text{Perm}(G)$ to characterize regular subgroups of $\text{Hol}(G, \star)$, and hence skew braces $(G, \star, \cdot)$ This approach does not seem to work well for transitive subgroups and skew bracoids.
- But see Stefanelli: affine structures etc.

Substructures

Definition

A *subskew bracoid* of a skew bracoid (G, N) consists of a subgroup H of G and a subgroup M of N such that (H, M) is a skew bracoid.

- It is possible for (G, N) to be reduced but for (H, M) to not be so.

Definition

A *left ideal* of a skew bracoid (G, N) is a subgroup M of N such that ${}^{\gamma(g)}M = M$ for all $g \in G$. An *ideal* is a left ideal M that is normal in N.

Proposition

If M is an ideal of (G, N) then $(G, N/M)$ is a skew bracoid.

Ideals

Proposition

Let M be a left ideal of (G, N), and let

$$G_M = \{g \in G \mid g \odot \mu \in M \text{ for all } \mu \in M\}.$$

Then (G_M, M) is a subskew bracoid of (G, N).

Proof.

It is clear that G_M is a subgroup of G.

Let $G_M^{(e)} = \{g \in G \mid g \odot e_N \in M\}$.

For all $g \in G$ and $\mu \in M$ we have

$$^{\gamma(g)}\mu = (g \odot e_N)^{-1} \star (g \odot \mu) \in M.$$

Hence $G_M^{(e)} = G_M$, so G_M is transitive on M. □

Back to Hopf-Galois structures

If L/K is a Galois extension with Galois group $(G, \cdot)$, Stefanello and Trappeniers show that there is a bijection between

- binary operations $\star$ on G such that $(G, \star, \cdot)$ is a skew brace;
- Hopf-Galois structures on L/K,

and also that the Hopf-Galois structure corresponding to $(G, \star, \cdot)$ is given by $L[G, \star]^{(G, \cdot)}$, acting via

$$\left(\sum_{g \in G} c_g g \right) [t] = \sum_{g \in G} c_g g[t].$$

Back to Hopf-Galois structures

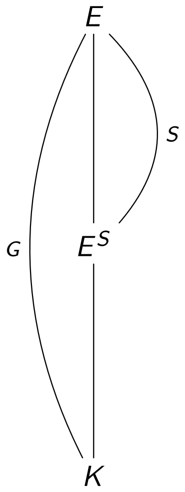
Theorem

Let E/K be a finite Galois extension with Galois group $(G, \cdot)$, and let $S \leq G$. There is a bijection between

- *binary operations $\star$ on $X = G/S$ such that $(G, \cdot, X, \star, \odot)$ is a skew bracoid;*
- *Hopf-Galois structures on E^S/K.*

Proof.

We have already seen how to get from a HGS on E^S/K to a skew bracoid $(G, \cdot, X, \star, \odot)$.



Back to Hopf-Galois structures

Proof continued...

Conversely, given a skew bracoid of the form $(G, \cdot, X, \star, \odot)$, consider $\rho_\star : X \to \mathrm{Perm}(X)$ defined by $\rho_\star(\overline{x})[\overline{y}] = \overline{y} \star \overline{x}^{-1}$.

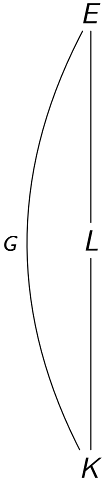
Then $\rho_\star(X)$ is a regular subgroup of $\mathrm{Perm}(X)$, and

$$\begin{aligned}
\lambda_\odot(g)\rho_\star(\overline{x})\lambda_\odot(g^{-1})[\overline{y}] &= g \odot ((g^{-1} \odot \overline{y}) \star \overline{x}^{-1}) \\
&= \overline{y} \star (g \odot \overline{e})^{-1} \star (g \odot \overline{x}^{-1}) \\
&= \overline{y} \star ((g \odot \overline{x})^{-1} \star (g \odot \overline{e})) \\
&= \rho_\star((g \odot \overline{e})^{-1} \star (g \odot \overline{x}))[\overline{y}] \\
&= \rho_\star \left({}^{\gamma(g)}\overline{x} \right) [\overline{y}]
\end{aligned}$$

So $\rho_\star(X)$ is G-stable, and therefore corresponds to a HGS on E^S/K. □

A more familiar perspective

- What if we **begin** with a finite separable extension L/K?
- To study HGS, we usually take E to be the Galois closure of L/K.
- But we can choose a larger finite Galois extension E/K.
- A given HGS yields numerous skew bracoids, depending on E. It turns out that these are all equivalent.



Hopf algebras and subalgebras

If L/K is a Galois extension with Galois group $(G, \cdot)$ and $(G, \star, \cdot)$ is a skew brace, Stefanello and Trappeniers show that

- The intermediate fields realized by the HGS $L[G, \star]^{(G, \cdot)}$ correspond with left ideals of $(G, \star, \cdot)$.
- If $(G', \star, \cdot)$ is a left ideal of $(G, \star, \cdot)$ then $L^{(G', \star)} = L^{(G', \cdot)}$.
- We obtain a quotient HGS on $L^{G'}/K$ if and only if $(G', \star, \cdot)$ is a strong left ideal, and a quotient skew brace if and only if $(G', \star, \cdot)$ is an ideal.

Hopf algebras and subalgebras

Now let E/K be Galois with group G, let $S \leq G$, and let $L = E^S$.

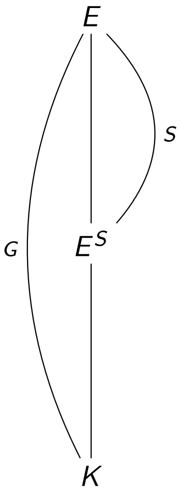
Let $(G, \cdot, X, \star, \odot)$ be a skew bracoid

Theorem

- *The corresponding Hopf-Galois structure on E^S/K is given by $E[X,\star]^{(G,\cdot)}$, acting via*

$$\left(\sum_{\overline{x} \in X} c_{\overline{x}} \overline{x} \right) [t] = \sum_{\overline{x} \in X} c_{\overline{x}} \overline{x}[t].$$

- *continued...*



Hopf algebras and subalgebras

Theorem (continued...)

- *The intermediate fields realized by the HGS correspond with left ideals of* $(G, \cdot, X, \star, \odot)$.
- *The left ideals have the form* $X' = G'/S$ *for certain* $G' \leq (G, \cdot)$, *and* $L^{(X', \star)} = E^{(G', \cdot)}$.
- *We obtain a quotient HGS on* $L^{(X', \star)}/K$ *and a quotient skew bracoid if and only if* X' *is an ideal.*
- *Since* $L^{(X', \star)} = E^{(G', \cdot)}$, *the extension* $L^{(X', \star)}/K$ *is Galois if and only if* G' *is normal in* G.

The natural questions

Question

Do skew bracoids have anything to do with groupoids?

- We think so, but we're not sure whether this perspective is beneficial.

Question

Are skew bracoids useful outside of their connection with Greither-Pareigis theory?

- We think they will have applications to classifying skew braces: e.g. via short exact sequences.

Question

Do skew bracoids have anything to do with the Yang-Baxter equation?

- Tentatively: Yes!

Thank you for your attention.