Introducing weak skew braces

Isabel Martin-Lyons and Paul Truman

Keele University, UK

Hopf algebras and Galois module theory
Friday 3rd June, 2022

Overview

Aim

Generalize the definition of skew braces to give objects corresponding to Hopf-Galois structures on separable, but non-normal, extensions.

- A route for constructing a skew brace from a Hopf-Galois structure on a Galois extension.
- Mimic this route in the non-normal case.
- Definition of weak skew brace.
- Substructures, homomorphisms, images, and kernels.
- Towards quotients.

What's in a name?

We have recently become aware of the paper

"Set-theoretic solutions of the Yang-Baxter equation associated to weak braces" by Francesco Catino, Marzia Mazzotta, Maria Maddalena Miccoli, Paola Stefanelli.

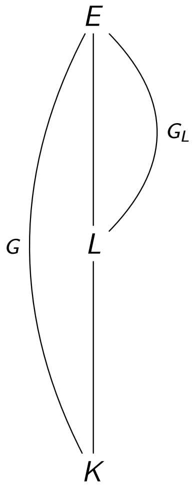
(They had previously called their objects "skew inverse semi-braces").

So we need a new name for our objects! Suggestions so far:

- dyads / skew dyads
- pre-skew braces / skew pre-braces
- non-normal skew braces
- **really** skew braces

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.



A route from a HGS to a skew brace

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

$$(\eta \cdot \mu)[e_G] = \eta[e_G]\mu[e_G].$$

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

$$\pi \cdot (\eta_1 \star \eta_2) = (\pi \cdot \eta_1) \star \pi^{-1} \star (\pi \cdot \eta_2),$$

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

A route from a HGS to a skew brace

Example

- Suppose that E/K is a Galois extension with Galois group

$$G = \langle r, s \mid r^4 = s^2 = e,\ sr\tilde{s} = \tilde{r} \rangle \cong D_4.$$

- Let $\eta = \lambda(r)$ and $\pi = \rho(s)$, and let $N = (N, \star) = \langle \eta, \pi \rangle$.
- Then N is a G-stable regular subgroup of $\mathrm{Perm}(G)$, isomorphic to $C_4 \times C_2$.
- Transporting the structure of G to N yields

$$\eta^i \pi^j \cdot \eta^k \pi^\ell = \eta^{i+(-1)^j k} \pi^{j+\ell},$$

and $(N, \star, \cdot)$ 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.
- As usual, let $G = \mathsf{Gal}(E/K)$, $G_L = \mathsf{Gal}(E/L)$, $X = G/G_L$.
- Suppose that $N = (N, \star)$ is a regular G-stable subgroup of $\mathrm{Perm}(X)$.
- The map $N \to X$ defined by $\eta \mapsto \eta[\overline{e_G}]$ is a bijection.
- Transport the action of G on X by left translation to N via

$$(g \odot \eta)[\overline{e_G}] = g\eta[\overline{e_G}].$$

This action is transitive.

Mimicking the route in the non-normal case

- How does this action interact with the group structure on N?
- For $\overline{x} \in X$, let $\mu_{\overline{x}} \in N$ be the unique element such that $\mu_{\overline{x}}[\overline{e_G}] = \overline{x}$.
- For $g \in G$ and $\eta \in N$ write $\theta_g(\eta) = \lambda(g)\eta\lambda(\tilde{g}) \in N$.
- We have

$$g \odot \eta = \theta_g(\eta) \star \mu_{\overline{g}}.$$

- Using this, we have:

$$\begin{aligned} g \odot (\eta_1 \star \eta_2) &= \theta_g(\eta_1 \star \eta_2) \star \mu_{\overline{g}} \\ &= \theta_g(\eta_1) \star \theta_g(\eta_2) \star \mu_{\overline{g}} \\ &= \theta_g(\eta_1) \star \mu_{\overline{g}} \star \mu_{\overline{g}}^{-1} \star \theta_g(\eta_2) \star \mu_{\overline{g}} \\ &= (g \odot \eta_1) \star \mu_{\overline{g}}^{-1} \star (g \odot \eta_2) \\ &= (g \odot \eta_1) \star (g \odot e_N)^{-1} \star (g \odot \eta_2). \end{aligned}$$

Mimicking the route in the non-normal case

Example

- Let $K = \mathbb{Q}$ and $L = K(\delta)$ with $\delta^4 = 2$.
- The Galois closure of L/K is $E = L(i)$.
- We have $G = \langle r, s \rangle \cong D_4$ with
$$r(\delta) = i\delta, \quad r(i) = i, \quad s(\delta) = \delta, \quad s(i) = -i.$$
- In this notation $G_L = \langle s \rangle$, and $X = \{\overline{e}, \overline{r}, \overline{r^2}, \overline{r^3}\}$.
- Let $\eta = \lambda(r) \in \mathrm{Perm}(X)$ and $N = \langle \eta \rangle$. Then N is regular and G-stable.
- The transitive action of G on N is given by
$$r^i s^j \odot \eta^k = \eta^{i+(-1)^j k}.$$

Mimicking the route in the non-normal case

Example (continued...)

Recall: The transitive action of G on N is given by

$$r^i s^j \odot \eta^k = \eta^{i+(-1)^j k}.$$

We have

$$\begin{aligned} r^i s^j \odot (\eta^k \star \eta^\ell) &= r^i s^j \odot (\eta^{k+\ell}) \\ &= \eta^{i+(-1)^j (k+\ell)}, \end{aligned}$$

whereas

$$\begin{aligned} (r^i s^j \odot \eta^k) \star (r^i s^j \odot e_N)^{-1} \star (r^i s^j \odot \eta^\ell) &= \eta^{i+(-1)^j k} \star \eta^{-i} \star \eta^{i+(-1)^j \ell} \\ &= \eta^{i+(-1)^j (k+\ell)}. \end{aligned}$$

The definition

Definition

A *weak skew brace* is a 5-tuple $\mathcal{W} = (G, \cdot, W, \star, \odot)$ where

- $(G, \cdot)$ and $(W, \star)$ are groups;
- $\odot$ is a transitive action of $(G, \cdot)$ on W such that for all $g \in G$ and $v, w \in W$ we have

$$g \odot (v \star w) = (g \odot v) \star (g \odot e_W)^{-1} \star (g \odot w)$$

where e_W is the identity element in W and $^{-1}$ denotes inverse with respect to $\star$.

The remarks

Recall: $\mathcal{W} = (G, \cdot, W, \star, \odot)$ with

$$g \odot (v \star w) = (g \odot v) \star (g \odot e_W)^{-1} \star (g \odot w) \tag{1}$$

- We call (1) *the weak skew brace relation.*
- We must have $|G|$ a multiple of $|W|$.
- A weak skew brace in which $|G| = |W|$ is essentially a skew brace.
- Where possible, we write $\mathcal{W} = (G, W, \odot)$, and say "weak brace".
- An alternative route is to transport the group structure of N to the set X, which already has a natural transitive action of G.
- We can also reinterpret the whole situation via Byott's translation theorem.
- All of these points of view ought to give "the same" answer: see later.

The correspondence

- We have seen that given a group G and a subgroup G_L, a regular G-stable subgroup of $\mathrm{Perm}(G/G_L)$ yields a weak brace $(G, N, \odot)$.
- Conversely, suppose that $\mathcal{W} = (G, W, \odot)$ is a weak brace.
- Let $\lambda_\star : W \to \mathrm{Perm}(W)$ be the left regular representation.
- Define $\lambda_\odot : G \to \mathrm{Perm}(W)$ by $\lambda_\odot(g)[w] = g \odot w$.
- We have

$$\begin{aligned} \lambda_\odot(g)\lambda_\star(v)\lambda_\odot(\tilde{g})[w] &= g \odot (v \star (\tilde{g} \odot w)) \\ &= (g \odot v) \star (g \odot e_W)^{-1} \star (g \odot (\tilde{g} \odot w)) \\ &= \lambda_\star((g \odot v) \star (g \odot e_W)^{-1})[w], \end{aligned}$$

So $\lambda_\star(W)$ is a G-stable subgroup of $\mathrm{Perm}(W)$.

The correspondence (continued)

- Now let $G' = \mathrm{Stab}_G(e_W)$.
- The map $W \to G/G'$ defined by

$$(g \odot e_W) \to gG'$$

is a well defined bijection, and induces an isomorphism

$$\mathrm{Perm}(W) \cong \mathrm{Perm}(G/G').$$

- This isomorphism transports $\lambda_\star(W)$ to a regular subgroup of $\mathrm{Perm}(G/G')$, and $\lambda_\odot(G)$ to $\lambda_.(G)$, the image of the left translation map.
- Hence we obtain a HGS on an appropriate separable extension.

Reducing problems

Definition

A weak brace $\mathcal{W} = (G, W, \odot)$ is said to be *reduced* if the action of G on W is faithful.

- Possibly this should be part of the definition, but this would cause problems concerning substructures: see later.
- Weak braces obtained from G/P theory are reduced.

Expectation

Every weak brace $\mathcal{W}$ should have a *reduced form*:

If $\mathcal{W} = (G, W, \odot)$ is not reduced then let $H = \ker(\lambda_{\odot})$ and consider $(G/H, W, \odot')$, with G/H acting in the natural way.

Need a notion of isomorphism to make this precise.

Substructures

Definition (Sub Weak Brace)

A weak brace $(H, V, \odot)$, is a sub weak brace of $(G, W, \odot)$ if

- H is a subgroup of G,
- V is a subgroup of W,
- $\odot$ restricts to a transitive action of H on V.

We also capture precisely these objects with the following formulation.

Proposition

Given a weak brace $\mathcal{W} = (G, W, \odot)$, if H is a subgroup of G and $V := \{h \odot e_W | h \in H\}$ is a subgroup of W, then $(H, V, \odot)$ is a sub weak brace of $\mathcal{W}$.

Morphisms

Definition (Homomorphism)

Let $\mathcal{W} = (G, W, \odot)$ and $\mathcal{W}' = (G', W', \odot')$ be weak braces,
$S = \mathrm{Stab}_G(e_W)$ and $S' = \mathrm{Stab}_{G'}(e_{W'})$.
A weak brace homomorphism $\boldsymbol{\varphi} : \mathcal{W} \to \mathcal{W}'$ comprises

- a group homomorphism $\varphi : G \to G'$ with $\varphi(S) \subseteq S'$
- an induced map $\bar{\varphi} : W \to W'$ given by $\bar{\varphi}(g \odot e_W) := \varphi(g) \odot' e_{W'}$, which we require is a group homomorphism $W \to W'$.

Definition (Isomorphism)

An isomorphism of weak braces is a homomorphism $\boldsymbol{\varphi}$ where the induced map $\bar{\varphi}$ is a group isomorphism and $\varphi(S) = S'$.

The Induced Map

$\boldsymbol{\varphi} : \mathcal{W} \to \mathcal{W}'$, $\varphi : G \to G'$ and $\bar{\varphi}(g \odot e_W) := \varphi(g) \odot' e_{W'}$.

Remarks

- Defining $\bar{\varphi}$ in this way ensures $\bar{\varphi}(g \odot w) = \varphi(g) \odot' \bar{\varphi}(w)$ in general. With $g \in G$, $w \in W$ and $g_w \in G$ such that $w = g_w \odot e_W$,

$$\begin{aligned} \bar{\varphi}(g \odot w) &= \bar{\varphi}(g \odot (g_w \odot e_W)) \\ &= \varphi(g \cdot g_w) \odot' e_{W'} \\ &= \varphi(g) \odot' (\varphi(g_w) \odot' e'_W) \\ &= \varphi(g) \odot' \bar{\varphi}(w). \end{aligned}$$

- Conversely, why not have unrelated homomorphism $\psi : W \to W'$ with $\psi(g \odot w) = \varphi(g) \odot' \psi(w)$ for all $g \in G$ and $w \in W$? Taking $w = e_W$, we end up back at our definition of $\bar{\varphi}$.

Reduction and Isomorphism

Recall that we call a weak brace $\mathcal{W} = (G, W, \odot)$ reduced if the action $\odot$ is faithful.

- Our current definition of isomorphic allows for a mismatch in the acting groups. This is motivated by G/P allowing for picking a larger extension than the Galois closure, and our feeling that this should give "the same" answer. On the weak brace end in the abstract, this is saying that if you throw away elements of G in the kernel of $\lambda_{\odot}$ then you have not lost anything meaningful.
- Unhappily, this means that it is possible for an isomorphism to have no inverse. But forcing the two weak braces to be reduced solves this.

Reduction and Isomorphism

Proposition

If there is a weak brace isomorphism $\varphi : \mathcal{W} \to \mathcal{W}'$, where $\mathcal{W}$ and $\mathcal{W}'$ are both reduced then $\varphi : G \to G'$ will also be an isomorphism.

Proof.

First show that φ is injective. Suppose $\varphi(g) = \varphi(h)$ for some $g, h \in G$,

$$\begin{aligned}
&\implies & \varphi(g) \odot' w' &= \varphi(h) \odot' w' && \forall w' \in W' \\
&\implies & \bar{\varphi}(g \odot w) &= \bar{\varphi}(h \odot w) && \forall w \in W \\
&\implies & g \odot w &= h \odot w && \forall w \in W \\
&\implies & g &= h.
\end{aligned}$$

The Orbit-Stabilizer theorem gives $|G| = |W||S| = |W'||S'| = |G'|$, so φ is really an isomorphism. □

Reduction

Proposition (Our Expectation)

For every weak brace $\mathcal{W} = (G, W, \odot)$ there is a reduced weak brace $\mathcal{W}' = (G', W, \odot')$ with $\mathcal{W}$ isomorphic to $\mathcal{W}'$.

Proof.

- If $\mathcal{W}$ is reduced then we are done. If not, let G' be $G/\ker(\lambda_{\odot})$, φ be the natural projection of G onto G', and G' act on W via $\odot'$ with $\bar{g} \odot' w = g \odot w$.
- Then $\bar{\varphi} : W \to W$ is given by $\bar{\varphi}(g \odot e_W) = \bar{g} \odot' e_W = g \odot e_W$, so that $\bar{\varphi}$ is in fact the trivial map $W \to W$, an isomorphism.
- The $\bar{g}$ for which $\bar{g} \odot' e_W = e_W$ are precisely those for which $g \odot e_W = e_W$ so $\varphi(\mathrm{Stab}_G(e_W)) = \mathrm{Stab}_{G'}(e_W)$.

□

Images and Kernels

As we would hope we find (fairly straightforwardly) that the image of a homomorphism is a sub weak brace of the codomain.

Much like our definition of isomorphism, we believe the focus with the kernel should be on the star groups. We propose

$$\ker(\boldsymbol{\varphi}) = (\varphi^{-1}(S'), \ker(\bar{\varphi}), \odot).$$

- The motivation for taking $\varphi^{-1}(S')$ as opposed to $\ker(\varphi)$ is that $\varphi^{-1}(S')$ acts transitively on $\ker(\bar{\varphi})$, where $\ker(\varphi)$ may not. This ensures that the kernel is a sub weak brace of the domain.
- Note that if the action $\odot$ is regular (so we essentially have a skew brace), S' is precisely $\{e_{G'}\}$ so $\varphi^{-1}(S')$ is actually the kernel of φ.

Kernels

Proposition

Let $\varphi : (G, \cdot, W, \star, \odot) \to (G', \cdot', W', \star', \odot')$ be a weak brace homomorphism. If $k \in \ker(\bar{\varphi})$ and $g \in G$, then

$$\gamma_g(k) = (g \odot e_W)^{-1} \star (g \odot k) \in \ker(\bar{\varphi}).$$

Proof.

Let $k \in \ker(\bar{\varphi})$ and $g \in G$. Then,

$$\begin{aligned}
\bar{\varphi}(\gamma_g(k)) &= \bar{\varphi}((g \odot e_W)^{-1} \star (g \odot k)) \\
&= (\bar{\varphi}(g \odot e_W))^{-1} \star' \bar{\varphi}(g \odot k) \\
&= (\varphi(g) \odot' e_{W'})^{-1} \star' (\varphi(g) \odot' e_{W'}) \\
&= e_{W'}.
\end{aligned}$$

Hence $\gamma_g(k) \in \ker(\bar{\varphi})$. □

Ideals

Bringing these properties together we form the definition of ideal.

Definition (Ideal)

Let $\mathcal{W} = (G, W, \odot)$, we define an ideal of $\mathcal{W}$ to be a sub weak brace $(H, V, \odot)$ where V is a normal subgroup W, and

$$\gamma_g(k) = (g \odot e_W)^{-1}(g \odot v) \in V$$

for all $g \in G$ and all $v \in V$.

Remark

When we specialize to the skew brace case, this definition amounts to a left ideal normal in the "additive" part. We do not require H to be normal in G as we expect this normality to correspond to intermediate Galois extensions on the Hopf-Galois end.

Towards Quotients

Proposition (A contender)

If $(H, V, \odot)$ is an ideal of $(G, W, \odot)$, then $(G, W/V, \odot)$ forms a weak brace, where $g \odot wV = (g \odot w)V$.

- The issue we have is that H is completely lost in the quotient.
- But we can use this to construct a weak skew brace from a genuine skew brace.

Weak Brace as the Quotient of a Skew Brace

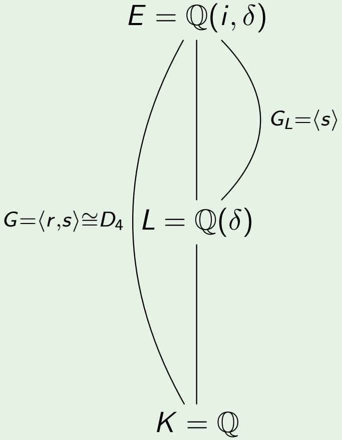
Example

Recall the setup for our examples, $\delta^4 = 2$.

$$\begin{tikzcd}
E = \mathbb{Q}(i, \delta) \arrow[d, no head] \arrow[d, no head, bend left=60, "G_L = \langle s \rangle"] \arrow[dd, no head, bend right=60, "G = \langle r, s \rangle \cong D_4"'] \\
L = \mathbb{Q}(\delta) \arrow[d, no head] \\
K = \mathbb{Q}
\end{tikzcd}$$

Weak Brace as the Quotient of a Skew Brace

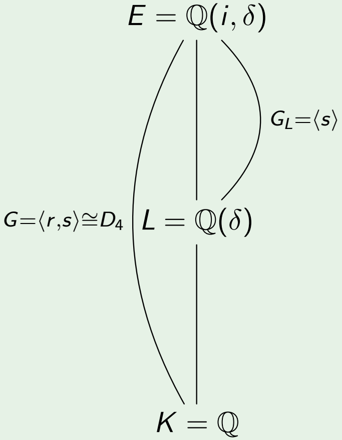
Example


$E = \mathbb{Q}(i, \delta)$
$G_L = \langle s \rangle$
$G = \langle r, s \rangle \cong D_4$
$L = \mathbb{Q}(\delta)$
$K = \mathbb{Q}$

Recall the setup for our examples, $\delta^4 = 2$. We found a skew brace coming from E/K given by $(N, \star, \cdot)$ where N is generated by $\eta = \lambda(r)$ and $\pi = \rho(s)$, $\star$ is composition in $\mathrm{Perm}(G)$, and $\eta^i \pi^j \cdot \eta^k \pi^\ell = \eta^{i+(-1)^j k} \pi^{k+\ell}$.

Weak Brace as the Quotient of a Skew Brace

Example



$E = \mathbb{Q}(i, \delta)$

$G_L = \langle s \rangle$

$G = \langle r, s \rangle \cong D_4$

$L = \mathbb{Q}(\delta)$

$K = \mathbb{Q}$

Recall the setup for our examples, $\delta^4 = 2$. We found a skew brace coming from E/K given by $(N, \star, \cdot)$ where N is generated by $\eta = \lambda(r)$ and $\pi = \rho(s)$, $\star$ is composition in $\mathrm{Perm}(G)$, and $\eta^i \pi^j \cdot \eta^k \pi^\ell = \eta^{i+(-1)^j k} \pi^{k+\ell}$.

Let M be the subgroup of $(N, \star)$ generated by π. Since $(N, \star)$ is abelian, this is automatically normal. Also,

$$\begin{aligned} (\eta^i \pi^j)^{-1} \star (\eta^i \pi^j \cdot \pi) &= \eta^{-i} \pi^{-j} \star \eta^i \pi^{j+1} \\ &= \pi \in M. \end{aligned}$$

Weak Brace as the Quotient of a Skew Brace

Example (continued...)

Now think of $(N, \star, \cdot)$ as the weak brace $(N, \cdot, N, \star, \odot)$ where $\odot$ is really the action of N on N via $\cdot$.

Weak Brace as the Quotient of a Skew Brace

Example (continued...)

Now think of $(N, \star, \cdot)$ as the weak brace $(N, \cdot, N, \star, \odot)$ where $\odot$ is really the action of N on N via $\cdot$.

Taking the quotient as we suggested we get $(N, \cdot, N/M, \star, \odot)$ where $\overline{\eta^i} \star \overline{\eta^j} = \overline{\eta^{i+j}}$ and $\eta^i \pi^j \odot \overline{\eta^k} = \overline{\eta^{i+(-1)^j k}}$. Checking the weak brace relation, we have

$$\begin{aligned} \eta^i \pi^j \odot (\overline{\eta^k} \star \overline{\eta^\ell}) &= \overline{\eta^{i+(-1)^j(k+\ell)}}, \\ (\eta^i \pi^j \odot \overline{\eta^k}) \star (\eta^i \pi^j \odot \overline{e_N})^{-1} \star (\eta^i \pi^j \odot \overline{\eta^\ell}) &= \overline{\eta^{i+(-1)^j k}} \star \overline{\eta^{-i}} \star \overline{\eta^{i+(-1)^j \ell}} \\ &= \overline{\eta^{i+(-1)^j(k+\ell)}}. \end{aligned}$$

Weak Brace as the Quotient of a Skew Brace

Example (continued...)

Now think of $(N, \star, \cdot)$ as the weak brace $(N, \cdot, N, \star, \odot)$ where $\odot$ is really the action of N on N via $\cdot$.

Taking the quotient as we suggested we get $(N, \cdot, N/M, \star, \odot)$ where $\overline{\eta^i} \star \overline{\eta^j} = \overline{\eta^{i+j}}$ and $\eta^i \pi^j \odot \overline{\eta^k} = \overline{\eta^{i+(-1)^j k}}$. Checking the weak brace relation, we have

$$\begin{aligned} \eta^i \pi^j \odot (\overline{\eta^k} \star \overline{\eta^\ell}) &= \overline{\eta^{i+(-1)^j(k+\ell)}}, \\ (\eta^i \pi^j \odot \overline{\eta^k}) \star (\eta^i \pi^j \odot \overline{e_N})^{-1} \star (\eta^i \pi^j \odot \overline{\eta^\ell}) &= \overline{\eta^{i+(-1)^j k}} \star \overline{\eta^{-i}} \star \overline{\eta^{i+(-1)^j \ell}} \\ &= \overline{\eta^{i+(-1)^j(k+\ell)}}. \end{aligned}$$

Hopefully this looks familiar, because what we have constructed is a relabeling of the example of a weak brace from earlier.

Where next?

- Refine notions of isomorphism and quotient.
- Examples and classifications: for example $|W| = pq$ (Byott / Martin-Lyons / Darlington).
- Almost classically Galois weak braces (Nicest examples of non-normal extensions).
- Opposite weak braces / links with Hopf-Galois correspondence (Koch / Truman / Childs / Caranti / Stefanello etc.)
- Isomorphism problems: when do two regular subgroups give isomorphic weak braces? (Koch / Truman)
- Does all of this have anything to do with the Yang-Baxter equation? (Paul's grant)

Thank you for your attention.