Abelian maps and brace blocks

Alan Koch

Agnes Scott College

Fauxmaha, May 25, 2021

Outline

Abelian maps: a review

Let $G = (G, \cdot)$ be a (nonabelian) group.

Let L/K be a Galois extension, Galois group G.

An *abelian map* on G is an endomorphism $\psi : G \to G$ such that $\psi(G) \leq G$ is abelian.

Denote by $\mathrm{Ab}(G)$ the set of all abelian maps on G.

In 2020 we showed how $\psi \in \mathrm{Ab}(G)$ could be used to put a Hopf-Galois structure on L/K, as well as construct a (bi-skew) brace.

The Hopf-Galois structure: a review

Let $\psi \in \mathrm{Ab}(G)$.

For $g \in G$ define $\eta_g : G \to G$ by $\eta_g[h] = g\psi(g^{-1})h\psi(g)$.

Note $\eta_g[1_G] = g$.

Then $N := \{\eta_g : g \in G\}$ is a regular, G-stable subgroup of $\mathrm{Perm}(G)$.

("G-stable" = "normalized by conjugation by $\lambda(G) \leq \mathrm{Perm}(G)$".)

Explicitly, for $k, g \in G$ we have ${}^k\eta_g = \eta_{kg\psi(g^{-1})k^{-1}\psi(g)}$.

So, by Greither-Pareigis, $L[N]^G$ is a Hopf algebra which puts a Hopf-Galois structure on L/K.

The HGS structure is said to be of *type* N.

Also, $\psi_1, \psi_2 \in \mathrm{Ab}(G)$ give the same Hopf-Galois structure if and only if $\psi_1(g)\psi_2(g^{-1}) \in Z(G)$ for all $g \in G$.

The commuting Hopf-Galois structure: a review

Recall that if N is a regular, G-stable subgroup, then so is

$$N' := \mathrm{Cent}_{\mathrm{Perm}(G)}(N) = \{\pi \in \mathrm{Perm}(G) : \pi\eta = \eta\pi \text{ for all } \eta \in N\}.$$

For $\psi \in \mathrm{Ab}(G)$ we have $N = \{\eta_g : g \in G\},\ \eta_g[h] = g\psi(g^{-1})h\psi(g)$.

Easy to verify that $N' = \{\pi_g : g \in G\}$ with

$$\pi_g[h] = h\psi(h^{-1})g\psi(h).$$

Thus, ψ gives us two related Hopf-Galois structures (G nonabelian).

"Related": the actions of $H := L[N]^G$ and $H' := L[N']^G$ on L/K commute with each other [Truman, 2018].

The brace: a review

Recall a *skew left brace* (hereafter, *brace*) is a triple $(B, \cdot, \circ)$ where $(B, \cdot)$ and $(B, \circ)$ are groups (*dot group* and *circle group* respectively) and, for all $x, y, z \in B$,

$$x \circ (y \cdot z) = (x \circ y) \cdot x^{-1} \cdot (x \circ z), \; x \cdot x^{-1} = 1_B.$$

Turns out $x \cdot 1_B = x \circ 1_B = x$ for all $x \in B$.

We will frequently suppress the dot and write $xy = x \cdot y$.

Proposition (K, 2020)

Let $\psi \in \mathrm{Ab}(G)$*, and define* $g \circ h = \eta_g[h] = g\psi(g^{-1})h\psi(g)$*.*
Then $(G, \cdot, \circ)$ *is a brace.*

Caveat. The "abelian map to brace" relationship here is different from the usual "regular, G-stable subgroup" to "brace" relationship given by Byott and Vendramin.

Opposite braces: a review

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

Then $(B, \cdot', \circ)$ is also a brace, where $a \cdot' b = b \cdot a$.

We call this is *opposite brace* to the one above. (Developed independently by K-Truman and Rump.)

Fact. [K-Truman, 2019] If $N \leq \mathrm{Perm}(G)$ is regular and G-stable, and $N' = \mathrm{Cent}_{\mathrm{Perm}(G)} N$, then their corresponding braces are opposite.

Yang-Baxter equation: a review

Braces give set-theoretic solutions to the Yang-Baxter equation.

A set-theoretic solution to the YBE is a set B and a function $R : B^2 \to B^2$ such that

$$(R \times \mathrm{id})(\mathrm{id} \times R)(R \times \mathrm{id}) = (\mathrm{id} \times R)(R \times \mathrm{id})(\mathrm{id} \times R).$$

If $(B, \cdot, \circ)$ is a brace and $\overline{a}$ is the inverse to $a \in (G, \circ)$ then

$$R(x, y) = (x^{-1}(x \circ y), \overline{x^{-1}(x \circ y)} \circ x \circ y),\ \ x, y \in B$$

is the corresponding solution.

By considering the opposite brace, we get the additional solution

$$R'(x, y) = ((x \circ y)x^{-1}, \overline{(x \circ y)x^{-1}} \circ x \circ y),\ \ x, y \in B,$$

which is inverse to the one above (in that $R'R = RR' = \mathrm{id}$).

Equivalent solutions

Suppose $(B_1, \cdot_1, \circ_1)$ and $(B_2, \cdot_2, \circ_2)$ are isomorphic braces, i.e., there is a bijection $\varphi : B_1 \to B_2$ which which preserve the dot and circle operations.

Let R_1, R_2 be the corresponding YBE solutions.

Then $R_1 \neq R_2$ in general, however we will say that these two solutions are *equivalent*.

Short rationale: B_1, B_2 each induce vector space solutions to the YBE $r : V \otimes V \to V \otimes V$ with analogous twisting property, where $\dim V = |B_1| = |B_2|$. Equivalent set-theoretic braces give the same vector space solution up to a choice of basis.

Fact. If $(G, \cdot, \circ)$ is a brace, the isomorphic braces with the same circle group $(G, \circ)$ are of the form $(G, \cdot_\varphi, \circ)$ where $\varphi \in \mathrm{Aut}(G, \circ)$ and $g \cdot_\varphi h = \varphi(\varphi^{-1}(g) \cdot \varphi^{-1}(h))$.

The solutions of interest to us: a review

Example (abelian map case)

For $\psi \in \text{Ab}(G)$ we get the brace described previously, which leads to the solution

$$R(g,h) = \left(\psi(g^{-1})h\psi(g), \psi(hg^{-1})h^{-1}\psi(g)g\psi(g^{-1})h\psi(gh^{-1})\right)$$

Using the opposite brace, we get the second solution

$$R'(g,h) = (g\psi(g^{-1})g\psi(g)g^{-1}, \psi(h)g\psi(h^{-1})).$$

We have seen that ψ_1, ψ_2 give the same brace (and hence the same solution) if and only if $\psi_1(g)\psi_2(g^{-1}) \in Z(G)$ for all $g \in G$.

Note that if $\psi \in \text{Ab}(G)$, then $\varphi\psi\varphi^{-1} \in \text{Ab}(G)$ for all $\varphi \in \text{Aut}(G)$, and their braces are necessarily isomorphic.

The bi-skew brace: a review

Recall that a brace $(B, \cdot, \circ)$ is a *bi-skew brace* if $(B, \circ, \cdot)$ is also a brace.

In other words, $(B, \cdot, \circ)$ is a bi-skew brace if any only if

$$\begin{aligned} a \circ (b \cdot c) &= (a \circ b) \cdot a^{-1} \cdot (a \circ c) \\ a \cdot (b \circ c) &= (a \cdot b) \circ \overline{a} \circ (a \cdot c). \end{aligned}$$

Easy to show: for $\psi \in \mathrm{Ab}(G)$ the resulting brace $(G, \cdot, \circ)$ is bi-skew.

In fact, $(G, \circ, \cdot)$ is the Byott-Vendramin brace corresponding to the regular, G-stable subgroup $N = \{\eta_g : g \in G\}$.

An observation from 2020

If $\psi \in \mathrm{Ab}(G) = \mathrm{Ab}(G, \cdot)$, then

$$\psi(g \circ h) = \psi(g) \circ \psi(h),$$

i.e., $\psi \in \mathrm{Ab}(G, \circ)$.

Thus we could apply the brace construction starting with $(G, \circ)$: if

$$g \star h = g \circ \psi(\overline{g}) \circ h \circ \psi(g)$$

then $(G, \circ, \star)$ is a bi-skew brace.

Repeating this idea would, in theory, create a “bi-skew brace chain”.

However, it turns out $(G, \cdot, \star)$ is also a bi-skew brace.

So perhaps more is going on here.

Brace blocks

This is our new construction for 2021.

Definition

A *brace block* is a set B together with a family of binary operations $\{\circ_n : n \in \mathbb{Z}^{\geq 0}\}$ such that $(B, \circ_m, \circ_n)$ is a brace for all $m, n \geq 0$.

Note that each brace in a brace block is necessarily bi-skew.

However, it is useful to simply regard them as (skew left) braces.

First examples

Example (Trivial brace block)

Let $(G, \cdot)$ be a group, and let $(g \circ_n h) = gh$ for all n. Then each brace is the trivial brace on G (i.e., the two operations coincide).

Example (Almost trivial brace block)

Let $(G, \cdot)$ be a group, and let

$$g \circ_n h = \begin{cases} gh & n \text{ even} \\ hg & n \text{ odd} \end{cases}.$$

Then $(G, \circ_m, \circ_n)$ is the trivial brace if $m \equiv n \pmod 2$; otherwise it is the *almost trivial brace*.

More interesting examples are coming.

Outline

Some notation

Let $(G,\cdot)$ be a group. Denote by $\mathsf{Map}(G)$ the set of functions $G \to G$.

For $\alpha, \beta \in \mathsf{Map}(G)$, $n \in \mathbb{Z}$ define

$$\begin{aligned}
(\alpha+\beta)(g) &= \alpha(g)\beta(g) \\
(\alpha\beta)(g) &= \alpha(\beta(g)) \\
\alpha^n &= \alpha\cdot\alpha\cdots\alpha,\ \alpha^0 = \mathrm{id} && (n>0) \\
(n\alpha)(g) &= \alpha(g^n) \\
(\alpha-\beta) &= \alpha + (-1\beta) \\
1 &= \mathrm{id} \\
0(g) &= 1_G.
\end{aligned}$$

Then $\mathsf{Map}(G)$ is a right near-ring ($(\mathsf{Map}(G),+)$ nonabelian, no left distributive law).

$(\alpha+\beta)(g)=\alpha(g)\beta(g),\ n\alpha(g)=\alpha(g^n)$

Some facts:

- Neither $\mathrm{Ab}(G)$ nor $\mathrm{End}(G)$ are closed under $+$.
- Both $\mathrm{Ab}(G)$ and $\mathrm{End}(G)$ are closed under multiplication.
- Both $\mathrm{Ab}(G)$ and $\mathrm{End}(G)$ contain 0, and $1 \in \mathrm{End}(G)$.
- If $\psi \in \mathrm{Ab}(G)$ then $-\psi \in \mathrm{Ab}(G)$.
- For $\psi \in \mathrm{Ab}(G)$ and $\phi \in \mathrm{End}(G)$ we have $\psi\phi \in \mathrm{Ab}(G)$.
- For $\psi \in \mathrm{Ab}(G),\ \psi^n \in \mathrm{Ab}(G)$ for all $n \geq 0$.
- For $\psi \in \mathrm{Ab}(G),\ k\psi^m + \ell\psi^n = \ell\psi^n + k\psi^m \in \mathrm{Ab}(G)$ for all $k, \ell, m, n \in \mathbb{Z},\ m, n > 0$.
- For $\psi \in \mathrm{Ab}(G),\ \alpha, \beta \in \mathrm{Map}(G),\ \psi(\alpha+\beta) = \psi\alpha + \psi\beta$.
- For all $\alpha, \beta \in \mathrm{Map}(G),\ -(\alpha+\beta) = -\beta - \alpha$.

Near-ring a definition

Let $\psi \in \mathrm{Ab}(G)$. For each $n \geq 0$, define

$$\boxed{\psi_n = -(1-\psi)^n + 1.}$$

For example,

$$\begin{aligned}
\psi_0 &= -1 + 1 = 0 \\
\psi_1 &= -(1-\psi) + 1 = (\psi - 1) + 1 = \psi \\
\psi_2 &= -(1-\psi)^2 + 1 = -\left((1-\psi)(1-\psi)\right) + 1 \\
&= -\left((1-\psi) - \psi(1-\psi)\right) + 1 \\
&= -\left(1 - \psi + \psi^2 - \psi\right) + 1 \\
&= 2\psi - \psi^2.
\end{aligned}$$

$\psi_n = -(1-\psi)^n + 1$

Properties, $\psi \in \mathrm{Ab}(G)$:

1. (Explicit formulation) $\psi_n = \binom{n}{1}\psi - \binom{n}{2}\psi^2 + \cdots \pm \binom{n}{n}\psi^n$, i.e.,
$$\psi_n(g) = \psi\left(g^{\binom{n}{1}}\right)\psi^2\left(g^{\binom{n}{2}}\right)^{-1}\cdots\psi^n(g^{\binom{n}{n}})^{\pm 1}.$$
2. (Recursive formulation) $\psi_n = \psi + \psi_{n-1}(1-\psi)$, i.e.,
$$\psi_n(g) = \psi(g)\psi_{n-1}(g\psi(g^{-1})).$$
3. (Compatibility with multiplication) $(\psi_m)_n = \psi_{mn}$.
4. (Abelianness) $\psi_n \in \mathrm{Ab}(G)$.

$\psi \in \mathrm{Ab}(G) \Rightarrow \psi_n \in \mathrm{Ab}(G),\ \psi_n = \psi + \psi_{n-1}(1 - \psi)$

That $\psi_n \in \mathrm{Ab}(G)$ means that we can use ψ_n to create braces.

Let $g \circ_n h = g\psi_n(g^{-1})h\psi_n(g)$.

Then $(G, \cdot, \circ_n)$ is a brace.

By the recursive formulation of ψ_n we can show

$$g \circ_n h = ((g\psi(g^{-1}) \circ_{n-1} h))\psi(g),\ g, h \in G.$$

Note that since $\psi_0 = 0$ and $\psi_1 = \psi$ we have $(G, \circ_0) = (G, \cdot)$ and $(G, \circ_1) = (G, \circ)$.

Main result

Theorem (K, 2021)

Let $\psi \in \mathrm{Ab}(G)$. Then $(G, \circ_m, \circ_n)$ is a brace, hence $\{G, \circ_0, \circ_1, \dots\}$ is a brace block.

This can (but won't) be shown by computation.

Case $m = 0$ Follows from above.

Case $m \mid n$ Follows from above using $(\psi_m)_{n/m} \in \mathrm{Ab}(G, \circ_m)$ since $(\psi_m)_n = \psi_{mn}$.

Recall

3. (Compatibility with multiplication) $(\psi_m)_n = \psi_{mn}$.

An abelian group wipes out the block

Suppose $(G, \circ_n)$ is abelian.

Then, since $\psi_k(x)\psi_\ell(y) = \psi_\ell(y)\psi_k(x)$ for $k, \ell > 0$,

$$\begin{aligned} g \circ_{n+1} h &= ((g\psi(g^{-1}) \circ_n h)\psi(g) \\ &= (h \circ_n g\psi(g^{-1}))\psi(g) \\ &= h\psi_n(h^{-1})g\psi(g^{-1})\psi_n(h)\psi(g) \\ &= h\psi_n(h^{-1})g\psi_n(h) \\ &= h \circ_n g \\ &= g \circ_n h. \end{aligned}$$

So $(G, \circ_m) = (G, \circ_n)$ for all $m \geq n$.

Once a brace block creates an abelian group, no new braces are constructed.

Outline

We can describe the regular, G-stable subgroups of $\mathrm{Perm}(G)$ arising from a brace block.

Let $\psi \in \mathrm{Ab}(G)$. For $n \geq 0$ define $N_n = \{\eta_g^{(n)},\ g \in G\} \subset \mathrm{Perm}(G)$ by

$$\eta_g^{(n)}[h] = g\psi_n(g^{-1})h\psi_n(g),\ g, h \in G.$$

Then $N_n \leq \mathrm{Perm}(G)$ is regular and G-stable.

Note $N_0 = \lambda(G)$.

In general, $N_n \ncong G$, in fact $\eta_g^{(n)}\eta_h^{(n)} = \eta_{g\circ_n h}^{(n)}$; hence, $N_n \cong (G, \circ_n)$.

A special case: fixed point free abelian maps

The theory of abelian maps comes from Childs's 2013 construction of "fixed point free abelian maps", i.e., $\psi \in \mathrm{Ab}(G)$ with $\psi(g) = g$ iff $g = 1_G$.

Turns out $\psi_n \in \mathrm{Ab}(G)$ is fixed point free if and only if ψ is.

If ψ is fixed point free, then $N_n \cong \lambda(G)$; in fact $L[N_n]^G \cong H_\lambda$ as K-Hopf algebras, where H_λ is the Hopf algebra giving the "canonical nonclassical" Hopf-Galois structure.

More generally

Consider the brace block induced by ψ.

Then we have groups $N_0, N_1, \dots$ with $N_m = (G, \circ_m)$.

Let $m \geq 0$, and let L_m/K_m be a Galois extension with $Gal(L_m/K_m) = N_m$.

We then have Hopf-Galois structures on L_m/K_m.

Question. For each $n \geq 0$, can we explicitly realize $N_n \leq \mathrm{Perm}(N_m)$?

As before, write $N_m = \{\eta_g^{(m)} : g \in G\},\ \eta_g^{(m)}[h] = g\psi_m(g^{-1})h\psi_m(g)$.

Similarly for N_n.

$N_m = \{\eta_g^{(m)} : g \in G\},\ \eta_g^{(m)}[h] = g\psi_m(g^{-1})h\psi_m(g)$

Let

$$\eta_g^{(n)}[\eta_h^{(m)}] = \eta_{g\circ_n h}^{(m)}.$$

This is a regular action, and

$$\lambda(\eta_k^{(m)})\eta_g^{(n)}\lambda(\eta_k^{(m)})^{-1} = \eta^{(n)}_{k\psi_m(k^{-1})g\psi_m(k)\psi_n(g^{-1})k^{-1}\psi_n(g)}.$$

In the special case $m = 0$ (so $N_0 \cong G$ via $\eta_g^{(0)} \leftrightarrow g$) we get

$$\eta_g^{(n)}[\eta_h^{(0)}] = \eta_{g\circ_n h}^{(0)} \leftrightarrow g \circ_n h = g\psi_n(g^{-1})h\psi_n(g) = \eta_g^{(n)}[h]$$

and

$$\lambda(\eta_k^{(0)})\eta_g^{(n)}\lambda(\eta_k^{(0)})^{-1} = \eta^{(n)}_{k\psi_0(k^{-1})g\psi_0(k)\psi_n(g^{-1})k^{-1}\psi_n(g)} = \eta^{(n)}_{kg\psi_n(g^{-1})k^{-1}\psi_n(g)}$$

as expected.

Outline

A collection of solutions

Recall $\psi \in \mathrm{Ab}(G)$ gives the brace $(G, \cdot, \circ)$ and the YBE solution

$$R(g,h) = \left(\psi(g^{-1})h\psi(g), \psi(hg^{-1})h^{-1}\psi(g)g\psi(g^{-1})h\psi(gh^{-1})\right).$$

Since $\psi_n \in \mathrm{Ab}(G)$ we quickly get solutions from the braces $(G, \cdot, \circ_n)$:

$$R(g,h) = \left(\psi_n(g^{-1})h\psi_n(g), \psi_n(hg^{-1})h^{-1}\psi_n(g)g\psi_n(g^{-1})h\psi_n(gh^{-1})\right).$$

More generally, for $(G, \circ_m, \circ_n)$ the solution is

$$\begin{aligned} R(g,h) = (&\psi_m(g)\psi_n(g^{-1})h\psi_n(g)\psi_m(g^{-1}), \\ &\psi_m(g)\psi_n(hg^{-1})h^{-1}\psi_n(g)\psi_m(g^{-1})g\psi_n(g^{-1})h\psi_n(gh^{-1})). \end{aligned}$$

Twice as many solutions

$$R(g,h) = (\psi_m(g)\psi_n(g^{-1})h\psi_n(g)\psi_m(g^{-1}),$$
$$\psi_m(g)\psi_n(hg^{-1})h^{-1}\psi_n(g)\psi_m(g^{-1})g\psi_n(g^{-1})h\psi_n(gh^{-1}))$$

The above comes from the brace $(G, \circ_m, \circ_n)$.

However, the opposite brace $(G, \circ'_m, \circ_n)$ with
$g \circ'_m h = h \circ_m g = h\psi_m(h^{-1})g\psi_m(h)$ gives another solution, namely

$$R'(g,h) = (g\psi_n(g^{-1})h\psi_n(g)\psi_m(h^{-1})g^{-1}\psi_m(h),$$
$$\psi_n(h)\psi_m(h^{-1})g\psi_m(h)\psi_n(h^{-1})).$$

Of course, $R = R'$ if and only if $(G, \circ_m)$ is abelian.

Not four times as many solutions

Of course, since $(B, \circ_m, \circ_n)$ is a bi-skew brace we would get *four* solutions, one from each of the braces

1. $(B, \circ_m, \circ_n)$
2. $(B, \circ'_m, \circ_n)$
3. $(B, \circ_n, \circ_m)$
4. $(B, \circ'_n, \circ_m)$.

However, when working with brace blocks we only consider solutions of type (1) and (2) to prevent double counting.

Outline

Semidirect products

Let $G = H \rtimes K$ with K abelian. Define $\psi : G \to G$ by $\psi(hk) = k$.

Then ψ is abelian, $\ker\psi = H$, $\psi(G) = K$, and $(G, \circ) \cong H \times K$.

Clearly, $\psi^n(hk) = k = \psi(k)$ for all $hk \in G$, hence $\psi^n = \psi$, $n \geq 1$. So,

$$\psi_n = \binom{n}{1}\psi - \binom{n}{2}\psi^2 + \cdots \pm \binom{n}{n}\psi^n = \left(\binom{n}{1} - \binom{n}{2} + \cdots \pm \binom{n}{n}\right)\psi = \psi.$$

Thus we have two trivial (nonisomorphic) braces $(G, \cdot, \cdot)$ and $(G, \circ, \circ)$, as well as the braces $(G, \cdot, \circ)$, $(G, \circ, \cdot)$ with $h_1k_1 \circ h_2k_2 = h_1h_2k_1k_2$.

We get 8 solutions to the YBE, or 6 if H is abelian; and

- 2 HGS on a Galois extension, Galois group G of type G, 1 or 2 of type $H \times K$.
- 1 or 2 HGS on an extension with Galois group $H \times K$ of type $H \times K$, 2 of type G.

Dihedral

Let $G = D_n = \langle r, s : r^n = s^2 = rsrs = 1_G \rangle$ and let $\psi \in \mathrm{Ab}(G)$.

Can show that $|\psi(g)| = 1, 2$ for all g, so $2\psi = 0$.

Possibilities:

- $\psi = 0$. Then $\psi_n = -(1-\psi)^n + 1 = -(1^n) + 1 = 0$ for all n. Every brace is trivial, and every Hopf-Galois structure is the canonical nonclassical one.
- $\psi \neq 0$, fixed point free. By [Childs, 2013], $\psi(G) = \langle x \rangle$ for some $x \in D_n$ of order 2.
  Since $\psi(x) \neq x,\ \psi(x) = 1_G$ and $\psi^2 = 0$.
  So $\psi_n = \binom{n}{1}\psi - \binom{n}{2}\psi^2 + \cdots \pm \binom{n}{n}\psi^n = n\psi = \begin{cases} 0 & 2 \mid n \\ \psi & 2 \nmid n \end{cases}.$
  The resulting braces are $(G, \cdot, \cdot) = (G, \circ, \circ)$, $(G, \cdot, \circ) \cong (G, \circ, \cdot)$, giving 4 nonequivalent solutions to the YBE.
  Note. $(G, \circ, \cdot) \cong (G, \cdot, \circ)$ via the map $1 - \psi : g \mapsto g\psi(g^{-1})$.

A quick aside: $(1-\psi)(g) = g\psi(g^{-1})$

Proposition

Let G be a nonabelian group, and suppose $\psi \in \mathrm{Ab}(G)$ is fixed point free. Then for all $0 \le m \le n$ we have $(G, \circ_m, \circ_n) \cong (G, \cdot, \circ_{n-m})$.

Sketch. Verify $1-\psi : (G, \circ_m, \circ_n) \to (G, \circ_{m-1}, \circ_{n-1})$ is an isomorphism.

(Easy to see–and well-known–that $\psi \in \mathrm{Ab}(G)$ is fixed point free if and only if $1-\psi$ is a bijection.)

In the D_n example, $\circ_2 = \circ_0 = \cdot$, so

$$(G, \cdot, \circ) = (G, \circ_0, \circ_1) \cong (G, \circ_1, \circ_2) = (G, \circ, \cdot).$$

Back to $G = \langle r, s \rangle$

Generally, let $\mathrm{FP}(\psi)$ be the subgroup of G consisting of fixed points.

- $\mathrm{FP}(\psi) \neq \{1_G\}$. By [K, 2020], $\psi(G) = \{1_G, x\} = \mathrm{FP}(\psi)$.
  Then $\psi^2(g) = \psi(g)$ for all $g \in G$, i.e., $\psi^2 = \psi$. Generally, $\psi^n = \psi$.
  We get four braces: $(G, \cdot, \cdot)$, $(G, \circ, \circ)$,$(G, \cdot, \circ)$, and $(G, \circ, \cdot)$.
  The trivial braces are different from each other since
  $(G, \circ) \cong C_n \times C_2$ or $D_{n/2} \times C_2$ (depending on various factors).

  We get either 6 or 8 solutions to the YBE, and:
  - 3 or 4 HGS for $\mathrm{Gal}(L/K) = D_n$: two of type D_n; and one of type C_{2n} or two of type $D_{n/2} \times C_2$.
  - 3 HGS for $\mathrm{Gal}(L/K) = C_{2n}$, *or* 4 HGS for $\mathrm{Gal}(L/K) = D_{n/2} \times C_2$.

Outline

$G = D_n \times D_n$

Let $G = \langle r, s : r^n = s^2 = rsrs = 1_G \rangle \times \langle t, u : t^n = u^2 = tutu = 1_G \rangle$, where $n \geq 3$ is odd.

Define $\psi : G \to G$ by $\psi(r) = \psi(t) = 1_G,\ \psi(s) = u,\ \psi(u) = s$.

Then $\psi(G) = \langle s, u \rangle \cong C_2 \times C_2$ so $\psi \in \mathrm{Ab}(G)$.

Since $su = \psi(us)$,

$$g \circ (su) = g \circ \psi(us) = g\psi(g^{-1})\psi(us)\psi(g) = g\psi(us) = gsu$$

and

$$(su \circ g) = su\psi(su)^{-1}g\psi(su) = suusgsu = gsu,$$

hence $su \in Z(G, \circ)$.

Since $Z(G, \cdot)$ is trivial we get $(G, \circ) \not\cong (G, \cdot)$.

Also, $Z(G, \circ)$ is not abelian ($r \circ u = ru,\ u \circ r = r^{-1}u$).

In fact, $(G, \circ) \cong C_2 \times ((C_n \times C_n) \rtimes C_2)$ where C_2 acts via inverse.

$G = \langle r, s, t, u \rangle,\ \psi(r) = \psi(t) = 1_G,\ \psi(s) = u,\ \psi(u) = s$

Now $\psi_2 = 2\psi - \psi^2$, so

$$\psi_2(r) = \psi(r^2)\psi^2(r^{-1}) = 1_G \qquad \psi_2(s) = \psi(s^2)\psi^2(s^{-1}) = s$$
$$\psi_2(t) = \psi(t^2)\psi^2(t^{-1}) = 1_G \qquad \psi_2(u) = \psi(u^2)\psi^2(u^{-1}) = u.$$

Thus $\ker \psi_2 = \langle r, t \rangle$ and $\mathrm{FP}(\psi_2) = \langle s, u \rangle$.

It follows that $(G, \circ_2) \cong \langle r, t \rangle \times \langle s, u \rangle \cong C_n \times C_n \times C_2 \times C_2 \cong C_{2n}^2$.

We get nine nonisomorphic braces $(G, \circ_m, \circ_n),\ 0 \le m, n \le 2$, which give one YBE solution when $m = 2$ and two solutions otherwise.

In total, we get $6 \cdot 2 + 3 = 15$ solutions.

Also, we get five HGS in each of the cases $\mathrm{Gal}(L/K) = D_n \times D_n,\ C_2 \times ((C_n \times C_n) \rtimes C_2)$, and $C_{2n} \times C_{2n}$: two of type $D_n \times D_n$, two of type $C_2 \times ((C_n \times C_n) \rtimes C_2)$, and one of type $C_{2n} \times C_{2n}$.

Semidirect products of certain cyclic groups

Thanks to Lindsay Childs for pointing these out.

Let $G = G_{h,k,b} = \langle s, t : s^h = t^k = tst^{-1}s^{-b} = 1_G \rangle$ where $k \mid \phi(h)$ and $b \in \mathbb{Z}_h^\times$ has order k.

We are interested in groups of the form G_{h,k,b^n} for some n.

Note that b^n may not have order k, but there is a $c \in \mathbb{Z}_h^\times$ of order k with $G_{h,k,c} = G_{h,k,b^n}$.

For brevity, write $G_n = G_{h,k,b^n}$ and assume h, k, b fixed.

$G_n = \langle s, t : s^h = t^k = tst^{-1}s^{-b^n} = 1_G \rangle$

Results we need:

Lemma (Childs, 2020)

We have $G_n \cong G_{\gcd(k,n)}$.

Lemma (Childs, 2020)

Assume h is prime. For all n we have

$$Z(G_n) = \begin{cases} \langle t^{k/gcd(k,n)} \rangle & k \nmid n \\ G & k \mid n \end{cases}.$$

So, $G_m \cong G_n$ if and only if $\gcd(k, n) = \gcd(k, m)$.

$G_n = \langle s, t : s^h = t^k = tst^{-1}s^{-b^n} = 1_G \rangle$

Let $G = G_1$.
Pick $j \in \mathbb{Z}$, and define $\psi : G \to G$ by $\psi(s) = 1_G,\ \psi(t) = t^{1-j}$.
Then $\psi \in \mathrm{Ab}(G)$.
We have, since $\psi_n = -(1-\psi)^n + 1$,

$$\begin{aligned} (1-\psi)(s) &= s \qquad & \psi_n(s) &= (-(1-\psi)^n(s))\, s = s^{-1}s = 1_G \\ (1-\psi)(t) &= t^j \qquad & \psi_n(t) &= (-(1-\psi)^n(t))\, t = t^{-j^n}t = t^{1-j^n} \end{aligned}$$

Hence,

$$\begin{aligned} s \circ_n g &= ss^{-1}gs = gs \\ t \circ_n t &= tt^{j-1}tt^{1-j} = t^2 \\ t \circ_n s &= tt^{j-1}st^{1-j} = s^{b^{j^n}}t = s^{b^{j^n}} \circ_n t, \end{aligned}$$

and so $(G, \circ_n) = G_{j^n} = G_{\gcd(j^n,k)}$.

Some examples. $\psi(s) = 1_G$, $\psi(t) = t^{1-j}$, $(G, \circ_n) = G_{j^n}$

- $j = 1$. Then ψ is trivial, and all braces are identical (and trivial). We get two HGS: the classical and the canonical nonclassical.
- $h = 13, k = 4, b = 4$. If $j = 2$ then the "sequence" of groups is

$$\begin{array}{ccccccccc} (G, \circ_0) & \longrightarrow & (G, \circ_1) & \longrightarrow & (G, \circ_2) & \longrightarrow & (G, \circ_3) & \longrightarrow & \cdots \\ \| & & \| & & \| & & \| & & \\ G_1 & \longrightarrow & G_2 & \longrightarrow & G_4 & \longrightarrow & G_4 & \longrightarrow & \cdots \end{array}$$

  Since G_4 is abelian, we have $2 \cdot 6 + 3 = 15$ solutions to the YBE. We have constructed 5 HGS in the case $\mathrm{Gal}(L/K) = (G, \circ_m)$ for $0 \leq m \leq 2$: two HGS of type $(G, \circ_0)$, two of type $(G, \circ_1)$, and one of type $(G, \circ_2)$.

Some examples. $\psi(s) = 1_G$, $\psi(t) = t^{1-j}$, $(G, \circ_n) = G_{j^n}$

- $h = 13, k = 12, b = 4, j = 2$. Similar, except now G_4 is nonabelian, giving us at least $2 \cdot 9 = 18$ solutions to the YBE.
  In fact, can show that $\circ_m = \circ_n$ if and only if $m \equiv n \pmod 2$ and $m, n \geq 2$.
  So $\{(G, \circ_m, \circ_n) : 0 \leq m, n \leq 3\}$ includes a complete set of braces.
  The total number of solutions to the YBE is $2 \cdot 16 = 32$ (though between 2 and 12 equivalent since $(G, \circ_2) \cong (G, \circ_3)$).
  - For $\mathrm{Gal}(L/K) = (G, \circ_0)$ we have 2 HGS of type $(G, \circ_0)$, 2 of type $(G, \circ_1)$, and either 2 or 4 HGS of type $(G, \circ_2)$. Total: 6 or 8.
  - For $\mathrm{Gal}(L/K) = (G, \circ_1)$ we have 2 HGS of type $(G, \circ_0)$, 2 of type $(G, \circ_1)$, and either 2 or 4 HGS of type $(G, \circ_2)$. Total: 6 or 8.
  - For $\mathrm{Gal}(L/K) = (G, \circ_2)$ we have 2 or 4 HGS of type $(G, \circ_0)$, 2 or 4 of type $(G, \circ_1)$, and either 4 or 6 HGS of type $(G, \circ_2)$. Total: between 8 and 14.

Issue. Need to determine if $(G, \circ_m, \circ_2) \cong (G, \circ_m, \circ_3)$.

A special case. $\psi(s) = 1_G,\ \psi(t) = t^{1-j},\ (G, \circ_n) = G_{j^n}$

Suppose k is also prime. Then G is *the* nonabelian group of order hk.

- If $k \mid j$ then $\ker\psi = \langle s\rangle,\ \mathrm{FP}(\psi) = \langle t\rangle$ and $(G, \circ_1) \cong C_h \times C_k \cong C_{hk}$. Two distinct groups, 6 solutions to YBE, 2 HGS of type G and 1 of type C_{hk} with $\mathrm{Gal}(L/K) = G$ as well as with $\mathrm{Gal}(L/K) = C_{hk}$.
- If j is picked to be a primitive root modulo k, then by [K-Truman 2020] we get $k-1$ nonisomorphic braces, hence $2(k-1)$ solutions to the YBE, and $2(k-1)$ HGS on L/K with $\mathrm{Gal}(L/K) = G$ (all of type G).

These account for all braces (up to isomorphism) of the form $(B, \cdot, \circ)$ with $(B, \cdot) \cong G$, along with the trivial brace on C_{hk}.

Special case II. $\psi(s) = 1_G$, $\psi(t) = t^{1-j}$, $(G, \circ_n) = G_{j^n}$

Let $N \gg 0$, let h be a prime with $h \equiv 1 \pmod{2^N}$, let $k = 2^N$ and $j = 2$.

Then $(G, \circ_n) \cong G_{\gcd(2^n, 2^N)} \cong G_{2^{\min\{n,N\}}}$ and $(G, \circ_N)$ is abelian.

The brace block includes $N + 1$ pairwise nonisomorphic groups, N of which are nonabelian.

We get

- $2N(N+1)$ total solutions from $(G, \circ_m, \circ_n)$ with $m \neq N$.
- $N + 1$ solutions from $(G, \circ_N, \circ_n)$.

In total, we have $2N(N+1) + (N+1) = 2N^2 + 3N + 1$ solutions.

Any extension L/K with $\mathrm{Gal}(L/K) = (G, \circ_n)$, $0 \le n \le N$ has 2 HGS of type $(G, \circ_m)$ with $m < N$ and 1 HGS of type $(G, \circ_N)$.

Thus, the number of braces, the number of YBE solutions, and the overall number of HGS produced by our brace blocks is unbounded.

Outline

The isomorphism type of $(G, \circ_n)$.

Generally, it appears to be difficult to know this for $n > 0$.

Special cases:

- If ψ is fixed point free then $(G, \circ_n) \cong G$ for all n.
- If $|\ker \psi_n| \cdot |\mathrm{FP}(\psi_n)| = |G|$ then $(G, \circ_n) \cong \ker \psi_n \times \mathrm{FP}(\psi_n)$.

Things we do know:

- $(G, \circ_n)$ contains subgroups isomorphic to $(1 - \psi)^m(G)$ for all $m < n$.
- $(G, \circ_n)$ contains a subgroup isomorphic to $\ker \psi_n \times \mathrm{FP}(\psi_n)$.
- $(G, \circ_n)$ is abelian if and only if $(1 - \psi)^n(G) \subseteq Z(G, \cdot)$.

Hopf algebra questions

1. Is there a simple way to understand $H_n := L[(G, \circ_n)]^G$ and/or its action on L?
   We do know that if $h = \sum_{g \in G} a_g \eta_g^{(n)} \in H_n$ then
   $h \cdot x = \sum_{g \in G} a_g g^{-1}(x)$.
   So knowing the elements of H_n makes the action transparent.

2. Is there a simple way to understand $H_{m,n} := L[(G, \circ_m)]^{(G, \circ_n)}$ (after suitably redefining L)?

3. Can we determine when $H_m \cong H_n$ as K-Hopf algebras?
   Note if ψ is fixed point free then $H_n \cong H_\lambda$ for all n.
   We suspect the converse is true.

4. Can we determine when $H_m \cong H_n$ as K-algebras?

Block structural questions

We do not have examples where our construction yields:

- A group $(G, \circ_n) \cong G$ which can not come from a fixed point free map.
- A block with $(G, \circ_n) \cong (G, \circ_{n+1}) \not\cong (G, \circ_{n+2})$.
- A block with $(G, \circ_n) \not\cong (G, \circ_{n+1})$ but $(G, \circ_n) \cong (G, \circ_m)$ for some $m \geq 2$.

The latter two seem unlikely since, for example, $\ker \psi_n \leq \ker \psi_{n+1}$.

Thank you.