Abelian Maps, Braces, and Hopf-Galois Structures

Alan Koch

Agnes Scott College

Faux-maha, May 25, 2020

Outline

Recall/Notation/Conventions

Let G be a (finite) group, $N \leq \mathrm{Perm}(G)$.

- We say N is *G-stable* if it is normalized by $\lambda(G)$.
- Associated to a regular, G-stable subgroup $N \leq \mathrm{Perm}(G)$ is a (skew left) brace $(N, \cdot, \circ)$: two groups satisfying the *brace relation*

$$a \circ (b \cdot c) = (a \circ b) \cdot a^{-1} \cdot (a \circ c),\ \ a, b, c \in N, a \cdot a^{-1} = 1_N$$

  We will frequently suppress the dot.
- Regular subgroups account for all finite braces.
- Every brace $(N, \cdot, \circ)$ gives a (non-degenerate set-theoretic) solution to the Yang-Baxter equation, i.e., a map $R : N \times N \to N \times N$ such that

$$R_{12} R_{23} R_{12} = R_{23} R_{12} R_{23}$$

  where $R_{ij} : N \times N \times N \to N \times N \times N$ applies R to the i^{th} and j^{th} component.

Stordy's Senior Thesis describes a solution to the YBE based on a fixed point free abelian endomorphism ψ of G.

Specifically, given $\psi : G \to G$ the solution obtained is

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

Idea

Can this be shown without using regular subgroups and braces?
Can we verify it by direct computation?

Yes, eventually.

Theorem 0.1. *Let G be a finite group, and let $\psi \in \mathrm{FPF}(G)$. Then the map $R : G \times G \to G \times G$ given by*

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

is a non-degenerate set-theoretic solution to the Yang-Baxter equation.

I will point out that this can be done via braces, but we prefer the computational version because we loathe ourselves.

Proof. First we show that it is indeed a solution. It is useful to realize that the components of $R(g,h)$ are computed by conjugating h and g by certain elements respectively. Thus, as ψ is constant on conjugacy classes,

$$(\psi \times \psi)R(g,h) = (\psi(h), \psi(g)), \ g,h \in G.$$

Now for $g,h,k \in G$ we have

$$R_{12}R_{23}R_{12}(g,h,k) = R_{12}R_{23}(\psi(g^{-1})h\psi(g), \psi(hg^{-1})h^{-1}\psi(g)g\psi(g^{-1})h\psi(gh^{-1}), k).$$

Using the observation above allows us to reduce the above to

$$R_{12}(\psi(g^{-1})h\psi(g), \psi(g^{-1})k\psi(g), \psi(kg^{-1})k^{-1}\psi(h)h^{-1}\psi(g)g\psi(g^{-1})h\psi(h^{-1})k\psi(gk^{-1})).$$

The components of the above, after R_{12} is applied, are

$$\psi((gh)^{-1})k\psi(gh) \quad (1)$$

$$\psi((ghk^{-1})^{-1})k^{-1}\psi(h)h\psi(h^{-1})k\psi(ghk^{-1}) \quad (2)$$

$$\psi(kg^{-1})k^{-1}\psi(h)h^{-1}\psi(g)g\psi(g^{-1})h\psi(h^{-1})k\psi(gk^{-1}) \quad (3)$$

On the other hand, we have

$$R_{23}R_{12}R_{23}(g,h,k) = R_{23}R_{12}(g, \psi(h^{-1})k\psi(h), \psi(kh^{-1})k^{-1}\psi(h)h\psi(h^{-1}k\psi(hk^{-1})),$$

which then becomes

$$R_{23}(\psi((hg)^{-1})k\psi(hg), \psi((hgk^{-1})^{-1})k^{-1}\psi(hg)g\psi((hg)^{-1})k\psi(hgk^{-1}), \psi(kh^{-1})k^{-1}\psi(h)h\psi(h^{-1}k\psi(hk^{-1})),$$

Date: May 14, 2020.

and the resulting components are

(1) $\psi((hg)^{-1})k\psi(hg)$

(2) $\psi((hk^{-1}g)^{-1})k^{-1}\psi(h)h\psi(h^{-1})k\psi(hk^{-1}g)$

(3) $\psi(g^{-1}k)k^{-1}\psi(h)h^{-1}\psi(g)g\psi(g^{-1})h\psi(h^{-1})k\psi(k^{-1}g).$

Therefore, we get a solution to the Yang-Baxter equation. We next show that the solution is non-degenerate, i.e., that

$$f_g : G \to G, f_g(h) = \psi(g^{-1})h\psi(g)$$
$$f_h : G \to G, f_h(g) = \psi(hg^{-1})h^{-1}\psi(g)g\psi(g^{-1})h\psi(gh^{-1})$$

are bijections for all $g,h \in G$. That f_g is a bijection is clear since it is simply conjugation of $h \in G$ by the fixed element $\psi(g^{-1})$. Now suppose $f_h(g_1) = f_h(g_2)$. Then

$$\psi(hg_1^{-1})h^{-1}\psi(g_1)g_1\psi(g_1^{-1})h\psi(g_1h^{-1}) = \psi(hg_2^{-1})h^{-1}\psi(g_2)g_2\psi(g_2^{-1})h\psi(g_2h^{-1}),$$

which simplifies to

$$\psi(g_1^{-1})h^{-1}\psi(g_1)g_1\psi(g_1^{-1})h\psi(g_1) = \psi(g_2^{-1})h^{-1}\psi(g_2)g_2\psi(g_2^{-1})h\psi(g_2).$$

If we apply ψ to both sides we quickly see that $\psi(g_1) = \psi(g_2)$, again since ψ is constant on conjugacy classes. Thus, we have

$$\psi(g_1^{-1})h^{-1}\psi(g_1)g_1\psi(g_1^{-1})h\psi(g_1) = \psi(g_1^{-1})h^{-1}\psi(g_1)g_2\psi(g_1^{-1})h\psi(g_1),$$

giving $g_1 = g_2$.

Figure: It's a little tedious

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

The key to showing that R is a solution is the following observation:

If $\psi : G \to G$ is abelian, then for all $g, h \in G$ we have

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

This is not a surprise, but what is a surprise is:

The proof never uses that ψ is fixed point free.

Regular subgroups account for all solutions

$N \leq \mathrm{Perm}(G)$ regular, G-stable	
$\Downarrow$	surjection
Left Skew Braces	
$\Updownarrow$	bijection
Solutions to YBE	

But if you drop "fixed point free", the subgroup

$$N_\psi = \{\lambda(g)\rho(\psi(g)) : g \in G\}$$

is irregular: if $\psi(g) = g$ then $\lambda(g)\rho(\psi(g))[1_G] = 1_G$.

How are we getting solutions to the YBE which don't come from regular G-stable subgroups?

Outline

Perspective and notation change. The abelian endomorphisms will often be on a group which we denote N instead of G.

Definition

An endomorphism $\psi : N \to N$ is said to be *abelian* if $\psi(N)$ is abelian.

Equivalently, $\psi(ab) = \psi(ba)$ for all $a, b \in N$.

Proposition

Let $\psi : N \to N$ be abelian. Define a binary operation $\circ$ on N via

$$a \circ b = a\psi(a^{-1})b\psi(a), \; a, b \in N.$$

Then $(N, \cdot, \circ)$ is a brace, where $\cdot$ is the usual operation on N.

$a \circ b = a\psi(a^{-1})b\psi(a)$

We need to show $(N, \circ)$ is a group and that the brace relation holds.

Clearly $a \circ 1_N = 1_N \circ a = a$. For associative:

$$\begin{aligned}
(a \circ b) \circ c &= (a\psi(a^{-1})b\psi(a)) \circ c \\
&= (a\psi(a^{-1})b\psi(a))\psi(\psi(a^{-1})b^{-1}\psi(a)a^{-1})c\psi(a\psi(a^{-1})b\psi(a)) \\
&= (a\psi(a^{-1})b\psi(a))\psi(b^{-1}a^{-1})c\psi(ab) && (\psi \text{ abelian}) \\
&= a\psi(a^{-1})b\psi(b^{-1})c\psi(b)\psi(a) && (\psi \text{ abelian}) \\
&= a\psi(a^{-1})(b \circ c)\psi(a) \\
&= a \circ (b \circ c).
\end{aligned}$$

$a \circ b = a\psi(a^{-1})b\psi(a)$

Let $x = \psi(a)a^{-1}\psi(a^{-1})$. Claim $x = \overline{a}$.

$$\begin{aligned}
a \circ x &= a\psi(a^{-1})(\psi(a)a^{-1}\psi(a^{-1}))\psi(a) = 1_N \\
x \circ a &= (\psi(a)a^{-1}\psi(a^{-1}))\psi(\psi(a)a\psi(a^{-1}))a\psi(\psi(a)a^{-1}\psi(a^{-1})) \\
&= \psi(a)a^{-1}\psi(a^{-1})\psi(a)a\psi(a^{-1}) \qquad (\psi \text{ abelian}) \\
&= 1_N.
\end{aligned}$$

So $(N, \circ)$ is a group; and

$$\begin{aligned}
(a \circ b)a^{-1}(a \circ c) &= a\psi(a^{-1})b\psi(a)a^{-1}a\psi(a^{-1})c\psi(a) \\
&= a\psi(a^{-1})bc\psi(a) \\
&= a \circ (bc),
\end{aligned}$$

hence $(N, \cdot, \circ)$ is a brace.

In summary

Proposition

Let $\psi : N \to N$ be an abelian map.
Then $(N, \cdot, \circ)$ is a brace, where

$$a \cdot b = ab$$
$$a \circ b = a\psi(a^{-1})b\psi(a).$$

This allows for a very easy way to construct (some) braces.

Remark

If ψ is fixed point free then $(N, \circ) \cong (N, \cdot)$.
If ψ has fixed points then $(N, \circ)$ may not be isomorphic to $(N, \cdot)$.

A question of uniqueness

Question

Do different choices of abelian maps ψ give different braces?

Not necessarily.

For example, if $\psi(N) \leq Z(N)$ (center of N) then for all $a, b, \in N$:

$$a \circ b = a\psi(a^{-1})b\psi(a) = ab$$

and we get the trivial brace $(N, \cdot, \cdot)$.

Adapting Lindsay's Result I

Suppose ψ_1, ψ_2 are abelian maps on N which give the same brace. Then

$$a\psi_1(a^{-1})b\psi_1(a) = a\psi_2(a^{-1})b\psi_2(a),\ \ a, b \in N.$$

For each a, let $z_a = \psi_2(a)\psi_1(a^{-1})$. Then $\psi_2(a) = z_a\psi_1(a)$ and

$$\begin{aligned} \psi_1(a^{-1})b\psi_1(a) &= \psi_1(a^{-1})z_a^{-1}bz_a\psi_1(a) \\ b &= z_a^{-1}bz_a \end{aligned}$$

for all $b \in N$, hence $z_a \in Z(N)$ for all a.

Note that $a \mapsto z_a$ is a homomorphism since

$$\begin{aligned} z_{ab} &= \psi_2(ab)\psi_1(b^{-1}a^{-1}) = \psi_2(a)(\psi_2(b)\psi_1(b^{-1}))\psi_1(a^{-1}) \\ &= \psi_2(a)z_b\psi_1(a^{-1}) = \psi_2(a)\psi_1(a^{-1})z_b = z_az_b. \end{aligned}$$

This homomorphism is clearly abelian.

Adapting Lindsay's Result II

Conversely, let ψ_1, ψ_2 be abelian maps on N such that $\psi_2(a) = z_a\psi_1(a)$ for all $a \in N$, where $z_a \in Z(N)$.

Denoting the corresponding circle operations by $\circ_1$ and $\circ_2$,

$$\begin{aligned} a \circ_2 b = a\psi_2(a^{-1})b\psi_2(a) &= a\psi_1(a^{-1})z_a^{-1}bz_a\psi_1(a) \\ &= a\psi_1(a^{-1})b\psi_1(a) \\ &= a \circ_1 b. \end{aligned}$$

Letting $\zeta(a) = z_a$ gives:

Proposition

Two abelian maps ψ_1, ψ_2 give the same brace if and only if $\psi_2(a) = \zeta(a)\psi_1(a)$ for some homomorphism $\zeta : N \to Z(N)$.

Brace to regular subgroup?

With ψ as above, $(N, \cdot, \circ)$ is a brace.

We can realize $(N, \cdot)$ as a subgroup of $\mathrm{Perm}(N, \circ)$ via

$$a[b] = a \cdot b.$$

If $(N, \circ)$ is isomorphic to some abstract group G, say $\phi : (N, \circ) \to G$, then we can view $N \leq \mathrm{Perm}(G)$ via

$$a[g] = \phi(a \cdot \phi^{-1}(g)).$$

This construction is one pullback of the map

$$\{N \leq \mathrm{Perm}(G) \text{ Regular, } G\text{-stable}\} \Rightarrow \{(B, \cdot, \circ) : (B, \cdot) \cong N, \ (B, \circ) \cong G\}.$$

Outline

The proposition, and the problem

Proposition (The proposition)

Let ψ be an abelian map on $(N, \cdot)$, and let $(N, \circ)$ be as defined above. Suppose $\phi : (N, \circ) \to G$ is an isomorphism. Then there is a regular, G-stable subgroup $N_{\psi,\phi} = \{\eta_a : a \in N\}$ of $\mathrm{Perm}(G)$ given by

$$\eta_a[g] = \phi(a \cdot \phi^{-1}(g)).$$

Furthermore, $N_{\psi,\phi} \cong (N, \cdot)$.

Problem

The exact regular subgroup depends on the chosen isomorphism ϕ.

Turns out we get a different, but related, subgroup in general when we use a different isomorphism $(N, \circ) \to G$.

Brace equivalence

Definition

Let G be a finite group, and let N_1, N_2 be regular, G-stable subgroups of $\mathrm{Perm}(G)$. We say N_1 and N_2 are *brace equivalent* if their corresponding braces are isomorphic.
An equivalence class of regular subgroups is called a *brace class*.

It is known that the brace class containing N is

$$\{\varphi^{-1} N \varphi : \varphi \in \mathrm{Aut}(G)\}.$$

Varying ϕ

If $\phi_1, \phi_2 : (N, \circ) \to G$ are isomorphisms then their corresponding regular, G-stable subgroups N_1, N_2 are brace equivalent. (Clear.)

Conversely, if N_1, given by an abelian map ψ and a chosen isomorphism $\phi_1 : (N, \circ) \to G$, is brace equivalent to N_2, then $N_2 = \varphi^{-1} N_1 \varphi$ for some $\varphi \in \mathrm{Aut}(G)$.

For any $\eta'_a = \varphi^{-1}\eta_a\varphi \in N_2$ we have

$$\begin{aligned}
\eta'_a[g] &= \varphi^{-1}\eta_a\varphi[g] \\
&= \varphi^{-1}\eta_a[\varphi(g)] \\
&= \varphi^{-1}\phi_1(a \cdot \phi^{-1}(\varphi(g))) \\
&= (\varphi^{-1}\phi_1)(a \cdot (\varphi^{-1}\phi_1)^{-1}(g))
\end{aligned}$$

Let $\phi_2 = \varphi^{-1}\psi_1$. Then $\phi_2 : (N, \circ) \to G$ is an isomorphism and $\eta'_a = \phi_2(a \cdot \phi_2^{-1}(g))$.

In summary

Given an abelian map ψ, the set of regular subgroups obtained forms an entire brace class.

Note: K.-Truman previously established this in the case ψ is fixed point free and abelian.

Outline

Recovering Lindsay

Suppose $\psi : G \to G$ is fixed point free and abelian.
Then $\phi : (G, \circ) \to (G, \cdot)$ given by $\phi(g) = g\psi(g^{-1})$ is an isomorphism: we have

$$\begin{aligned}
\phi(g \circ h) &= \phi(g\psi(g^{-1})h\psi(g)) \\
&= \left(g\psi(g^{-1})h\psi(g)\right)\psi(\psi(g^{-1})h^{-1}\psi(g)g^{-1}) \\
&= g\psi(g^{-1})h\psi(g)\psi(h^{-1}g^{-1}) \\
&= g\psi(g^{-1})h\psi(h^{-1}) \\
&= \phi(g)\phi(h),
\end{aligned}$$

and by fixed point freeness, $\ker\phi$ is trivial.
Then $(G, \cdot)$ acts on itself via $g[h] = \phi(g \cdot \phi^{-1}(h))$, hence if $h = k\psi(k^{-1})$,

$$\begin{aligned}
g[h] = \phi(gk) = gk\psi(k^{-1}g^{-1}) &= g(k\psi(k^{-1})\psi(g^{-1}) \\
&= gh\psi(g^{-1}) = \lambda(g)\rho(\psi(g))[h].
\end{aligned}$$

A dihedral example

Let $N = D_4 = \langle r, s : r^4 = s^2 = rsrs = 1\rangle$.

Define $\psi : D_4 \to D_4$ by $\psi(r) = 1,\ \psi(s) = s$.

$\psi(D_4) = \langle s\rangle$ so ψ is abelian.

Since $\psi(r^i) = 1$ for all i, $r^i \circ a = r^i a$ for all $a \in N$. Also,

$$r^i s \circ r^j = r^i s\psi(r^i s)r^j\psi(r^i s) = r^i ssr^j s = r^{i+j}s$$
$$r^i s \circ r^j s = r^i s\psi(r^i s)r^j s\psi(r^i s) = r^i ssr^j ss = r^{i+j}.$$

In general, $r^i s^k \circ r^j s^\ell = r^{i+j}s^{k+\ell}$ and $(N, \circ) \cong C_4 \times C_2$.

Explicitly, $\phi : (N, \circ) \to C_4 \times C_2 = \langle x, y\rangle,\ \phi(r) = x,\ \phi(s) = y$ is an isomorphism.

$\phi : (N, \circ) \to C_4 \times C_2 = \langle x, y \rangle,\ \phi(r) = x,\ \phi(s) = y$

$$r^i s^k \circ r^j s^\ell = r^{i+j} s^{k+\ell}$$

Let us realize N as a subgroup of $\mathrm{Perm}(C_4 \times C_2)$ using ϕ.
Write $r^{\circ m} = \underbrace{r \circ \cdots \circ r}_{m \text{ times}}$.

$$\eta_r[x^i] = \phi(r\phi^{-1}(x^i)) = \phi(r \cdot r^i) = \phi(r^{i+1}) = \phi(r^{\circ(i+1)}) = x^{i+1}$$
$$\eta_r[x^i y] = \phi(r\phi^{-1}(x^i y)) = \phi(r \cdot r^i s) = \phi(r^{i+1} s) = \phi(r^{\circ(i+1)} \circ s) = x^{i+1} y.$$

So $\eta_r = \lambda(x)$, and

$$\eta_s[x^i] = \phi(s \cdot r^i) = \phi(r^{-i} s) = \phi(r^{\circ(-i)} \circ s) = x^{-i} y$$
$$\eta_s[x^i y] = \phi(s \cdot (r^i s)) = \phi(r^{-i}) = \phi(r^{\circ(-i)}) = x^{-i}.$$

Another dihedral example: $N = \langle r, s \rangle \cong D_4$

Define $\psi : N \to N$ by $\psi(r) = rs, \psi(s) = 1$. $\psi(N) = \langle rs \rangle$.

Note (consider cases based on parity of i):

$$r^i \circ r^i = r^i (rs)^i r^i (rs)^i = 1$$
$$r^i s \circ r^i s = r^i s (rs)^i r^i s (rs)^i = 1.$$

So every nontrivial element of $(N, \circ)$ has order 2.

$$(N, \circ) \cong C_2 \times C_2 \times C_2.$$

Further details are left to the audience.

Outline

ψ is a homomorphism

Let ψ be an abelian map on N, and define $(N, \circ)$ as above. Then, for all $a, b \in N$,

$$\begin{aligned}\psi(a) \circ \psi(b) &= \psi(a)\psi(\psi(a^{-1}))\psi(b)\psi(\psi(a)) \\ &= \psi\big(a\psi(a^{-1})b\psi(a)\big) \\ &= \psi(a \circ b)\end{aligned}$$

So ψ is an endomorphism of $(N, \circ)$. Furthermore,

$$\psi(a) \circ \psi(b) = \psi(a \circ b) = \big(a\psi(a^{-1})b\psi(a)\big) = \psi(ab) = \psi(a)\psi(b)$$

shows that:

- $\psi : (N, \cdot) \to (N, \cdot)$ is an endomorphism
- $\psi : (N, \cdot) \to (N, \circ)$ is a homomorphism
- $\psi : (N, \circ) \to (N, \cdot)$ is a homomorphism
- $\psi : (N, \circ) \to (N, \circ)$ is an endomorphism.

Consequence I

Question

Given the "symmetric interplay" created by ψ, could $(N, \cdot, \circ)$ be a bi-skew brace?

Recall Lindsay's construction (with my notation):

Definition

A triple $(B, \cdot, \circ)$ is a *bi-skew brace* if both $(B, \cdot, \circ)$ and $(B, \circ, \cdot)$ are braces.

Thus, $(B, \cdot, \circ)$ is a bi-skew brace if $(B, \cdot)$ and $(B, \circ)$ are groups and

$$a \circ (bc) = (a \circ b)a^{-1}(a \circ c)$$
$$a(b \circ c) = (ab) \circ \overline{a} \circ (ac)$$

hold for all $a, b, c \in B$.

$a(b \circ c) = (ab) \circ \overline{a} \circ (ac)$

Let's see if the second brace relation holds.

Recall $\overline{a} = \psi(a)a^{-1}\psi(a^{-1})$.

$$\begin{aligned} a(b \circ c) &= ab\psi(b^{-1})c\psi(b) \\ (ab) \circ \overline{a} \circ (ac) &= ab\psi(b^{-1}a^{-1})\psi(a)a^{-1}\psi(a^{-1})\psi(ab) \circ (ac) \\ &= ab\psi(b^{-1})a^{-1}\psi(b) \circ (ac) \\ &= \left(ab\psi(b^{-1})a^{-1}\psi(b)\right)\psi(b^{-1})ac\psi(b) \\ &= ab\psi(b^{-1})c\psi(b). \end{aligned}$$

Proposition

An abelian map $\psi : N \to N$ gives rise to a bi-skew brace.

Consequences of Consequence I

10 Minutes ago

An abelian map ψ on N gives a regular, G-stable subgroup of $\mathrm{Perm}(G)$ for some G isomorphic to $(N, \circ)$.

Interesting, but a little backward if you are trying to find Hopf-Galois structures on L/K with $\mathrm{Gal}(L/K) = G$.

Now

An abelian map ψ on G gives a regular, G-stable subgroup $N \leq \mathrm{Perm}(G)$ with $N \cong (G, \circ)$.

ψ on $G \Rightarrow$ brace $(G, \cdot, \circ) \Rightarrow$ brace $(G, \circ, \cdot)$.

$\psi : G \to G$ gives N

This can be made quite explicit, and proven directly.
Given ψ, let $N = \{\eta_g : g \in G\} \leq \mathrm{Perm}(G)$, where

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

(So $\eta_g = \lambda(g)C(\psi(g^{-1}))$, C conjugation.)
N is regular. If $\eta_g[h] = h$ then $g\psi(g^{-1})h\psi(g) = h$.
Taking ψ of both sides:

$$\psi(gh) = \psi(h)$$

so $g \in \ker\psi$, hence

$$h = g\psi(g^{-1})h\psi(g) = gh$$

whence $g = 1_G$.

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

N is G-stable. Claim ${}^k\eta_g = \eta_{kg\psi(g^{-1})k^{-1}\psi(g)}$, $k \in G$.

$$
\begin{aligned}
{}^k\eta_g[h] &= k\eta_g[k^{-1}h] = kg\psi(g^{-1})k^{-1}h\psi(g) \\
\eta_{kg\psi(g^{-1})k^{-1}\psi(g)}[h] &= \left(kg\psi(g^{-1})k^{-1}\psi(g)\right)\psi(g^{-1})h\psi(g),
\end{aligned}
$$

which are clearly equal, giving:

Theorem

Let $\psi : G \to G$ be abelian. Then

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

is a regular, G-stable subgroup of G.

Old example

Theorem

Let $\psi : G \to G$ be abelian. Then

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

is a regular, G-stable subgroup of G.

Example

Let $G = D_4 = \langle r, s \rangle, \ \psi(r) = 1, \ \psi(s) = s$.
Then

$$\lambda(r)C(\psi(r^{-1}))[g] = rg$$
$$\lambda(s)C(\psi(s^{-1})) = ssgs = gs$$

The regular subgroup is $\langle \lambda(r), \rho(s) \rangle \cong C_4 \times C_2$.

Consequence II: another brace

Also, since ψ is abelian on $(N,\cdot)$ we have

$$\psi(a\circ b)=\psi(ab)=\psi(ba)=\psi(b\circ a)$$

and ψ is abelian on $(N,\circ)$.

We can apply the construction above on the abelian map on $(N,\circ)$ and obtain a new (bi-skew) brace!

The new brace is $(N,\circ,\star)$ with

$$\begin{aligned}a\star b &= a\circ\psi(\overline{a})\circ b\circ\psi(a)\\ &\overset{\text{eventually}}{=\!=}(a\psi(a^{-1})(\psi(a^{-1})\psi(\psi(a))(b\psi(a))(\psi(a)\psi(\psi(a^{-1}))).\end{aligned}$$

Fixed point free case

Example

If $\psi : G \to G$ is fixed point free abelian, let $\phi : G \to G$ be given by $\phi(g) = g\psi(g^{-1})$.

$$\begin{aligned}\phi(g \circ h) &= \phi(g\psi(g^{-1})h\psi(g)) = (g\psi(g^{-1})h\psi(g))\psi(\psi(g^{-1})h^{-1}\psi(g)g^{-1})) \\ &= g\psi(g^{-1})h\psi(h^{-1}) = \phi(g)\phi(h) \\ \phi(g \star h) &= \phi(g) \circ \phi(h) \qquad \text{(similarly)}\end{aligned}$$

So $\phi : (G, \circ, \star) \to (G, \cdot, \circ)$ is a bijective morphism of braces.
Thus $(G, \cdot, \circ) \cong (G, \circ, \star)$ as braces, and the corresponding embedding into $\mathrm{Perm}(G)$ is the same.

A disappointing example

Return to $N = \langle r, s \rangle \cong D_4,\ \psi(r) = 1, \psi(s) = s$.

Then $(N, \circ) \cong C_4 \times C_2$, and $(N, \circ, \star)$ is a brace with

$$a \star b = a \circ \psi(\overline{a}) \circ b \circ \psi(a) = a \circ b$$

since $(N, \circ)$ is abelian.

Thus, $(N, \circ, \star)$ is the trivial brace $(N, \circ, \circ)$.

Can we do this construction again?

Sure, if you want.

Define

$$a \diamond b = a \star \psi(\tilde{a}) \star b \star \psi(a).$$

Then $(N, \star, \diamond)$ is a brace.

We can do this until we run out of LaTeX binary (and unary) operation symbols.

But if we get the trivial brace at any point, we will get the trivial brace on every subsequent construction.

This seems to happen a lot.

Brace chains

Generally, if $\psi : N \to N$ is abelian we get a *chain* of bi-skew braces

$$(N, \circ_0, \circ_1), (N, \circ_1, \circ_2), (N, \circ_2, \circ_3), \ldots$$

where $a \circ_0 b = a \cdot b = a *_N b$ and

$$a \circ_{n+1} b = a \circ_n \psi(a^{\circ_n(-1)}) b \psi(a).$$

Let us denote the chain by

$$(N, \circ_0, \circ_1, \ldots)$$

and define G_i to be the abstract group $(N, \circ_i)$ and form the corresponding *group chain* $(N = G_0, G_1, G_2, \ldots)$.

(Notation suggestions are most welcome.)

The number of distinct braces in a brace chain is necessarily finite.

Two familiar examples

Example (Fixed point free, revisited)

If $\psi : G \to G$ is fixed point free then the chain consists of only $(G, \cdot, \circ_1, \circ_2 \dots)$ with $(G, \circ_{n-1}, \circ_n) \cong (G, \cdot, \circ)$.
The corresponding group chain is

$$(G, G, G, \dots).$$

Example (Dihedral, revisited)

Let $N = D_4, \phi(r^i s^j) = s^j$ as before. We get $(N, \cdot, \circ, \circ, \dots)$ corresponding to the group chain

$$(D_4, C_4 \times C_2, C_4 \times C_2, C_4 \times C_2, \dots).$$

Even more braces

Suppose we have a brace chain $(N, \cdot, \circ, \star)$. Then $(a \star b)a^{-1}(a \star c)$ is

$$
\begin{aligned}
&a\psi(a^{-1})^2\psi^2(a)b\psi(a)^2\psi^2(a^{-1})a^{-1}\psi(a^{-1})^2\psi^2(a)c\psi(a)^2\psi^2(a^{-1})\\
&= a\psi(a^{-1})^2\psi^2(a)b\psi(a)^2\psi^2(a^{-1})\psi(a^{-1})^2\psi^2(a)c\psi(a)^2\psi^2(a^{-1})\\
&= a\psi(a^{-1})^2\psi^2(a)bc\psi(a)^2\psi^2(a^{-1})\\
&= a \star (bc)
\end{aligned}
$$

and the brace condition is satisfied for $(N, \cdot, \star)$.

More elegantly, if $\Psi : N \to N$ is given by $\Psi(a) = \psi(a^{-2})\psi^2(a^{-1})$ then Ψ is an abelian endomorphism, and $a \star b = a\Psi(a^{-1})b\Psi(a)$.

Generally, $(N, \circ_{n-2}, \circ_n)$ is also a bi-skew brace.

Outline

Predicting the group

Return to our original construction: $\psi : N \to N$ abelian gives a brace $(N, \cdot, \circ)$.

Question

Is there any way to predict the group type of $(N, \circ)$?
In particular, for which ψ is $(N, \circ) \cong (N, \cdot)$?

That ψ be fixed point free is sufficient, but not necessary.

As far as I know.

Some facts

- For all $a \in N$, $a^{\circ(n)} = (a\psi(a^{-1}))^n a^n$. Thus,

  $$|a|_\circ \leq \operatorname{lcm}(|a\psi(a^{-1})|_\cdot, |a|_\cdot).$$

  So, e.g., no group chain starting with a non-cyclic p-group will ever include a cyclic p-group.

- $K_0 := \ker \psi$ is a normal subgroup of $(N, \circ)$ (as well as $(N, \cdot)$). So, e.g., a group chain containing A_5 will contain no other groups.

- $K_1 := \{a \in N : \psi(a) = a\}$ is a subgroup of both $(N, \cdot)$ and $(N, \circ)$. Note $(K_0, \cdot, \circ)$ and $(K_1, \cdot, \circ)$ are sub-braces of $(N, \cdot, \circ)$.

Some more fact

$K_0 = \ker\psi,\ K_1 = \{a \in N : \psi(a) = a\}$.

- K_0K_1 is a subgroup of both $(N, \cdot)$ and $(N, \circ)$. In fact,

$$(k_0k_1) \circ (\ell_0\ell_1) = (k_0\ell_0)(\ell_1k_1),\ k_0, \ell_0 \in K_0,\ k_1\ell_1 \in K_1$$

  so $(K_0K_1, \circ) \cong K_0 \times K_1$.

Example

Let $\psi : D_4 \to D_4$ be given by $\psi(r) = 1, \psi(s) = s$. Then $K_0 = \langle r\rangle$ and $K_1 = \langle s\rangle$, so

$$(N, \circ) = (K_0K_1, \circ) \cong C_4 \times C_2,$$

as we have seen.

In his 2019 bi-skew brace paper, Lindsay constructs a family of bi-skew braces in the case G is a product of complementary subgroups. That is the case here if $|K_0K_1| = G$.

A deeper dive into D_4

$K_0 = \ker \psi,\ K_1 = \{a \in D_4 : \psi(a) = a\}.$

Question

What are the possible groups in a group chain starting with D_4?

- If K_1 is trivial then ψ is fixed point free abelian, so the group obtained is D_4. Assume $K_1 \neq 1_{D_4}$.
- $K_0 \lhd D_4 \Rightarrow K_0 = \langle r^2 \rangle$ or $|K_0| = 4$.
- If $K_0 = \langle r \rangle$ then $|K_0 K_1| = 8$ and $(N, \circ) \cong C_4 \times C_2$.
- If $K_0 \cong C_2 \times C_2$ then $K_1 \cong C_2$, so $(N, \circ) \cong C_2 \times C_2 \times C_2$.
- If $|K_0| = |K_1| = 2$ then $(N, \circ)$ has a subgroup isomorphic to $C_2 \times C_2$.

A group chain starting with D_4 can only contain D_4 and at most one of $C_4 \times C_2$, $C_2 \times C_2 \times C_2$.

In particular, it is impossible to get C_8 or Q_8.

Another example

Question

What are the possible groups in a group chain starting with $S_n, n \geq 5$?

- $K_0 = S_n$ (giving the trivial brace) or $K_0 = A_n$.
- Assuming $K_0 = A_n$:
  - If K_1 is trivial, then we have a fixed point free map and $(S_n, \circ) \cong S_n$.
  - If K_1 is not trivial, $K_1 \cong C_2$ and $(S_n, \circ) \cong A_n \times C_2$.

An example of the latter situation is

$$\psi(\sigma) = \begin{cases} 1 & \sigma \in A_n \\ (12) & \sigma \notin A_n \end{cases}.$$

Chain, or tree?

Question

If $(N, \circ_0, \circ_1, \ldots, \circ_n)$ is a chain, is $(N, \circ_m, \circ_n)$ a brace for all $m < n$?

Clearly, it suffices to show that $(N, \cdot, \circ_n)$ is a brace.

We do know $(N, \circ_m, \circ_{2^i+m})$ is a brace for all $i \in \mathbb{Z}^{\geq 0}$. (Follows from $(N, \cdot, \star)$ being a brace.)

What about opposites?

Recall that any brace has an opposite brace.

Here, one formulation of the opposite is $(N, \cdot, \circ')$ with

$$a \circ' b = \psi(a) b \psi(a^{-1}) a.$$

So we really get two braces, hence two chains.

Question

Are brace chains compatible with opposites?

Isomorphism problems

Recall that if L/K is Galois, group G, and $\psi : G \to G$ is fixed point free abelian then $H = L[N]^G$ is isomorphic as a K-Hopf algebra to H_λ, the Hopf algebra which gives the canonical nonclassical Hopf-Galois structure on L/K.

This obviously doesn't extend to $\psi : N \to N$ abelian if $N \not\cong G$.

However, we can ask:

Question

Are the Hopf algebras corresponding to two different regular, G-stable subgroups of $\mathrm{Perm}(G)$, $G \cong (N, \circ)$ isomorphic as Hopf algebras?

How does it end?

Question

If $(N, \circ_0, \circ_1, \dots)$ is a chain, does it stabilize, cycle, eventually cycle or none of these?

Stabilize: $(N, \circ_{n-1}, \circ_n) = (N, \circ_n, \circ_{n+1})$ for sufficiently large n.

Cycle: There exists a $k > 0$ such that $(N, \circ_{n-1} . \circ_n) = (N, \circ_{n-1+k}, \circ_{n+k})$ for all n.

Cycle eventually: There exists a $k > 0$ such that $(N, \circ_{n-1} . \circ_n) = (N, \circ_{n-1+k}, \circ_{n+k})$ for all n sufficiently large.

None of these: None of those.

All of our examples have stabilized.

"Cycle (eventually)" seems very unlikely (excluding $k = 1$).

"None of these" seems impossible given the finite number of braces of any given order.

Interesting examples are needed

To date, I have no example of:

1. a brace chain $(N, \cdot, \circ, \star)$ with $(N, \star) \ncong (N, \circ)$.
2. a brace $(N, \cdot, \circ)$ with $(N, \circ) \cong (N, \cdot)$ which could not have come from a fixed point free abelian map.

Thank you.