Existence theorems for Hopf Galois structures and skew braces

Lindsay N. Childs

Realizability

Existence questions:

1. Given L/K Galois with group Γ, for which G with $|G| = |\Gamma|$ is there a Hopf Galois structure on L/K of type G?
2. Given an "additive" group $G = (G, \star)$, for which Γ with $|\Gamma| = |G|$ is there a skew brace structure on G so that the adjoint group $G^\circ \cong \Gamma$?

A neutral version of these questions:
Let Γ, G be two groups of the same order. Call (Γ, G) realizable if there is a Γ-Galois extension with a Hopf Galois structure of type G, or equivalently, there is a skew brace $B = (B, \circ, \star)$ with adjoint group $B^\circ \cong \Gamma$ and additive group $B^\star \cong G$.
The equivalence follows from the correspondence between Hopf Galois structures on Galois extensions of fields and skew braces.

Viewpoints

Historically, the realizability question has been looked at in different ways by Hopf Galois theorists and brace theorists.
Hopf Galois theorists have typically started with the Galois group and asked about types.
Brace theorists have typically started with the additive group (which until 2016 was always abelian) and asked about possibilities for the adjoint group.
In this talk we'll try to be unbiased and just ask about realizability of (Γ, G).
This is mostly a "history of math" talk...

The earliest non-trivial realizability results were in Nigel's uniqueness paper [By96] and Tim Kohl's:

Theorem (Ko98)

Let $\Gamma \cong C_{p^n}$ be cyclic of order p^n for p odd, then (Γ, G) is realizable only for $G \cong \Gamma$.

The proof reduces to showing that if G is a non-cyclic group of order p^n, then $\mathrm{Hol}(G)$ has no element of order p^n, which implies that there is no regular embedding of Γ into $\mathrm{Hol}(G)$.
Commentaries or new proofs of Kohl's result may be found in [By07] and Tsang [19].

p-groups, p odd, cyclic case, ctd.

Soon after inventing braces, W. Rump considered the reverse problem to Kohl's. [Ru07] studied braces $(B, \circ, +)$ where $G^+ \cong C_{p^n}$ ("cyclic braces") and determined the groups Γ for which (Γ, G) is realizable. His question was: given a brace B with additive group C_{p^n}, what could the adjoint group B° be? For HGS theorists: for which Galois groups Γ of order p^n could L/K have a Hopf Galois structure of cyclic type?

Theorem

For p odd, if B is a brace of order p^n and $G = B^+$ is cyclic of order p^n, then the adjoint group $\Gamma = B^\circ$ is also cyclic.

Crepo-Salguero

Rump's result was independently proved by Crespo and Salguero in the Hopf Galois setting [CS19]. Their result specializes to: if L/K is Γ-Galois and has a Hopf Galois extension of type G, cyclic of odd prime power degree, then $\Gamma \cong G$.

Non-cyclic abelian p-group case

Let G be a finite abelian p-group. [FCC12]:

Theorem

Let L/K be a Galois extension with abelian Galois group Γ of order p^n. Suppose L/K has an H-Hopf Galois structure of type G, an abelian group of order p^n and p-rank m where $m+1<p$. Then $\Gamma \cong G$.

Since the p-rank m of an abelian p-group is at most n, this implies that if Γ is an abelian group of order p^n with $n+1<p$, and G is an abelian group, then (Γ, G) is realizable if and only if $G \cong \Gamma$.

Commutative radical rings

Extending [CDVS06], Caranti observed that if G is an abelian p-group of order p^n and N is any abelian regular subgroup of $\mathrm{Hol}(G) \subset \mathrm{Perm}(G)$, then G becomes a commutative radical ring B with multiplication $\cdot$, so that N is isomorphic to the adjoint group $G^\circ = (G, \circ)$ of B (where $g \circ h = g + h + g \cdot h$ for g, h in B).

The main theorem of [FCC12] then says that if $G = G^+$ has p-rank m and $m + 1 < p$, then for every element g of G, the order of g in G^+ is equal to the order of g in G°. This implies that $N \cong G^\circ \cong G^+$.

Bachiller

Since every radical algebra defines a left brace, it was natural (in retrospect) to try to extend this result to the left brace setting, where $(G, \circ, +)$ is a left brace with p^n elements. This was done by Bachiller [Bac16] with a proof very similar to [FCC12]:

Theorem

Let $G = G^+$ be an abelian p-group of p-rank m, and $(G, \circ, +)$ be a left brace with additive group G^+. If $m + 1 < p$, then for every element g of G^+, the order of g in G^+ is equal to the order of g in G°. Hence if G° is abelian, then $G^\circ \cong G^+$.

Examples

Bachiller's theorem is illustrated in his work on the classification of braces of order p^3, p odd [Bac14].

There are five groups of order p^3: three abelian, namely C_p^3, $C_p \times C_{p^2}$ and C_{p^3} of exponents p, p^2 and p^3, resp., and two non-abelian groups, the Heisenberg group H_3 of exponent p and the group $M_3(p)$ of exponent p^2.

He showed that a brace with additive group of exponent p, resp. p^2, resp. p^3 must have a circle group with the same exponent, except when $p = 3$.

There exists one brace with additive group $C_3 \times C_9$ and circle group C_3^3, and one with additive group C_p^3 and circle group $C_3 \times C_9$.

[FCC12] and [Ch07], and, of course, these last examples from [Bac14], show that the condition $m + 1 < p$ is sharp.

The elementary abelian case

Bachiller's theorem when B^+ is elementary abelian implies that to classify braces of order p^m with additive group isomorphic to $\mathbb{F}_p^m$, it suffices to look at adjoint groups of order p^m and exponent p. But there turn out to be many possibilities.

For example, Vaughn-Lee showed that for $p \geq 11$ and $m = 8$, the number of groups of order p^8 and exponent p is

$$p^4 + 2p^3 + 20p^2 + 147p + (3p+29)\mathrm{gcd}(p-1), 3) + 5\mathrm{gcd}(p-1, 4) + 1246.$$

On the realizability of (Γ, C_p^n)

One might ask: Given any group Γ of order p^m and exponent p with $m + 1 < p$, is there a brace with additive group C_p^m and circle group $\cong \Gamma$?

It's true for $m = 3 < p$ by Bachiller's classification [By14]. But [Ba16] showed that the converse is false. He found a group of order p^{10} and exponent p which is not the adjoint group of a brace with additive group $\mathbb{F}_p^{10}$.
/
Vendramin asks
Problem 31: What is the minimum cardinality of a solvable group which is not the adjoint group of a left brace?

2-groups–Byott

The case $p = 2$ is different, as [By07] showed.

Let $\Gamma = C_{2^n}$. For $n = 1$ (Γ, G) is realizable only for $G = C_2$, of course; But for $n = 2$, (C_{2^n}, G) is realizable for G cyclic or $= C_2 \times C_2$, and for $n > 2$, G can be C_{2^n}, the cyclic group of order 2^n, or D_{2^n}, the dihedral group of order 2^n, or Q_{2^n}, the quaternion group of order 2^n (and there are equal numbers of Hopf Galois structures of each type).

2-groups–Rump

From the brace point of view, Rump [Ru07] proved that for $G = C_{2^n}$, $(\Gamma, G) = (\Gamma, C_{2^n})$ is realizable if and only if Γ is a group of order 2^n with a cyclic subgroup of index 2.
Thus for $n = 3$, Γ has one of the following types:
$C_{2^n}, C_2 \times C_2^{n-1}, D_{2^n}($ dihedral $), Q_{2^n}($ quaternion $)$. For $n \geq 4$ two types of semidirect products $\Gamma = C_{2^{n-1}} \rtimes C_2$ can also occur, where

$$\Gamma = \langle x, y | x^{2^n - 1} = b^2 = 1, bab^{-1} = a^{-1+2^{m-2}} \rangle$$

or

$$\Gamma = \langle x, y | x^{2^n - 1} = b^2 = 1, bab^{-1} = a^{1+2^{m-2}} \rangle.$$

For each of these groups Γ (and no others), (Γ, C^{2^n}) is realizable.

Nilpotent additive groups

As shown by Smoktunowicz and Vendramin [SV17],

Theorem

Suppose B is a skew brace of order n with a nilpotent additive group $B^\star$. Then $B = \prod_{p|n} B_p$ where $(B_p)^\star$ is the p-Sylow subgroup of $B^\star$, and each B_p is a skew brace, as is the product $\prod_{p\in J} B_p$ for any set J of distinct primes dividing n.

A special case of this result was obtained by Byott [By12] in the setting of commutative radical algebras.

If B^+ is nilpotent ...

One consequence is that for each prime p with $p^r \| n$ ($r > 0$), the product $\prod_{q \neq p} B_q^\circ$ is a subgroup of B of order $p' = n/p^r$. Thus it follows by a theorem of Hall that

Theorem

If B is a skew brace with $B^\star$ nilpotent, then B° is solvable.

This was first proved by Byott [By15].
The Smoktunowicz-Vendramin result (or Byott's special case) also implies the Etingof, Schedler and Soloviev [ESS99] theorem that the adjoint group of a brace is solvable.

If G is cyclic...

For $B^\star$ cyclic, results of Rump (2009) on cyclic braces of prime power order yield

Theorem

([Ru19]) Let B be a brace with $G = B^+$ cyclic of order n. Then $\Gamma = B^\circ$ is solvable, 2-nilpotent and almost Sylow-cyclic.

Here Γ is 2-nilpotent if the 2-Sylow subgroup of Γ is a direct summand of Γ, and Γ is almost Sylow-cyclic if the p-Sylow subgroups of Γ are cyclic for p odd, and the 2-Sylow subgroup is either trivial or has a cyclic subgroup of index 2.

For $n = 80$

Rump [Ru19] shows that for Γ a group of order 80, the 2-Sylow subgroup of Γ could be $C_{16}, C_8 \times C_2, D_8, Q_4$, or

$$M_8 = \langle a, b | a^8 = b^2 = 1, bab^{-1} = a^5 \rangle$$

or

$$SD_8 = \langle a, b | a^8 = b^2 = 1, bab^{-1} = a^3 \rangle.$$

Rump shows that 23 of the 52 groups of order 80 can be Galois groups of Galois extensions with a Hopf Galois structure of cyclic type.

Γ nilpotent

If Γ is nilpotent, the question of what G looks like was posed by Vendramin [Ve18]:
Problem 47: If Γ is nilpotent and (Γ, G) is realizable, must G be solvable?

But Tsang [TQ20] proved

Theorem

Given groups Γ, G of the same order, suppose (Γ, G) is realizable.
1) If Γ is abelian, then G is metabelian.
2) If Γ is nilpotent, then G is solvable.

Tsang's proof for Γ nilpotent

Theorem

If (Γ, G) is realizable and Γ is nilpotent, then G is solvable.

The idea of the proof is to use that if Γ is nilpotent, then so is any homomorphic image. So let $\beta : \Gamma \to \mathrm{Hol}(G) = \lambda(G)\mathrm{Aut}(G)$ be a regular embedding. One observes that $\lambda(G)$ is a subgroup of $\beta(\Gamma)\pi(\beta(\Gamma)) \subset \mathrm{Hol}(G)$ where π is the canonical map from $\mathrm{Hol}(G)$ to $\mathrm{Aut}(G)$.

Since Γ is nilpotent, so is $\pi(\beta(\Gamma))$, and the product of nilpotent groups is known to be solvable. Hence $\lambda(G)$ is a subgroup of a solvable group. Tsang's proof that Γ is abelian implies that G is metabelian follows the same outline.

In [By15], Byott wrote: ”We do not have any examples where an extension with insoluble Galois group Γ admits a Hopf-Galois structure of soluble type”
This is now referred to as
Byott’s conjecture: (Γ, G) is not realizable for Γ insolvable and G solvable.
Tsang and Qin [TQ20] presents extensive numerical evidence in support of Byott’s conjecture.

The opposite to Byott's conjecture

One might ask the opposite: Could (Γ, G) be realizable for Γ solvable and G insolvable.

The answer is yes: Byott showed that $(A_4 \times C_5, A_5)$ is realizable, using the method of fixed point free pairs of homomorphisms.

When Γ must be isomorphic to G

For which Γ is (Γ, G) realizable only for $G \cong \Gamma$? We mentioned [Ko98] earlier for $\Gamma = C_{p^n}$, p odd.
The next big result was in [By04]. If Γ is simple and (Γ, G) is realizable, then $G \cong \Gamma$.

• [BC12],section 6, contains examples of cyclic groups Γ of odd order $n = p^3 q$ (e. g. $(p, q) = (7, 19)$ or (11, 7)) such that every Hopf Galois structure on a Galois extension with Galois group Γ has only Hopf Galois structures of type Γ.

• Tsang [Ts19] showed that if $\Gamma = 2A_n$ is the double cover of the alternating group A_n, then for $n \geq 5$, (Γ, G) is realizable only for $G = \Gamma$.
Other non-trivial examples are scarce?
How about the opposite extreme?

Cases where given Γ, G can be anything

Non-trivial examples include
• Γ has order pq where p, q are primes and $p \equiv 1 \pmod q$ [By04a]
• $\Gamma = \mathrm{Hol}(C_p)$ where p is a safeprime, so $|\Gamma| = n = 2pq$ with q prime [Ch04].
• Γ is any cyclic group of square-free order [AB18]. Every group G of square-free order n is a semidirect product. So for $\Gamma = C_n$, a Hopf Galois structure of type G can be constructed via the method of fixed point free pairs of homomorphisms.
There are likely to be other examples in the square-free case that we'll hear about in the next talk.

Kohl's non-existence result

Now for something of an entirely different character:
A theorem of Kohl (2018):

Theorem

Kohl (2018): If for some m, G has more characteristic subgroups of order m than Γ has subgroups of order m, then (Γ, G) is not realizable.

The proof uses the Galois correspondence for Hopf Galois extensions and the FTGT for classical Galois extensions: a most unbraceful argument!

If Γ satisfies property A, then G ...?

Nasybulloh (2018) proved:

Theorem

If Γ is abelian and (Γ, G) is realizable, then G is metabelian.

Byott (2015) gave two proofs that if Γ is abelian and (Γ, G) is realizable, then G is solvable. His second proof shows that G is a subgroup of a metabelian group, hence a subgroup of a solvable group, hence solvable. But it is known that a subgroup of a metabelian group is metabelian.

What about the opposite: if G is abelian and (Γ, G) is realizable, is Γ metabelian? The answer is ”no”, as we'll see soon.

Let A be a finite radical (hence nilpotent) ring with $A^n = 0, A^{n-1} \neq 0$.
Then $(A, \circ, +)$ is a brace, so (A°, A^+) is realizable.
Now A° is a nilpotent group of class at most $n - 1$, because for each k, A^k is a normal subgroup of A° and

$$A \supset A^2 \supset \ldots \supset A^{n-1} \supset A^n = 0$$

is a central series of A°. In particular

Theorem

If A is a radical ring with $A^3 = 0$ then (A°, A^+) is realizable and A° is metabelian.

A converse

Ault and Watters [AW73] prove that if Γ is a finite nilpotent group of class 2, i. e. metabelian, then there exists a radical algebra A with $A^3 = 0$ and adjoint group $A^\circ \cong \Gamma$. So setting $G = A^+$, we have

Theorem

If Γ is any finite metabelian group, then there is an abelian group G so that (Γ, G) is realizable.

Kruse's example

On the other hand,
Kruse [Kr70]: There is a radical algebra A with p^{2n} elements so that A° is not metabelian.
Let G be the additive group of a radical algebra A on two generators over $\mathbb{Z}/p^n\mathbb{Z}$ with p^{2n} elements, generated as an algebra by a, b with $a^2 = ab = pa, b^2 = ba = pb$ and $p^n a = p^n b = 0$. Then the adjoint group A° has a shortest upper central series

$$G = A \supset pA \supset \ldots \supset p^{n-1}A \supset p^n A = 1$$

where $c = n$ is the class of the group A°.) A metabelian group has $c = 2$. So if $n \geq 3$ then A° is not metabelian.
(But A° is clearly solvable.)

Γ and G can be a lot different

As earlier noted, Γ can be solvable and G simple: $(A_4 \times C_5, A_5)$ is realizable. This is an example of applying the method of fixed point free pairs to Zappa-Szép products that are not semidirect products.
Let $G = HJ$ be a Zappa-Szép product, let $\Gamma = H \times J$. Then the two homomorphisms $f_H, f_J : \Gamma \to G$ by $f_H(h, j) = h, f_J(h, j) = j$ form a fixed point free pair, hence any Γ-Galois extension has a Hopf Galois structure of type G.
Another example (Byott) is $(S_{n-1} \times Z_n, S_n)$–the two groups have different composition series.
While on $\Gamma = S_n$ ...

$\Gamma = S_n$ or A_n

Extending work of [CaC99] is some recent work of Crespo, Rio and Vela [CRV19] and Tsang [Ts20] on realizability of (S_n, G) for various groups G.
[CaC99] showed that for $n = 5$ or ≥ 7, (S_n, G) is realizable for $G = S_n$ or $A_n \times C_2$.

Tsang [Ts20] proved:

Theorem

For $n = 5$ or $n \geq 7$, (S_n, G) is realizable only for $G = S_n$ and $A_n \times C_2$.

The case $n = 5$ had previously been done in [CRV18].

$\Gamma = S_6, S_4, A_4$

For $n = 6$, [CaC99] and [Ts20] together yield

Theorem

(S_6, G) is realizable for $G = S_6, A_6 \times C_2$ and M_{10} and not realizable for any other group.

M_{10} is the Mathieu group of degree 10. It has a subgroup of index 2 isomorphic to A_6. So this result supports Byott's conjecture that if Γ is not solvable and (Γ, G) is realizable, then G is not solvable.
Crespo, Rio and Vela [CRV18] also looks at the case $n = 4$:

Theorem

(A_4, G) is realizable only for $G = A_4$ and $C_3 \times V_4$; (S_4, G) is realizable only for $G = S_4$ and the direct products $A_4 \times C_2, S_3 \times V_4$ and $C_6 \times V_4$.

If (Γ, G) is realizable then (G, Γ) is also?

The answer is often no. For example, as Kohl [13] showed, for $n = 2pq$ where $p = 2q + 1$ and p, q are primes, then (Γ, G) is not realizable in the four (of 36) cases where Γ is D_{pq} or $D_q \times C_p$ and $G = C_p \rtimes C_{p-1}$ or $(C_p \rtimes C_q) \times C_2$.
Also, for $p = 2$, there are cases where Γ is cyclic of order 2^n and G is not cyclic, where (Γ, G) is realizable but (G, Γ) is not, as can be seen by comparing Byott's results in the former case with Rump's in the latter case.

Bi-skew braces

But in some cases the answer is yes: when a realizable pair (Γ, G) yields a biskew brace. I talked about this last year.

A biskew brace is a set B with two group operations $\circ$ and $*$ so that B is a skew brace with either group acting as the additive group. Then both (B°, B^*) and (B^*, B°) are realizable.

There are at least two non-trivial general settings for bi-skew braces:

semi-direct products

One is where G is the semidirect product of two groups, $G = H \rtimes J$, and $\Gamma = H \times J$.

It is known from [CRV16] that if Γ is a semidirect product of two groups H and J, then $(\Gamma, G) = (H \rtimes J, H \times J)$ is realizable. The Hopf Galois structure so constructed is called induced.

By the method of fixed point free pairs of homomomorphisms, $(H \times J, H \rtimes J)$ is realizable, and the corresponding skew brace B with $B^\circ = H \times J$ and $B^* = H \rtimes J$ is a biskew brace. Thus the pair $(H \rtimes J, H \times J)$ is also realizable, recovering the result of [CRV16]. An example: if n is squarefree, then for every group Γ of order n, (Γ, C_n) is realizable.

Radical algebras A with $A^3 = 0$

Another setting for biskew braces is where G is the additive group A^+ of a radical algebra A. In general, the pair (A°, A^+) is realizable. But if also $A^3 = 0$, then $(A, \circ, +)$ is a biskew brace, so (A^+, A°) is also realizable.

Thus, since every metabelian group Γ is the adjoint group of a radical algebra A with $A^3 = 0$, we have

Theorem

If Γ is a metabelian group, then there is an abelian group G so that both (Γ, G) and (G, Γ) are realizable.

A final example

There are many examples. One I'll mention is the non-commutative $\mathbb{F}_p$-algebra A of dimension 6 over $\mathbb{F}_p$, p odd, generated by x, y, z, a, b, c with $xy = a$, $yz = b$, $zx = c$ and all other products of basis elements $= 0$. So $A^3 = 0$. Then with A° defined by the operation $u \circ v = u + v + uv$, A° is metabelian but not a semidirect product, and both (C_p^6, A°) and (A°, C_p^6) are realizable.

On bi-skew braces

As we saw yesterday (or will today) A. Caranti, T. Kohl and A. Koch have obtained examples of bi-skew braces, some related to multiple holomorphs, that go beyond the examples just described.

Summary

This is far from a complete survey–I'm sure I've missed realizability results, especially in the brace theory literature.

It has also been abundantly clear since Byott's simple groups paper (2004) that the problem of realizability of pairs of groups (Γ, G) can involve deep results in finite group theory.
So I'm confident that we are very far from the last word on the subject!

Thank you!