Hopf Galois structures, regular subgroups of the holomorph, and skew braces: two *(brief)* stories

Elena Campedel[1], Andrea Caranti[2],
Francesca Dalla Volta[1], Ilaria Del Corso[3]

Omaha / Trento, 25 May 2020, 8:00 CDT / 15:00 CEST

[1]Università degli Studi di Milano Bicocca
[2]Università degli Studi di Trento
[3]Università degli Studi di Pisa
Italy

The holomorph, and its regular subgroups

The holomorph

$$\mathrm{Hol}(G) = N_{S(G)}(\rho(G))$$

The (permutational) holomorph of a group G is the normaliser, inside the group $S(G)$ of permutations on the set G, of the image $\rho(G)$ of the right regular representation (as per Cayley's Theorem)

$$\rho : \; G \to S(G), \qquad g \mapsto (x \mapsto xg).$$

$\rho(G)$ is a regular subgroup of $\mathrm{Hol}(G)$ (transitive & trivial stabilisers), but there may be well (plenty of) other regular subgroups, most notably the image of the left regular representation $\lambda : g \mapsto (x \mapsto gx)$.

The stabiliser of 1 in $\mathrm{Hol}(G)$ is $\mathrm{Aut}(G)$, so that

$$\mathrm{Hol}(G) = \mathrm{Aut}(G)\rho(G) \cong \mathrm{Aut}(G) \ltimes G,$$

the last group being the (abstract) holomorph.

Regular subgroups and Hopf-Galois structures

- Regular subgroups of the holomorph parametrise Hopf-Galois structures:

Cornelius Greither and Bodo Pareigis
Hopf Galois theory for separable field extensions
J. Algebra **106** (1987), 239–258

N. P. Byott
Uniqueness of Hopf Galois structure for separable field extensions
Comm. Algebra **24** (1996), 3217–3228

Rephrasing in terms of a single function

If N is a regular subgroup of $\mathrm{Hol}(G) = \mathrm{Aut}(G)\rho(G) \le S(G)$, then

$$N \to G$$
$$n \mapsto 1^n$$

is a bijection. Let $\nu : G \to N$ be its inverse, that is, the map that takes $g \in G$ to the unique $\nu(g) \in N$ such that

$$1^{\nu(g)} = g.$$

Then

$$\mathrm{Aut}(G)\rho(G) = \mathrm{Hol}(G) \ni \nu(g) = \gamma(g)\rho(g),$$

for a suitable function $\gamma : G \to \mathrm{Aut}(G)$.

We study the regular subgroups N of $\mathrm{Hol}(G)$ via this function γ, which is characterised by the functional equation

$$\gamma(x^{\gamma(y)}y) = \gamma(x)\gamma(y), \qquad \text{for } x, y \in G.$$

Regular subgroups and (right) skew braces

Let $G = (G, \cdot)$ be a group. Define a correspondence between

- maps $\gamma : G \to G^G$, (G^G is the set of maps from G to G), and
- binary operations $\circ$ on G,

$$\text{via} \quad x \circ y = x^{\gamma(y)} \cdot y, \quad \text{and} \quad x^{\gamma(y)} = (x \circ y) \cdot y^{-1}.$$

Certain properties of $\circ$ correspond to properties of γ.

$\circ$ is associative	$\gamma(x^{\gamma(y)} \cdot y) = \gamma(x)\gamma(y)$
$\circ$ admits inverses	$\gamma(g)$ is bijective
$(x \cdot y) \circ g = (x \circ g) \cdot g^{-1} \cdot (y \circ g)$	$\gamma(g) \in \mathrm{End}(G)$

Therefore it is equivalent to deal with

- (right) skew braces $(G, \cdot, \circ)$, and
- maps $\gamma : G \to \mathrm{Aut}(G)$ such that $\gamma(x^{\gamma(y)} \cdot y) = \gamma(x)\gamma(y)$.
- regular subgroups $N \leq \mathrm{Hol}(G)$.

Note $\nu(g) = \gamma(g)\rho(g)$ yields an isomorphism $\nu : (G, \circ) \to N$.

Groups having the same holomorphs

A group that parametrizes regular subgroups

Kohl has revived the study of the group

$$\begin{aligned} T(G) &= N_{S(G)}(\mathrm{Hol}(G)) / \mathrm{Hol}(G) \\ &= N_{S(G)}(N_{S(G)}(\rho(G))) / N_{S(G)}(\rho(G)), \end{aligned}$$

which parametrises the regular subgroups N of $\mathrm{Hol}(G)$ which

- are isomorphic to G, and
- have the same holomorph as G, that is,

$$\mathrm{Aut}(N) \ltimes N \cong N_{S(G)}(N) = N_{S(G)}(\rho(G)) = \mathrm{Hol}(G).$$

$N_{S(G)}(N_{S(G)}(\rho(G)))$ is called the multiple holomorph of G.

Spinoffs 1

W.H. Mills
Multiple holomorphs of finitely generated abelian groups
Trans. Amer. Math. Soc. **71** (1951), 379–392

Francesca Dalla Volta and A.C. have redone this using commutative, radical rings.

A.C. and F. Dalla Volta
The multiple holomorph of a finitely generated abelian group
J. Algebra **481** (2017), 327–347

The case of abelian groups leads to the following question:

> *Study the rings $(A, +, \cdot)$ such that all automorphisms of the additive group $(A, +)$ are also automorphisms of the ring $(A, +, \cdot)$.*

Spinoffs 2

A.C. and F. Dalla Volta
Groups that have the same holomorph as a finite perfect group
J. Algebra **507** (2018), 81–102

The case of finite perfect groups Q (i.e. $Q' = Q \neq \{ 1 \}$) leads to the following question about quasi-simple groups Q (i.e. $Q' = Q$, and $Q/Z(Q)$ non-abelian simple):

> *What are the finite, quasi-simple groups Q for which $\mathrm{Aut}(Q)$ does* not *induce the inversion map on $Z(Q)$?*

These groups have been classified

Russell Blyth and Francesco Fumagalli
On the holomorph of finite semisimple groups
arXiv 1912.0729, December 2019

Kohl noted that $T(G) = N_{S(G)}(\mathrm{Hol}(G))/\mathrm{Hol}(G)$ is often a 2-group. For instance, this holds if G is in the previously mentioned classes. But the structure of $T(G)$ can be more complicated:

A.C.
Multiple Holomorphs of Finite p-Groups of Class Two
J. Algebra **516** (2018), 352–372

If G is a finite p-group of class 2, with p an odd prime, $T(G)$ always contains a cyclic group of order $p - 1$. And there are examples where $T(G)$ contains large elementary abelian p-subgroups.

This has been extended to finite p-groups of class $< p$:

Cindy Tsang
On the multiple holomorph of groups of squarefree or odd prime power order
J. Algebra **544** (2020), 1–28

Classifications

Classifications

There are classifications of skew braces of low orders, like p, p^2, p^3, pq, where p and q are distinct primes.

N. P. Byott
Uniqueness of Hopf Galois structure for separable field extensions
Comm. Algebra **24** (1996), 3217–3228

N. P. Byott
Hopf-Galois structures on Galois field extensions of degree pq
J. Pure Appl. Algebra **188** (2004), 45–57

Kayvan Nejabati Zenouz
Skew braces and Hopf-Galois structures of Heisenberg type
J. Algebra **524** (2019), 187–225

Elena Campedel, Ilaria Del Corso and A.C. have begun a classification for the case p^2q, where p, q are distinct primes. We use the skew brace operation $\circ$, and the gamma functions.

Elena Campedel, A.C., Ilaria del Corso
Hopf-Galois structures on extensions of degree p^2q and skew braces of order p^2q: the cyclic Sylow p-subgroup case
J. Algebra **556** (2020) 1165–1210

Note also

Emiliano Acri, Marco Bonatto
Skew braces of size p^2q
arXiv:2004.04232, April 2020, and *arXiv:1912.11889*, May 2020

Are you sure you want to see three more statements like this?

Proposition

Let $G = C_q \rtimes_p C_{p^2}$*, with* $p \mid q-1$*. (Centre has order* p*.)*

Then in $\mathrm{Hol}(G)$ *there are:*

1. $\mathbf{2}pq$ *abelian regular subgroups, which split into* $2p$ *conjugacy classes of length* q*;*
2. $\mathbf{2}qp(p-2)+2p$ *regular subgroups isomorphic to* G*, which split into* $2p(p-2)$ *conjugacy classes of length* q*, and* $2p$ *conjugacy classes of length* 1*;*
3. $\mathbf{2}qp^2(p-1)$ *further regular subgroups isomorphic to* $G = C_q \rtimes_1 C_{p^2}$ *(centre is trivial), if* $p^2 \mid q-1$*, which split into* $2p(p-1)$ *conjugacy classes of length* qp*.*

Methods

Duality

Alan Koch and Paul J. Truman
Opposite skew left braces and applications
J. Algebra **546** (2020), 218–235

If G is a non-abelian group, then **inv** $: x \mapsto x^{-1}$ is not an automorphism of G, so that

$$\mathbf{inv} \notin \mathrm{Hol}(G) = N_{S(G)}(\rho(G)) = \mathrm{Aut}(G)\rho(G).$$

But...

$$\begin{aligned} \mathbf{inv} \in N_{S(G)}(N_{S(G)}(\rho(G))) &= N_{S(G)}(\mathrm{Hol}(G)) \\ &= N_{S(G)}(\mathrm{Aut}(G)\rho(G)), \end{aligned}$$

as

$$[\mathbf{inv}, \mathrm{Aut}(G)] = 1, \text{ and } \rho(G)^{\mathbf{inv}} = \lambda(G) \leq \mathrm{Hol}(G).$$

Duality (continued)

$$\rho(G)^{\mathbf{inv}} = \lambda(G).$$

Note that $\rho(G)$ corresponds to the gamma function $\gamma(x) \equiv 1$, while $\lambda(G)$ corresponds to the gamma function $\gamma(x) = \iota(x^{-1})$ (conjugacy by x^{-1}):

$$y^{\iota(x^{-1})\rho(x)} = xyx^{-1}x = xy = y^{\lambda(x)}.$$

In general, if $N \leq \mathrm{Hol}(G)$ is a regular subgroup corresponding to the gamma function γ, then $N^{\mathbf{inv}}$ is another regular subgroup of $\mathrm{Hol}(G)$, which corresponds to the gamma function

$$\overline{\gamma}(x) = \gamma(x^{-1})\iota(x^{-1}).$$

This explains why the number of regular subgroups was even.

⏩ Skip Apps

Applications

A result of Kohl

Larger kernels of γ appear to make life easier: we have methods that combined with duality allow us to switch to larger kernels.

This allows us also to extend a result of Kohl.

T. Kohl
Hopf-Galois structures arising from groups with unique subgroup of order p
Algebra Number Theory **10** (2016), 37–59

Theorem (Kohl)

Let $G = MP$, with $P \trianglelefteq G$ of order a prime p, such that

$$p \nmid |M|, \quad \textit{and} \quad p \nmid |\mathrm{Aut}(M)|.$$

Let N be a regular subgroup of $\mathrm{Hol}(G)$. Then there is a Sylow p-subgroup of N which is normalised by $\rho(G)$.

Sketch of proof

Theorem (Kohl)

$G = MP$, $|P| = p$ prime, $P \trianglelefteq G$, $p \nmid |M| \cdot |\mathrm{Aut}(M)|$.

N a regular subgroup of $\mathrm{Hol}(G)$, so N normalises $\rho(G)$.

Then the Sylow p-subgroup $\nu(P)$ of N is normalised by $\rho(G)$.

Recall the isomorphism $\nu : (G, \circ) \to N$, $\nu(g) = \gamma(g)\rho(g)$.

If $[P, M] = 1$, then $\nu(P) = \rho(P) \trianglelefteq \rho(G)$.

If $[P, M] \neq 1$, then $p \nmid |\mathrm{Aut}(M)|$ implies that the automorphisms of G of order p are inner, induced by conjugation by elements of P.

Thus for $P = \langle a \rangle$ one has $\gamma(a) = \iota(a^{-\sigma})$ for some $\sigma \in \mathrm{End}(P)$. It turns out that σ is an idempotent, so that we have the duality:

- either $\sigma = 1$, so that $\nu(P) = \lambda(P)$ is centralized by $\rho(G)$;
- or $\sigma = 0$, so that $\nu(P) = \rho(P) \trianglelefteq \rho(G)$.

One More Method

Plain morphisms

Lemma

Let G be a group, and $\gamma : G \to \mathrm{Aut}(G)$ a function.

Then any two of the following conditions imply the third one.

1. γ *satisfies* $\gamma(x^{\gamma(y)} \cdot y) = \gamma(x)\gamma(y)$, *for* $x, y \in G$.
2. $\gamma : G \to \mathrm{Aut}(G)$ *is a morphism of groups.*
3. $\gamma([G, \gamma(G)]) = \{ 1 \}$.

Valeriy G. Bardakov, Mikhail V. Neshchadim and Manoj K. Yadav
On λ-homomorphic skew braces
arXiv 2004.05555, April 2020

Skip to end

Also related to work of Kohl

Bi-skew braces

A bi-skew brace is a skew brace $(G, \cdot, \circ)$ such that $(G, \circ, \cdot)$ is also a skew brace.

L. N. Childs
Bi-skew braces and Hopf Galois structures.
New York J. Math. **25** (2019), 574–588.

A. Caranti
Bi-Skew Braces and Regular Subgroups of the Holomorph
arXiv:2001.01566, January 2020

Regular subgroups and gamma functions

A bi-skew brace is a skew brace $(G, \cdot, \circ)$ such that $(G, \circ, \cdot)$ is also a skew brace.

Rather naturally, bi-skew braces correspond to

1. the regular subgroups N of $S(G)$ such that

$$N \leq \mathrm{Hol}(G) = N_{S(G)}(\rho(G)), \quad \text{and} \quad \rho(G) \leq N_{S(G)}(N).$$

2. the functions $\gamma : G \to \mathrm{Aut}(G)$ that satisfy

$$\begin{cases} \gamma(x^{\gamma(y)}y) = \gamma(x)\gamma(y) \\ \gamma(x^{\gamma(y)}) = \gamma(x)^{\gamma(y)} \end{cases} \quad \text{or} \quad \begin{cases} \gamma(xy) = \gamma(y)\gamma(x) \\ \gamma(x^{\gamma(y)}) = \gamma(x)^{\gamma(y)}. \end{cases}$$

It follows that all the examples of Kohl, A.C and Dalla Volta, and Tsang yield bi-skew braces, as they satisfy $\gamma(x^{\beta}) = \gamma(x)^{\beta}$ for $\beta \in \mathrm{Aut}(G)$.

That’s All, Thanks!