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

Elena Campedel\textsuperscript{1}, Andrea Caranti\textsuperscript{2}, Francesca Dalla Volta\textsuperscript{1}, Ilaria Del Corso\textsuperscript{3}

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

\textsuperscript{1}Università degli Studi di Milano Bicocca
\textsuperscript{2}Università degli Studi di Trento
\textsuperscript{3}Università degli Studi di Pisa
Italy
The holomorph, and its regular subgroups
The holomorph

\[ \text{Hol}(G) = N_{S(G)}(\rho(G)) \]

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)

\[ \rho : \ G \rightarrow S(G), \quad g \mapsto (x \mapsto xg). \]

\( \rho(G) \) is a regular subgroup of \( \text{Hol}(G) \) (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 \( \text{Hol}(G) \) is \( \text{Aut}(G) \), so that

\[ \text{Hol}(G) = \text{Aut}(G)\rho(G) \cong \text{Aut}(G) \rtimes G, \]

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**
If $N$ is a regular subgroup of $\text{Hol}(G) = \text{Aut}(G) \vartriangleleft \mathbb{S}(G)$, then

\[
N \to G \\
\begin{array}{c}
n \\ \mapsto \end{array} 1^n
\]

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

\[
\text{Aut}(G) \vartriangleleft \mathbb{S}(G) \ni \nu(g) = \gamma(g)\rho(g),
\]

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

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

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

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

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

<table>
<thead>
<tr>
<th>$\circ$ is associative</th>
<th>$\gamma(x^{\gamma(y)} \cdot y) = \gamma(x)\gamma(y)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\circ$ admits inverses</td>
<td>$\gamma(g)$ is bijective</td>
</tr>
<tr>
<td>$(x \cdot y) \circ g = (x \circ g) \cdot g^{-1} \cdot (y \circ g)$</td>
<td>$\gamma(g) \in \text{End}(G)$</td>
</tr>
</tbody>
</table>

Therefore it is equivalent to deal with

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

Note $\nu(g) = \gamma(g)\rho(g)$ yields an isomorphism $\nu : (G, \circ) \to N$. 4/18
Groups having the same holomorphs
Kohl has revived the study of the group

\[ T(G) = NS(G)(\text{Hol}(G))/\text{Hol}(G) \]

\[ = NS(G)(NS(G)(\rho(G)))/NS(G)(\rho(G)), \]

which parametrizes the regular subgroups \( N \) of \( \text{Hol}(G) \) which

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

\[ \text{Aut}(N) \rtimes N \cong NS(G)(N) = NS(G)(\rho(G)) = \text{Hol}(G). \]

\( NS(G)(NS(G)(\rho(G))) \) is called the multiple holomorph of \( G \).
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* \((A, +, \cdot)\).
Groups that have the same holomorph as a finite perfect group


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 $Aut(Q)$ 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 $T(G) = N_{S(G)}(\text{Hol}(G))/\text{Hol}(G)$ 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**


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**

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**

- N. P. Byott
  **Hopf-Galois structures on Galois field extensions of degree $pq$**

- Kayvan Nejabati Zenouz
  **Skew braces and Hopf-Galois structures of Heisenberg type**
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 $p^2q$**

Proposition

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

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

1. $2pq$ abelian regular subgroups, which split into $2p$ conjugacy classes of length $q$;

2. $2qp(p - 2) + 2p$ regular subgroups isomorphic to $G$, which split into $2p(p - 2)$ conjugacy classes of length $q$, and $2p$ conjugacy classes of length $1$;

3. $2q p^2 (p - 1)$ 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
If $G$ is a non-abelian group, then $\text{inv} : x \mapsto x^{-1}$ is not an automorphism of $G$, so that

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

But...

$$\text{inv} \in N_{S(G)}(N_{S(G)}(\rho(G))) = N_{S(G)}(\text{Hol}(G)) = N_{S(G)}(\text{Aut}(G)\rho(G)),$$

as

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

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 \( N \leq \text{Hol}(G) \) is a regular subgroup corresponding to the gamma function \( \gamma \), then \( N^{\text{inv}} \) is another regular subgroup of \( \text{Hol}(G) \), 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.
Applications
Larger kernels of $\gamma$ 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 $P \triangleleft G$ of order a prime $p$, such that

\[ p \nmid |M|, \quad \text{and} \quad p \nmid |\text{Aut}(M)|. \]

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

Theorem (Kohl)

\[ G = MP, \ |P| = p \text{ prime}, \ P \trianglelefteq G, \ p \nmid |M| \cdot |\text{Aut}(M)|. \]

\( N \) a regular subgroup of \( \text{Hol}(G) \), 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 \( p \nmid |\text{Aut}(M)| \) 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 \( \gamma(a) = \nu(a^{-\sigma}) \) for some \( \sigma \in \text{End}(P) \). It turns out that \( \sigma \) 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
Lemma

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

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

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

Valeriy G. Bardakov, Mikhail V. Neshchadim and Manoj K. Yadav

On $\lambda$-homomorphic skew braces

arXiv 2004.05555, April 2020
Also related to work of Kohl
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.


A. Caranti

Bi-Skew Braces and Regular Subgroups of the Holomorph

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

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

2. the functions \(\gamma : G \rightarrow \text{Aut}(G)\) that satisfy

\[
\begin{align*}
\gamma(x\gamma(y)y) &= \gamma(x)\gamma(y) \\
\gamma(x\gamma(y)) &= \gamma(x)\gamma(y)
\end{align*}
\quad \text{or} \quad
\begin{align*}
\gamma(xy) &= \gamma(y)\gamma(x) \\
\gamma(x\gamma(y)) &= \gamma(x)\gamma(y).
\end{align*}
\]

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 \(\beta \in \text{Aut}(G)\).
Thanks!

That’s All, Thanks!