Hopf-Galois structures on separable extensions

Andrew Darlington

Wednesday 26th July 2023

University of Exeter

Review of Galois Theory

L, K fields over $\mathbb{Q}$ s.t. $K < L$. If L is the *splitting field* of some $p(x) \in K[x]$, we say L/K is **Galois**. Otherwise it is **non-normal**.

If L/K is Galois, we can associate the group

$$\mathrm{Gal}(L/K) := \{\sigma \in \mathrm{Aut}(L) \mid \sigma(x) = x \ \forall x \in K\}$$

and $|\mathrm{Gal}(L/K)| = [L : K]$.

Theorem (Fundamental Theorem of Galois Theory)
If L/K is Galois, then there is a bijective correspondence between

Fields $K < F < L$, and

Subgroups $H < \mathrm{Gal}(L/K)$

given by $F = L^H$.

Replacing with a Hopf algebra

L/K Galois, $G := \mathrm{Gal}(L/K)$. Define an action of $K[G]$ on L by

$$\left(\sum_{g\in G} a_g g\right) \cdot x = \sum_{g\in G} a_g g(x).$$

- L is a $K[G]$-module algebra
- The linear map

$$x \otimes h \mapsto \theta_{x\otimes h}(y) = x(h \cdot y),$$

  $x, y \in L$, $h \in K[G]$, is bijective
- $K[G]$ has the structure of a K-Hopf algebra.

This gives an example of a **Hopf-Galois Structure**.

Some facts

Fact 1: $K[G]$ may not be the only Hopf algebra to act on L in a similar way (unlike there being a unique Galois group)

Fact 2: This also makes sense for non-normal extensions (it can actually be defined for certain rings as well)

Fact 3: There is an analogous "Hopf-Galois Correspondence". It is always injective, but not always surjective.

My work focuses on studying, describing and counting Hopf-Galois structures for different field extensions.

Group theory

N group.

$$Hol(N) = N \rtimes \mathrm{Aut}(N)$$

where

$$(\eta, \alpha)(\mu, \beta) = (\eta\alpha(\mu), \alpha\beta).$$

Note: $\mathrm{Hol}(N)$ has a natural action on N given by:

$$(\eta, \alpha) \cdot \mu = \eta\alpha(\mu)$$

L/K (not necessarily Galois) extension, E Galois closure, and $G := \mathrm{Gal}(E/K)$. In 1996, Byott [Byo96] (building on [GP87]) showed that HGS on L/K correspond with **transitive** subgroups of $\mathrm{Hol}(N)$ (where N, the *type* of HGS, cycles through the groups of order $[L : K]$) isomorphic to G.

$$H = E[N]^G$$

Note link with skew braces in Galois case.

Worked example

L/K separable of degree 6. There are two groups of order 6:

$$N_1 := C_6 \cong \langle x, y \mid x^3 = y^2 = 1, xy = yx\rangle,$$
$$N_2 := C_3 \rtimes C_2 \cong S_3 \cong D_3 \cong \langle r, s \mid r^3 = s^2 = 1, sr = r^{-1}s\rangle.$$

Then

$$\mathrm{Hol}(N_1) \cong C_6 \rtimes C_2 \cong \langle x, y, \alpha\rangle;\ \alpha(x) = x^2,$$
$$\mathrm{Hol}(N_2) \cong D_3 \rtimes D_3 \cong \langle r, s, \alpha, \beta\rangle;\ \alpha(r) = r^2,\ \beta(s) = rs.$$

Trick: $r\beta$ commutes with s, so we can form a semidirect product of two abelian groups:

$$\mathrm{Hol}(N_2) \cong \langle r, r\beta\rangle \rtimes \langle s, \alpha\rangle \cong \mathbb{F}_3^2 \rtimes \langle s, \alpha\rangle$$

Worked example

Transitive subgroups of $\mathrm{Hol}(N_1)$:

$$\langle x, y\rangle \cong N_1, \qquad \langle x, y, \alpha\rangle \cong \mathrm{Hol}(N_1),$$
$$\langle x, (y, \alpha)\rangle \cong N_2.$$

Transitive subgroups of $\mathrm{Hol}(N_2)$:

$$\begin{array}{lll}
\langle r, s, \alpha, \beta\rangle \cong \mathrm{Hol}(N_2), & \langle r, s, \beta\rangle \cong & \langle r, (s, \alpha), \beta\rangle, \\
\langle r, s, \alpha\rangle \cong \mathrm{Hol}(N_1) \cong & \langle r, s, \beta\alpha\rangle \cong & \langle r, s, \beta^2\alpha\rangle \cong \\
\langle (r, \beta), s, \alpha\rangle \cong & \langle (r, \beta), rs, (r, \alpha)\rangle \cong & \langle (r, \beta), r^2 s, (r^2, \alpha)\rangle, \\
\langle r, (s, \alpha)\rangle \cong & \langle r, (s, \beta\alpha)\rangle \cong & \langle r, (s, \beta^2\alpha)\rangle \cong \\
\langle (r, \beta), s\rangle \cong & \langle (r, \beta), rs\rangle \cong & \langle (r, \beta), r^2 s\rangle \cong N_1, \\
\langle r, s\rangle \cong & \langle (r, \beta), (s, \alpha)\rangle \cong N_2. &
\end{array}$$

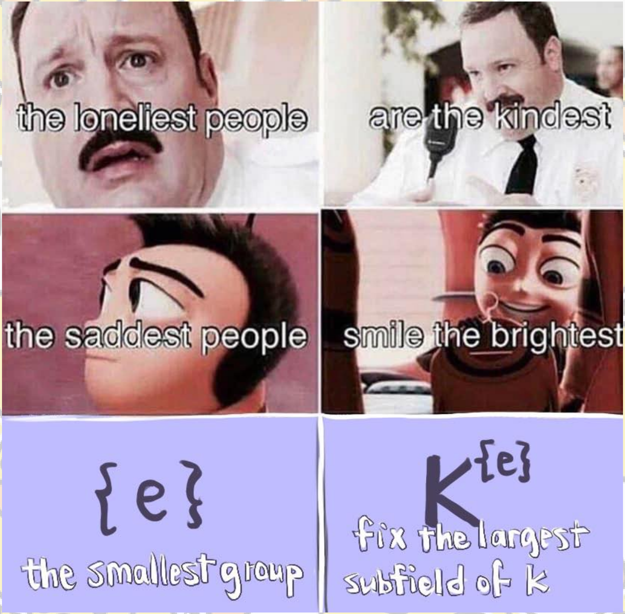
Examples in literature

- $K[G]$ is a HGS on L/K of type G.
- N is a transitive subgroup of $\mathrm{Hol}(N)$.
- $\mathrm{Hol}(N)$ is a transitive subgroup of $\mathrm{Hol}(N)$
- If $G < \mathrm{Hol}(N)$ is transitive then $G < \mathrm{Hol}(N^{\mathrm{op}})$ is transitive.
- L/K degree p^2, $2p$ [CS20], mp with $(m, p) = 1$ [Koh07] & [Koh16], squarefree Galois [AB20],...
- [Dar23] (preprint) L/K separable, degree pq.

Questions

- How far can we go using the methods of [AB20] and [Dar23]?
- Exploit connection with skew braces when Galois
- Give results for skew bracoids?
- HGS on related field extensions L/K, L'/K.

Thank You!


the loneliest people
are the kindest
the saddest people
smile the brightest
{e}
the smallest group
$K^{\{e\}}$
fix the largest subfield of K

- Ali A. Alabdali and Nigel P. Byott, *Hopf-Galois structures of squarefree degree*, J. Algebra **559** (2020), 58–86. MR 4093704
- N. P. Byott, *Uniqueness of Hopf Galois structure for separable field extensions*, Comm. Algebra **24** (1996), no. 10, 3217–3228. MR 1402555
- Teresa Crespo and Marta Salguero, *Computation of Hopf Galois structures on low degree separable extensions and classification of those for degrees p^2 and $2p$*, Publ. Mat. **64** (2020), no. 1, 121–141. MR 4047559
- Andrew Darlington, *Hopf-Galois structures on separable field extensions of degree pq*, 2023, arxiv preprint: 2303.11229.
- Cornelius Greither and Bodo Pareigis, *Hopf Galois theory for separable field extensions*, J. Algebra **106** (1987), no. 1, 239–258. MR 878476
- Timothy Kohl, *Groups of order $4p$, twisted wreath products and Hopf-Galois theory*, J. Algebra **314** (2007), no. 1, 42–74.