**Introduction**

Fix a prime $p > 3$ and let $L/K$ be a Galois field extension of degree $p^3$ with Galois group $G$.

- Our main objective is to classify (or count) the Hopf-Galois structures on the extension $L/K$.
- This is directly related to classifying, for each group $N$ of order $p^3$, all subgroups of the holomorph of $N$.

$$\text{Hol}(N) \triangleleft N \rtimes \text{Aut}(N) = \{n \in N \mid n \in N, \alpha \in \text{Aut}(N)\}$$

isomorphic to $G$ which are regular on $N$. A subgroup $H \subset \text{Hol}(N)$ is regular if the map

$$h \times n \rightarrow n \times h \text{ given by } (hn) = xy(z) \text{ for } x, z \in L, y \in H$$

is an isomorphism.

The classical Hopf-Galois structure on $L/K$ is the group ring $K[G]$, where $G$ acts on $L$ in such a way that the $K$-module homomorphism

$$f : L \otimes K \rightarrow \text{End}(L) \text{ given by } (f \otimes x)(z) = xz$$

is a bijection.

Byott classified the abelian type of order $p^3$ for all primes $p$ in [Bac15].

**Method**

Therefore, to classify the Hopf-Galois structures and braces of order $p^3$ one needs to study $\text{Aut}(N)$, classify all regular subgroups of $\text{Hol}(N)$, for each group $N$ of order $p^3$, and follow the procedures described in the previous column.

**Groups of order $p^3$**

Up to isomorphism, there are 5 different groups of order $p^3$ as follows:

- The cyclic group $C_{p^3}$ where $\text{Aut}(C_{p^3}) \cong C_p \times C_{p-1}$.
- The elementary abelian group $C_{p}^3$ where $\text{Aut}(C_{p}^3) \cong \text{GL}_2(p)$.
- Abelian, exponent $p^2$ group $C_p \times C_{p^2}$

$$1 \rightarrow C_{p^2} \rightarrow \text{Aut}(C_p \times C_{p^2}) \rightarrow \text{UP}_2(C_p) \rightarrow 1$$

- Nonabelian, exponent $p^2$ group $M_i \defeq (\sigma, \tau) \mid |\sigma^p = 1, \sigma^{p+1} = \tau = \sigma \tau| \tau \in \text{Aut}(C_{p^3}) \rightarrow \text{UP}_2(C_p) \rightarrow 1$

- Nonabelian, exponent $p$ group $M_i \defeq (\sigma, \tau) \mid |\sigma^p = 1, \sigma^{p+1} = \tau = \sigma \tau| \tau \in \text{Aut}(C_{p^3}) \rightarrow \text{UP}_2(C_p) \rightarrow 1$

Where all short sequences of groups above are exact and we denote by $\text{UP}_2(C_p) \subset \text{GL}_2(C_p)$ the set of upper triangular matrices and $\text{UP}_2(C_p)$ its subset whose elements have upper left entry 1. It can be shown that the above exact sequences are split – a fact useful when finding braces of order $p^3$.

**Regular subgroups in $\text{Hol}(N)$**

It is common in Hopf-Galois theory to organise the regular subgroups of $\text{Hol}(N)$ according to the size of their image under the projection

$$\sigma : \text{Hol}(N) \rightarrow \text{Aut}(N) \quad \eta \mapsto \alpha$$

although in brace theory they are organised by the size of their Socle which is the size of their intersection with $K\sigma$. To construct regular subgroups $H \subset \text{Hol}(N)$ with $|\psi(H)| = m$, where $m$ divides $|N|$, we take a subgroup of order $m$ of $\text{Aut}(N)$ which may be generated by $\alpha_1, \ldots, \alpha_s \in \text{Aut}(N)$, say

$$H \triangleleft \text{Hol}(N),$$

a subgroup of order $\frac{|N|}{m}$ of which may be generated by $v_1, \ldots, v_s \in N$.

Then search for all $v_i$ such that the group $H \subset \text{Hol}(N)$, i.e., $H$ has the same size as $N$ and acts freely on $N$. For $H$ to satisfy $|\psi(H)| = m$, it is necessary that for every relation $R(\alpha_1, \ldots, \alpha_s) = 1$ in $H_2$ we require

$$R(\alpha(\psi(v_1)), \ldots, \alpha(\psi(v_s)))w \in H_1$$

for all $w \in H_1$.

For $H$ to act freely on $N$ it is necessary that for every word $W(\alpha_1, \ldots, \alpha_s) \neq 1$ in $H_2$ we require

$$W(\alpha(\psi(v_1)), \ldots, \alpha(\psi(v_s)))w \psi(v_1, \ldots, v_s)^{-1} \notin H_1$$

for all $w \in H_1$.

However, in general there will be other conditions on $v_i$ which we have to consider – for example, some elements of $H$ need to satisfy relations between generators of a group of order $|N|$. We repeat this process for every $m$, every subgroup of order $m$ of $\text{Aut}(N)$, and every subgroup of order $\frac{|N|}{m}$ of $N$.

- David Bautista
  - Classification of braces of order $p^3$
- N. P. Byott
  - Uniqueness of Hopf Galois structure for separable field extensions.
- Nigel P. Byott
  - Hopf-Galois structures on Galois field extensions of degree $p^3$.
- Lindsey N. Childs
  - Taming wild extensions: Hopf algebras and local Galois module theory, volume 80 of Mathematical Surveys and Monographs.
- L. Guarnieri and L. Vendramin
  - Skew braces and the Yang–Baxter equation.
- Wolfgang Rump
  - Skew braces, radical rings, and the quantum Yang–Baxter equation.