Hopf-Galois Structures on Galois Field Extensions of Degree $p^3$ and Their Relationship to Skew Braces

Kayvan Nejabati Zenouz$^1$

University of Exeter, UK

Groups, Rings and the Yang-Baxter equation

Spa

June 23, 2017

$^1$Kn249@ex.ac.uk
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 $N$
  \[ \text{Hol}(N) = N \rtimes \text{Aut}(N) = \{ \eta \alpha \mid \eta \in N, \alpha \in \text{Aut}(N) \} \]

  isomorphic to $G$ which are *regular* on $N$: a subgroup $H \subset \text{Hol}(N)$ is *regular* if the map
  \[ H \times N \longrightarrow N \times N \text{ given by } (\eta \alpha, \sigma) \longmapsto (\eta \alpha(\sigma), \sigma) \]

  is a bijection. N. P. Byott classified Hopf-Galois structures of order $pq$ and $p^2$ for all primes $p$ and $q$ in [Byo04] and [Byo96].

- It turns out that doing the above, as $G$ runs through all groups of order $p^3$, is directly related to the classification of *braces* (or *skew braces*) of order $p^3$. D. Bachiller classified *braces of abelian type* of order $p^3$ for all primes $p$ in [Bac15].
Definition (Hopf-Galois structure [Chi00])

A Hopf-Galois structure on $L/K$ consists of a finite dimensional cocommutative $K$-Hopf algebra $H$ with an action of $H$ on $L$ making $L$ into an $H$-Galois extension.

The classical Hopf-Galois structure on $L/K$ is the group ring $K[G]$, however, there may be more Hopf-Galois structures on $L/K$.

Fact (Hopf-Galois structures on $L/K$ and regular subgroups [Chi00])

Hopf-Galois structures on $L/K$ correspond bijectively to the regular subgroups $N \subset \text{Perm}(G)$ normalised by $G$, i.e., every $K$-Hopf algebra $H$ which makes $L$ into an $H$-Galois extension is of the form $L[N]^G$ for some $N$ with the above property; this $N$ is known as the type of the Hopf-Galois structures.

The relationship between $G$ and $N$ above may be reversed. In particular, if $e(G, N)$ is the number of Hopf-Galois structures on $L/K$ of type $N$, then

$$e(G, N) = \frac{|\text{Aut}(G)|}{|\text{Aut}(N)|} e'(G, N)$$

where $e'(G, N)$ is the number of regular subgroups of $\text{Hol}(N)$ isomorphic to $G$. 
Definition (Brace (Skew brace [GV17, Rum07]))

A (left) skew brace \((B, \oplus, \odot)\) is a set \(B\) with two operations \(\oplus, \odot\) such that \((B, \oplus)\) and \((B, \odot)\) are groups, and the two operations are related by

\[
a \odot (b \oplus c) = (a \odot b) \ominus a \oplus (a \odot c) \text{ for every } a, b, c \in B.
\]

A skew brace is said to have abelian type if \((B, \oplus)\) is an abelian group.

Fact (Braces and regular subgroups [GV17])

For every brace \((B, \oplus, \odot)\) the group \((B, \odot)\) can be embedded as a regular subgroup of \(\text{Hol}(B, \oplus)\) and every regular subgroup of \(\text{Hol}(B, \oplus)\) gives rise to a brace; furthermore, isomorphic braces correspond to regular subgroups which are conjugate by an element of \(\text{Aut}(B, \oplus)\).

Every group is trivially a brace. We call a brace \((B, \oplus, \odot)\) with \((B, \odot) \cong G\) and \((B, \oplus) \cong N\) a \(G\) brace of type \(N\) and let \(\tilde{e}(G, N)\) denote the number of \(G\) braces of type \(N\). Thus, to classify \(G\) braces of type \(N\), one can find the set of regular subgroups of \(\text{Hol}(N)\) isomorphic to \(G\), then extract from this set a maximal subset whose elements are not conjugate by any element of \(\text{Aut}(N)\).
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 $p^3$, then follow the procedures described in the previous slides. Up to isomorphism, there are 5 different groups of order $p^3$.

- The cyclic group $C_{p^3}$ where $\text{Aut}(C_{p^3}) \cong C_{p^2} \times C_{p-1}$.
- The elementary abelian group $C_{3^p}$ where $\text{Aut}(C_{3^p}) \cong \text{GL}_3(\mathbb{F}_p)$.
- Abelian, exponent $p^2$ group $C_p \times C_{p^2}$

$$1 \longrightarrow C_p \longrightarrow \text{Aut}(C_p \times C_{p^2}) \longrightarrow \text{UP}_2(\mathbb{F}_p) \longrightarrow 1.$$  

- Nonabelian, exponent $p^2$ group

$$M_2 = \langle \sigma, \tau \mid \sigma^{p^2} = \tau^p = 1, \sigma^{p+1} \tau = \tau \sigma \rangle$$

$$1 \longrightarrow C_p \longrightarrow \text{Aut}(M_2) \longrightarrow \text{UP}_2(\mathbb{F}_p) \longrightarrow 1.$$  

- Nonabelian, exponent $p$ group

$$M_1 = \langle \rho, \sigma, \tau \mid \rho^p = \sigma^p = \tau^p = 1, \rho \tau = \tau \rho, \sigma \rho = \rho \sigma, \rho \sigma \tau = \tau \sigma \rangle$$

$$1 \longrightarrow C_p \longrightarrow \text{Aut}(M_1) \longrightarrow \text{GL}_2(\mathbb{F}_p) \longrightarrow 1.$$
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

\[
\Theta : \text{Hol}(N) \rightarrow \text{Aut}(N) \quad \eta \alpha \mapsto \alpha.
\]

To construct regular subgroups \( H \subset \text{Hol}(N) \) with \( |\Theta(H)| = m \), 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

\[
H_2 = \langle \alpha_1, \ldots, \alpha_s \rangle \subseteq \text{Aut}(N),
\]

a subgroup of order \( \frac{|N|}{m} \) of \( N \) which may be generated by \( \eta_1, \ldots, \eta_r \in N \), say

\[
H_1 = \langle \eta_1, \ldots, \eta_r \rangle \subseteq N,
\]

general elements \( \nu_1, \ldots, \nu_s \in N \), and we consider subgroups of \( \text{Hol}(N) \) of the form

\[
H = \langle \eta_1, \ldots, \eta_r, \nu_1 \alpha_1, \ldots, \nu_s \alpha_s \rangle \subseteq \text{Hol}(N).
\]
Then search for all $v_i$ such that the group $H$ is regular, i.e., $H$ has the same size as $N$ and acts freely on $N$. For $H$ to satisfy $|\Theta(G)| = m$, it is necessary that for every relation $R(\alpha_1, \ldots, \alpha_s) = 1$ in $H_2$ we require

$$R(u_1(v_1\alpha_1)w_1, \ldots, u_s(v_s\alpha_s)w_s) \in H_1 \text{ for all } u_i, w_i \in H_1.$$ 

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

$$W(u_1(v_1\alpha_1)w_1, \ldots, u_s(v_s\alpha_s)w_s)W(\alpha_1, \ldots, \alpha_s)^{-1} \notin H_1 \text{ for all } u_i, w_i \in H_1.$$ 

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 $N$. 
Following the above procedures we can enumerated all Hopf-Galois structures on a field extension with Galois group $G$ of order $p^3$, and, as a corollary, we can classify all braces of order $p^3$ for $p > 3$. Our results are summarised in tables below (rows correspond to $G$ and columns correspond to $N$).

<table>
<thead>
<tr>
<th>$e(G, N)$</th>
<th>$C_{p^3}$</th>
<th>$C_{p^2} \times C_p$</th>
<th>$C_p^3$</th>
<th>$M_1$</th>
<th>$M_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_{p^3}$</td>
<td>$p^2$</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>$C_{p^2} \times C_p$</td>
<td>-</td>
<td>$(2p - 1)p^2$</td>
<td>-</td>
<td>-</td>
<td>$(2p - 1)(p - 1)p^2$</td>
</tr>
<tr>
<td>$C_p^3$</td>
<td>-</td>
<td>-</td>
<td>$(p^4 + p^3 - 1)p^2$</td>
<td>$(p^3 - 1)(p^2 + p - 1)p^2$</td>
<td>-</td>
</tr>
<tr>
<td>$M_1$</td>
<td>-</td>
<td>-</td>
<td>$(p^2 + p - 1)p^2$</td>
<td>$(2p^3 - 3p + 1)p^2$</td>
<td>-</td>
</tr>
<tr>
<td>$M_2$</td>
<td>-</td>
<td>$(2p - 1)p^2$</td>
<td>-</td>
<td>-</td>
<td>$(2p - 1)(p - 1)p^2$</td>
</tr>
</tbody>
</table>

**Table:** Number of Hopf-Galois structures on Galois field extensions of degree $p^3$

<table>
<thead>
<tr>
<th>$\tilde{e}(G, N)$</th>
<th>$C_{p^3}$</th>
<th>$C_{p^2} \times C_p$</th>
<th>$C_p^3$</th>
<th>$M_1$</th>
<th>$M_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_{p^3}$</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>$C_{p^2} \times C_p$</td>
<td>-</td>
<td>9</td>
<td>-</td>
<td>-</td>
<td>$4p + 1$</td>
</tr>
<tr>
<td>$C_p^3$</td>
<td>-</td>
<td>-</td>
<td>5</td>
<td>$2p + 1$</td>
<td>-</td>
</tr>
<tr>
<td>$M_1$</td>
<td>-</td>
<td>-</td>
<td>$2p + 1$</td>
<td>$2p^2 - p + 3$</td>
<td>-</td>
</tr>
<tr>
<td>$M_2$</td>
<td>-</td>
<td>$4p + 1$</td>
<td>-</td>
<td>-</td>
<td>$4p^2 - 3p - 1$</td>
</tr>
</tbody>
</table>

**Table:** Number of skew braces of order $p^3
References


