Hopf-Galois Structures on Galois Field Extensions of Degree $p^3$

Kayvan Nejabati Zenouz
University of Exeter, UK
June 20, 2017

**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, for each group $N$ of order $p^3$, all subgroups of the holomorph of $N$ $\text{Hol}(N) = N \rtimes \text{Aut}(N) = \{ \eta \alpha | \eta \in N, \alpha \in \text{Aut}(N) \}$

isomorphic to $G$ which are regular on $N$: a subgroup $H \subset \text{Hol}(N)$ is regular if the map $x \cdot \eta \mapsto (x, \eta) \cdot \alpha$ is a bijection. N. P. Byott classified Hopf-Galois structures of order $p^3$ and $p^1$ for all primes $p$ and $q$ in [Byo94] and [Byo96]. It turns out that the doing 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 $p^3$ in [Bac15].

**Hopf-Galois Structures**

**Definition (Hopf-Galois Structures)**

A Hopf-Galois structure on $L/K$ consists of a $K$-Hopf algebra $H$ with an action of $G$ on $L$ making $L$ into an $H$-Galois extension, i.e., $H$ acts on $L$ in such a way that the $K$-module homomorphism $j : L \otimes_K H \to \text{End}_K(L)$ given by $j(x \otimes y)z = xy(z)$ for $x, z \in L, y \in H$ is an isomorphism. The classical Hopf-Galois structure on $L/K$ is the group ring $K[G]$, however, there may be more Hopf-Galois structures on $L/K$.

**Fact (Hopf-Galois structures on $L/K$ and regular subgroups)**

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, where the action of $G$ on $L[N]$ is induced by the action of $G$ on $N$ by conjugation inside $\text{Perm}(G)$ and on $L$ by Galois automorphism. This $N$ is known as the type of the Hopf-Galois structure.

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 $e(G, N) = \text{Aut}(G) / e'(G, N)$ where $e'(G, N)$ is the number of regular subgroups of $\text{Hol}(N)$ isomorphic to $G$.

**Braces**

**Definition (Skew brace)**

A left skew brace $(B, \circ, \circ)$ is a set $B$ with two operations $\circ, \circ$ such that $(B, \circ)$ and $(B, \circ)$ are groups, and the two operations are related by $a \circ (b \circ c) = (a \circ b) \circ (a \circ c)$ for every $a, b, c \in B$.

A left skew brace is called abelian type, or a brace, if $(B, \circ)$ is abelian.

Braces were introduced by W. Rump [Rum07] in order to study the set-theoretic solutions of the Yang-Baxter equation which arises in mathematical physics.

**Fact (Skew braces and regular subgroups)**

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

Every group is trivially a skew brace. We call a skew brace $(B, \circ, \circ)$ with $(B, \circ) \cong G$ and $(B, \circ) \cong N$ a $G$-skew brace of type $N$ and let $\mathcal{E}(G, N)$ denote the number of $G$ braces of type $N$. Thus, to classify $G$-skew braces of type $N$, one can find the set of all regular subgroups of $\text{Hol}(N)$ which are isomorphic to $G$, then extract from this set a maximal subset whose elements are not conjugate to each other by any element of $\text{Aut}(N)$.

**Method**

Therefore, to classify the Hopf-Galois structures and braces of order $p^3$ one needs to study $\mathcal{E}(N)$, 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 $C_p$ where $\text{Aut}(C_p) \cong C_{p-1}$.
- The elementary abelian group $C_p^3$ where $\text{Aut}(C_p^3) \cong GL_3(F_p)$.
- Abelian, exponent $p^2$ group $C_p \times C_p$.
- Nonabelian, exponent $p^2$ group $M_2 = \{ (\rho, \sigma) | \rho^p = \sigma^p = 1, \rho \sigma = \sigma \rho, \rho \sigma \tau = \tau \sigma \}$.
- Nonabelian, exponent $p$ group $M_3 = \{ (\rho, \sigma, \tau) | \rho^p = \sigma^p = 1, \rho \sigma = \rho, \rho \tau = \sigma \rho \}$.

All short sequences of groups above are exact, and we have denote by $UP_2(F_p) \subset GL_2(F_p)$ the set of upper triangular matrices and $UP_2(F_p)$ its subset whose elements have upper left entry $1$.

**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 $\vartheta : \text{Hol}(N) \to \text{Aut}(N)$ $\eta \alpha \mapsto \alpha$.

although in brace theory they are organised by the size of their Socle which is the size of their intersection with $\text{Ker} \vartheta$. To construct regular subgroups $H \subset \text{Hol}(N)$ with $|\vartheta(H)| = m$, where $m$ divides $|N|$, we take a subgroup of order $m$ of $\text{Aut}(N)$ which may be generated by $\alpha_1, \ldots, \alpha_k \in \text{Aut}(N)$, say $H \alpha = \langle \alpha_1, \ldots, \alpha_k \rangle \subset \text{Aut}(N)$, a subgroup of order $m$ which may be generated by $\alpha_1, \ldots, \alpha_k \in \text{Aut}(N)$, and consider subgroups of $\text{Hol}(N)$ of the form $H = \langle \alpha_1, \ldots, \alpha_k \rangle \subset \text{Hol}(N)$.

Then search for all $\alpha_1$ 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 $|\vartheta(H)| = m$ it is necessary that for every relation $R(\alpha_1, \ldots, \alpha_k) = 1$ in $F_2$ we require $R(u_1(v_1, \alpha_1), \ldots, u_k(v_k, \alpha_k)w) \in H$, for all $u_i, w_i \in H$.

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

$W(u_1(v_1, \alpha_1), \ldots, u_k(v_k, \alpha_k)w) W(\alpha_1, \ldots, \alpha_k)^{-1} \not\in H$, for all $u_i, w_i \in H$.

However, in general there will be other conditions on $\alpha_i$ 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 $m$ of $N$. To find the non-isomorphism skew braces we need to check which one of these subgroups are conjugate to each other by elements of $\text{Aut}(N)$.

**Results**

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 skew braces of order $p^3$ for $p > 3$. Our results are summarised in tables below.

**References**

- David Stanek: Classification of braces of order $p^3$.
- Nigel P. Byott: Hopf-Galois structures on Galois field extensions of degree $p^3$.
- Wolfgang Rump: Braces, radical rings, and the quantum Yang-Baxter equation.