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

$$\mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N) = \{\eta\alpha \mid \eta \in N,\ \alpha \in \mathrm{Aut}(N)\}$$

  isomorphic to G which are *regular* on N: a subgroup $H \subset \mathrm{Hol}(N)$ 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 $N \subset \mathrm{Perm}(G)$ 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

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

where $e'(G, N)$ is the number of regular subgroups of $\mathrm{Hol}(N)$ 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 $\mathrm{Hol}(B, \oplus)$ and every regular subgroup of $\mathrm{Hol}(B, \oplus)$ gives rise to a brace; furthermore, isomorphic braces correspond to regular subgroups which are conjugate by an element of $\mathrm{Aut}(B, \oplus)$.

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 $\widetilde{e}(G, N)$ 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 $\mathrm{Hol}(N)$ isomorphic to G, then extract from this set a maximal subset whose elements are not conjugate by any element of $\mathrm{Aut}(N)$.

Therefore, to classify the Hopf-Galois structures and braces of order p^3 one needs to study $\mathrm{Aut}(N)$, classify all regular subgroups of $\mathrm{Hol}(N)$, 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 $\mathrm{Aut}(C_{p^3}) \cong C_{p^2} \times C_{p-1}$.
- The elementary abelian group C_p^3 where $\mathrm{Aut}(C_p^3) \cong \mathrm{GL}_3(\mathbb{F}_p)$.
- Abelian, exponent p^2 group $C_p \times C_{p^2}$

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

- Nonabelian, exponent p^2 group

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

$$1 \longrightarrow C_p^2 \longrightarrow \mathrm{Aut}(M_2) \longrightarrow \mathrm{UP}_2^1(\mathbb{F}_p) \longrightarrow 1.$$

- Nonabelian, exponent p group

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

$$1 \longrightarrow C_p^2 \longrightarrow \mathrm{Aut}(M_1) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p) \longrightarrow 1.$$

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

$$\Theta : \mathrm{Hol}(N) \longrightarrow \mathrm{Aut}(N) \qquad \eta\alpha \longmapsto \alpha.$$

To construct regular subgroups $H \subset \mathrm{Hol}(N)$ with $|\Theta(H)| = m$, where m divides $|N|$, we take a subgroup of order m of $\mathrm{Aut}(N)$ which may be generated by $\alpha_1, ..., \alpha_s \in \mathrm{Aut}(N)$, say

$$H_2 = \langle \alpha_1, ..., \alpha_s \rangle \subseteq \mathrm{Aut}(N),$$

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

$$H_1 = \langle \eta_1, ..., \eta_r \rangle \subseteq N,$$

general elements $v_1, ..., v_s \in N$, and we consider subgroups of $\mathrm{Hol}(N)$ of the form

$$H = \langle \eta_1, ..., \eta_r, v_1\alpha_1, ..., v_s\alpha_s \rangle \subseteq \mathrm{Hol}(N).$$

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 $R(\alpha_1, ..., \alpha_s) = 1$ in H_2 we require

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

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

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

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 $\mathrm{Aut}(N)$, 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).

$e(G,N)$	C_{p^3}	$C_{p^2} \times C_p$	C_p^3	M_1	M_2
C_{p^3}	p^2	-	-	-	-
$C_{p^2} \times C_p$	-	$(2p-1)p^2$	-	-	$(2p-1)(p-1)p^2$
C_p^3	-	-	$(p^4+p^3-1)p^2$	$(p^3-1)(p^2+p-1)p^2$	-
M_1	-	-	$(p^2+p-1)p^2$	$(2p^3-3p+1)p^2$	-
M_2	-	$(2p-1)p^2$	-	-	$(2p-1)(p-1)p^2$

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

$\widetilde{e}(G,N)$	C_{p^3}	$C_{p^2} \times C_p$	C_p^3	M_1	M_2
C_{p^3}	3	-	-	-	-
$C_{p^2} \times C_p$	-	9	-	-	$4p+1$
C_p^3	-	-	5	$2p+1$	-
M_1	-	-	$2p+1$	$2p^2-p+3$	-
M_2	-	$4p+1$	-	-	$4p^2-3p-1$

Table: Number of skew braces of order p^3

References

[Bac15] David Bachiller. Classification of braces of order p^3. *J. Pure Appl. Algebra*, 219(8):3568–3603, 2015.

[Byo96] N. P. Byott. Uniqueness of Hopf Galois structure for separable field extensions. *Comm. Algebra*, 24(10):3217–3228, 1996.

[Byo04] Nigel P. Byott. Hopf-Galois structures on Galois field extensions of degree pq. *J. Pure Appl. Algebra*, 188(1-3):45–57, 2004.

[Chi00] Lindsay N. Childs. *Taming wild extensions: Hopf algebras and local Galois module theory*, volume 80 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2000.

[GV17] L. Guarnieri and L. Vendramin. Skew braces and the Yang–Baxter equation. *Math. Comp.*, 86(307):2519–2534, 2017.

[Rum07] Wolfgang Rump. Braces, radical rings, and the quantum Yang-Baxter equation. *J. Algebra*, 307(1):153–170, 2007.