Hopf Algebras and Galois Module theory
May 24-28, 2021

# *Hopf Galois structures on separable field extensions of odd prime power degree*

Teresa Crespo, Universitat de Barcelona

May 24th, 2021

## Hopf Galois extensions

Let $L/K$ be a finite field extension, $H$ a finite cocommutative $K$-Hopf algebra. We shall say that $L/K$ is *$H$-Galois* if there exists a $K$-algebra morphism $\mu : H \to End_K(L)$ such that

$$\begin{array}{rcl} \mu(h)(xy) & = & \sum \mu(h_1)(x) \cdot \mu(h_2)(y), \text{ for } \Delta(h) = \sum h_1 \otimes h_2 \\ \mu(h)(1) & = & \varepsilon(h) \cdot 1, \end{array}$$

for $h \in H, x, y \in L$ and the $K$-linear map

$$\widehat{\mu} : L \otimes H \to End_K(L), \quad \widehat{\mu}(x \otimes h)(y) = x\mu(h)(y), h \in H, x, y \in L,$$

is an isomorphism.

We shall call $(H, \mu)$ a *Hopf Galois structure* on $L/K$.

$L/K$ is a Hopf Galois extension if it has at least one Hopf Galois structure.

**Formulation in group terms** (Greither-Pareigis)

For a finite separable extension $L/K$ of degree $n$, we denote by

$$G\left\{\begin{array}{l}\widetilde{L}\\ \Big|\; G'\\ L\\ \Big|\; n\\ K\end{array}\right.$$

$\widetilde{L}$ normal closure of $L/K$,

$G = \mathrm{Gal}(\widetilde{L}/K), G' = \mathrm{Gal}(\widetilde{L}/L)$,

$G/G'$ left cosets.

$G$ acts on $G/G' : g \cdot hG' = (gh)G'$

$\lambda : G \hookrightarrow \mathrm{Sym}(G/G') \simeq S_n$.

**Theorem** (Greither-Pareigis) *There is a one-to-one correspondence between the set of isomorphism classes of Hopf Galois structures $(H, \mu)$ on $L/K$ and the set of regular subgroups $N$ of* $\mathrm{Sym}(G/G')$ *normalized by $\lambda(G)$.*

The isomorphism class of $N$ will then be called *type* of the Hopf Galois structure.

If $N$ is a regular subgroup of $\mathrm{Sym}(G/G')$ normalized by $\lambda(G)$, the corresponding Hopf Galois structure $(H, \mu)$ is

$$H = \widetilde{L}[N]^G, \quad \mu \text{ obtained from } \eta \cdot x = \eta^{-1}(1_G)(x), \text{ for } \eta \in N, x \in \widetilde{L}.$$

**Theorem.** (Childs, Byott) *Let $G$ be a finite group, $G' \subset G$ a subgroup and $\lambda : G \hookrightarrow \mathrm{Sym}(G/G')$ the morphism given by the action of $G$ on the left cosets $G/G'$. Let $N$ be a group of order $[G : G']$ with identity element $1_N$. Then there is a bijection between*

$$\mathcal{N} = \{\alpha : N \hookrightarrow \mathrm{Sym}(G/G') \text{ such that } \alpha(N) \text{ is regular}\}$$

*and*

$$\mathcal{G} = \{\beta : G \hookrightarrow \mathrm{Sym}(N) \text{ such that } \beta(G') \text{ is the stabilizer of } 1_N\}$$

*Under this bijection, if $\alpha, \alpha' \in \mathcal{N}$ correspond to $\beta, \beta' \in \mathcal{G}$, respectively, then $\alpha(N) = \alpha'(N)$ if and only if $\beta(G)$ and $\beta'(G)$ are conjugate by an element of $\mathrm{Aut}(N)$; if $\alpha \in \mathcal{N}$ corresponds to $\beta \in \mathcal{G}$, then $\alpha(N)$ is normalized by $\lambda(G)$ if and only if $\beta(G)$ normalizes $\lambda(N)$.*

The normalizer of $\lambda(N)$ in $\mathrm{Sym}(N)$ is equal to $\rho(N) \cdot \mathrm{Aut}(N)$ and is isomorphic to $\mathrm{Hol}(N) := N \rtimes \mathrm{Aut}\, N$, the holomorph of $N$.

**Hopf Galois structures of abelian type.**

**Theorem 1.** *A separable field extension of degree $p^n$, with $p$ a prime number, $n \geq 3$, $p > n$, has at most one abelian type of Hopf Galois structures.*

Theorem 1 generalizes Caranti, Childs and Featherstonhaugh (2012).

**Lemma 1.1.** *Let $G$ be a subgroup of $\mathrm{Hol}(N)$, for $N$ a group of order $p^n$. Then $G$ is transitive if and only if $\mathrm{Syl}_p(G)$ is transitive.*

**Lemma 1.2.** *Let $N$ be an abelian group of order $p^n$, $p > n$, $G$ a transitive subgroup of $\mathrm{Hol}(N)$, of order $|G| = p^m, m \geq n$.*
*We consider the surjective map*

$$\pi : G \to N, \quad (a, \varphi) \mapsto a.$$

*If $\pi(a, \varphi) = a$, then*

$$a^{p^k} = e_N \Leftrightarrow (a, \varphi)^{p^k} \in \mathrm{Stab}_{\mathrm{Hol}(N)}(e_N).$$

*Proof of Theorem 1.*

Let $L/K$ be a separable field extension, $[L:K]=p^n$, $\widetilde{L}$ normal closure of $L/K$, $G=\mathrm{Gal}(\widetilde{L}/K), G'=\mathrm{Gal}(\widetilde{L}/L)$.

Assume that $L/K$ has a Hopf Galois structure of abelian type $N$. Then

$$\beta : G \to \mathrm{Hol}(N), \text{ with } \beta(G') = \mathrm{Stab}_{\mathrm{Hol}(N)}(e_N).$$

By Lemma 1.1, we may assume that the order of $G$ is a $p$-power.

$$\pi : \mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N) \to N.$$

The composition $\pi \circ \beta$ is surjective and, for $x \in G$, Lemma 1.2 gives

$$x^{p^k} \in G' \Leftrightarrow (\pi \circ \beta)(x)^{p^k} = e_N.$$

*Idea of the proof of Lemma 1.2*

For $(a,\varphi),(b,\psi) \in \mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N)$, $(a,\varphi)(b,\psi) = (a\varphi(b), \varphi\psi)$.

For $(a,\varphi) \in \mathrm{Hol}(N)$,

$$(a,\varphi)^{\ell} = ((\mathrm{Id} + \varphi + \cdots + \varphi^{\ell-1})(a), \varphi^{\ell}) \tag{1}$$

$\gamma : G \to \mathrm{Aut}(N)$ is a group morphism. Assume $(a,\varphi) \in G$.

$\delta := -\mathrm{Id} + \varphi \in \mathrm{End}(N)$. For $b \in N$, $\delta(b) = b^{-1}\varphi(b) = [b, \varphi^{-1}] \in [N, \gamma(G)]$.
Then $\delta^n = 0 \in \mathrm{End}(N)$.

Write (1) in terms of $\delta$ with $\ell = p$:

$$(a,\varphi)^p = ((p\,\mathrm{Id} + \binom{p}{2}\delta + \cdots + \binom{p}{n}\delta^{n-1})(a), \varphi^p).$$

If $a$ has order $p$ in $N$, $(p\,\mathrm{Id} + \binom{p}{2}\delta + \cdots + \binom{p}{n}\delta^{n-1})(a) = e_N$, which gives $(a,\varphi)^p \in \mathrm{Stab}_{\mathrm{Hol}(N)}(e_N)$.

**Remark.** Condition $p > n$ in Theorem 1 is necessary. For example,

a Galois extension with Galois group $C_9 \times C_3 \times C_3$ has Hopf Galois structures of types $C_9^2$ and $C_3^4$;

a Galois extension with Galois group $C_3^4$ has Hopf Galois structures of type $C_9 \times C_3 \times C_3$.

**Hopf Galois structures of nonabelian type.**

Let $N$ be a group of order $p^n$ such that $[N,N]$ has order $p$. We put $[N,N]=\langle c\rangle$.

$$N/[N,N]=\oplus_{i=1}^{s}\langle b_i\rangle,\quad \pi:N\to N/[N,N],\quad \beta_i\in\pi^{-1}(b_i).$$

$$\beta_i\beta_j\beta_i^{-1}\beta_j^{-1}=c^k, k\in\mathbb{Z}\Rightarrow(\beta_i\beta_j)^p=\beta_i^p\beta_j^p.$$

Define an abelian group $A$ of order $p^n$, such that $A$ has the same number of elements of order $p^m$ as $N$, for $1\leq m\leq n$.

If $\operatorname{ord}(\beta_i)=\operatorname{ord}(b_i), \forall i=1,\dots,s, A:=\oplus_{i=1}^{s}\langle\alpha_i\rangle\oplus\langle d\rangle$, $\operatorname{ord}(\alpha_i)=\operatorname{ord}(\beta_i), \operatorname{ord}(d)=p$,

If $\exists i_0:\operatorname{ord}(\beta_{i_0})=p\operatorname{ord}(b_{i_0}), A:=\oplus_{i=1}^{s}\langle\alpha_i\rangle$, $\operatorname{ord}(\alpha_i)=\operatorname{ord}(\beta_i)$. Define $d:=\alpha_{i_0}^{\operatorname{ord}(\alpha_{i_0})/p}$.

$$A/\langle d\rangle\simeq N/[N,N]$$

**Theorem 2.** *Let $N$ and $A$ be groups of order $p^n$ as above. If a separable field extension of degree $p^n$ has a Hopf Galois structure of type $N$, then it has a Hopf Galois structure of type $A$.*

*Proof.* We define automorphisms $\varphi_i, 1 \leq i \leq s$, of $A$ by

$$\varphi_i(d) = d,\ \varphi_i(\alpha_j) = d^{k/2}\alpha_j \text{ if } \ \beta_i\beta_j\beta_i^{-1} = c^k\beta_j, 0 \leq k < p.$$

$$N' := \langle \{(\alpha_i, \varphi_i)\}_{1 \leq i \leq s} \cup \{d\} \rangle.$$

$N'$ is a regular subgroup of $\mathrm{Hol}(A)$ isomorphic to $N$.

$$A \subset \mathrm{Nor}_{\mathrm{Hol}(A)}(N')$$

The bijection $f : A \to N, d^r \prod \alpha_i^{r_i} \mapsto c^r \prod \beta_i^{r_i}$ induces a group monomorphism

$$\widetilde{f} : \mathrm{Aut}\, N \to \mathrm{Aut}\, A, \chi \mapsto \widetilde{\chi} := f^{-1} \circ \chi \circ f.$$

$$\widetilde{f}(\mathrm{Aut}\, N) \subset \mathrm{Nor}_{\mathrm{Hol}(A)}(N').$$

$$|\,\mathrm{Nor}_{\mathrm{Hol}(A)}(N')| = |\mathrm{Hol}(N')|$$

**Examples.** Theorem 2 may be applied for instance to the following pairs of groups.

1) $N = C_{p^{n-1}} \rtimes C_p$, $A = C_{p^{n-1}} \times C_p$, for $n \geq 3$;

2) $N = \langle a, b : a^{p^n} = 1, b^{p^n} = 1, bab^{-1} = a^{1+p^{n-1}} \rangle$, $A = C_{p^n} \times C_{p^n}$, for $n \geq 2$;

3) $N = \langle a, b, c : a^{p^n} = 1, b^p = 1, c^p = 1, bab^{-1} = a, cac^{-1} = a, cbc^{-1} = ba^{p^{n-1}} \rangle$, $A = C_{p^n} \times C_p \times C_p$, for $n \geq 2$;

4) $N = \langle a, b, c : a^{p^n} = 1, b^p = 1, c^p = 1, bab^{-1} = a, cac^{-1} = a^{1+p^{n-1}}, cbc^{-1} = b \rangle$, $A = C_{p^n} \times C_p \times C_p$, for $n \geq 2$;

5) $N = \langle a, b, c : a^{p^n} = 1, b^p = 1, c^p = 1, bab^{-1} = a, cac^{-1} = ab, cbc^{-1} = b \rangle$, $A = C_{p^n} \times C_p \times C_p$, for $n \geq 2$.

**Remark.** The condition $|[N,N]| = p$ in Theorem 2 is necessary. The groups

$$N := \langle a, b, c : a^{p^2} = 1, b^p = 1, c^p = 1, bab^{-1} = a^{1+p}, cac^{-1} = ab, cbc^{-1} = b \rangle,$$

$$A := C_{p^2} \times C_p \times C_p$$

have the same number of elements of order $p^2$, namely $p^4 - p^3$, but

$$[N, N] = \langle a^p, b \rangle$$

has order $p^2$.

For $p = 5$, we have checked with Magma that $\mathrm{Hol}(A)$ has regular subgroups isomorphic to $N$ but the order of their normalizers in $\mathrm{Hol}(A)$ is not equal to the order of $\mathrm{Hol}(N)$.