Subextension techniques to describe Hopf-Galois structures

Teresa Crespo **Anna Rio** Montse Vela

Math Department

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

14 March 2019

Hopf-Galois Project in Barcelona

Montse Vela

Teresa Crespo

Hopf Galois Extensions

K/k finite

K/k Hopf-Galois

$$\Updownarrow$$

There exist

- a $k-$Hopf algebra H of finite dimension
- a Hopf action $\mu : H \longrightarrow End_k(K)$ (K *is* H*-module*)

such that

$$(1, \mu) : K \otimes_k H \longrightarrow End_k(K) \text{ isomorphism}$$

$$\Longrightarrow \dim H = [K : k]$$

Hopf Galois Extensions

K/k Galois

$$\Updownarrow$$

$(1, \mu) : K \otimes_k k[G] \to End_k(K)$ isomorphism

with $(1, \mu)(s \otimes h)(t) = s \cdot (\mu(h)(t))$

Non-unicity: a Hopf Galois extension can have different Hopf Galois structures (H, μ)

Crespo, T.; Rio, A.; Vela, M.: Non-isomorphic Hopf Galois structures with isomorphic underlying Hopf algebras, J. Algebra 422 (2015), 270-276.

Separable Hopf Galois Extensions

K/k separable

- $\widetilde{K}/k$ normal closure K/k
- $G = Gal(\widetilde{K}/k) \qquad G' = Gal(\widetilde{K}/K)$

Provide the information on the Hopf Galois character of K/k

Greither-Pareigis

K/k Hopf Galois $\Leftrightarrow \exists$ regular subgroup $N \subseteq Sym(G/G')$ normalized by $\lambda(G)$

$\lambda(G), \rho(G)$ image of G under left,right regular reperesentation

Separable Hopf Galois Extensions

Let K/k be a separable field extension, then there is a one-to-one correspondence between

1. Hopf-Galois structures on K/k
2. regular subgroups $N \subseteq Sym(G/G')$ normalized by $\lambda(G)$

K/k Galois non abelian, at least two different structures: classical $N = \rho(G)$ and non classical $N = \lambda(G)$

Hopf Galois structures enumeration: problem in group theory.

Separable Hopf Galois Extensions

Hopf algebra attached (twist of a group algebra)

$$H = \widetilde{K}[N]^G$$

G acts on $\widetilde{K}$ as automorphism group
$\lambda(G)$ acts on N via conjugation

H is a $\widetilde{K}$-form of $\widetilde{K}[N]$:

$$H \otimes_k \widetilde{K} \simeq \widetilde{K}[N]$$

Hopf action $\mu : H \longrightarrow End_k(K)$

$$(\sum_{n\in N} c_n n) \cdot x = \sum_{n\in N} c_n \; n^{-1}(\,\overline{1}_G\,)(x)$$

Almost classical Hopf Galois extensions

K/k almost classical if G' has normal complement N in G
($G = N \rtimes G'$)

Example $[K:k] = n$ and $G \simeq D_{2n}$
$N \simeq C_n$

Example $G \simeq$ Frobenius group
$G' \simeq$ Frobenius *complement*
$N =$ Frobenius *kernel*

Byott's reformulation

Bijection between

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

and

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

- If $\alpha, \alpha' \in \mathcal{N} \leftrightarrow \beta, \beta' \in \mathcal{G}$
  $\alpha(N) = \alpha'(N) \iff \beta(G) = \sigma\beta'(G)\sigma^{-1}$ with $\sigma \in \mathrm{Aut}(N)$
- $\alpha(N)$ normalized by $\lambda(G) \iff \beta(G) \subset Hol(N)$

$Hol(N) = N \rtimes \mathrm{Aut}(N)$

$$(g, \sigma)(h, \tau) = (g\sigma(h), \sigma\tau)$$

Procedure

Input $n = [K : k]$ $G = Gal(\widetilde{K}/k)$

Conjugacy class of $G' = Gal(\widetilde{K}/K)$

- G' has normal complement N in G?
- N (type) runs over a system of representatives of isomorphism classes of groups of order n
- Compute $Hol(N) \subseteq S_n$ (Magma)
- $\beta(G) \subseteq Hol(N)$?

Hopf Galois property for intermediate extensions

$$K \subseteq F \subseteq \tilde{K}$$

How does the Hopf Galois character of K/k rule the Hopf Galois character of F/k?

$\tilde{K}$ Galois $\Rightarrow$ Hopf-Galois

G' ¿ ?

K Hopf-Galois or not

n

k

n=4,5,6,7 Hopf Galois in small degree

n=6

	Name	$\|G\|$	K/k
$6T1$	C_6	6	Galois
$6T2$	S_3	6	Galois
$6T3$	$D_{2\cdot 6}$	12	almost classical
$6T4$	A_4	12	not Hopf-Galois
$6T5$	F_{18}	18	almost classical
$6T6$	$2A_4$	24	not Hopf Galois
$6T7$	$S_4(6d)$	24	not Hopf Galois
$6T8$	$S_4(6c)$	24	not Hopf Galois
$6T9$	$F_{18}:2$	36	almost classical
$6T10$	F_{36}	36	not Hopf Galois
$6T11$	$2S_4$	48	not Hopf Galois
$6T12$	A_5	60	not Hopf Galois
$6T13$	$F_{36}:2$	72	not Hopf Galois
$6T14$	S_5	120	not Hopf Galois
$6T15$	A_6	360	not Hopf Galois
$6T16$	S_6	720	not Hopf Galois

http://galoisdb.math.upb.de

Degree 6 with Galois group A_4 is not Hopf-Galois

$$f(x) = x^6 - 3x^2 - 1$$

12 is the minimum $|G|$ of an extension K/k not Hopf-Galois

- G' has not normal complement: A_4 has not degree 6 subgroup
- Possible types: C_6 and S_3
- $Hol(C_6) \simeq D_{2\cdot 6}$ and $Hol(S_3) \simeq S_3 \times S_3$
- $S_3 \times S_3$ has not subgroup isomorphic to A_4

 Intermediate extensions

$$\begin{array}{c} \tilde{K} = \tilde{F} \\ | \\ F \\ | \\ K \\ {}_n| \\ k \end{array}$$

F/k Hopf Galois?

$n = 4 \qquad G = S_4$

If $[F : k] = 12$, $Gal(\tilde{K}/F)$ has normal complement $N = A_4$
F/k almost classical

If $[F : k] = 8$, $G \subset Hol(C_2 \times C_2 \times C_2)$
F/k Hopf Galois not almost classical

n=6 $\quad Gal(\widetilde{K}/k) \simeq F_{18}:2 \simeq S_3 \times S_3 \simeq Hol(S_3)$

$$k \subset K \subset F \subset \widetilde{K}$$

K/k	$[F:k]$	F/k	N
Hopf Galois	12	Hopf Galois not almost classical	$D_{2\cdot 6}$
Hopf Galois	18	Hopf Galois almost classical	$S_3 \times C_3$

$n = 4, 5, 6, 7$

- Complete study of intermediate extensions $K \subseteq F \subseteq \tilde{K}$
- With K/k Hopf-Galois, we always obtained F/k Hopf-Galois

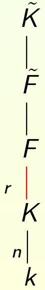
T. Crespo, A. Rio, M. Vela, *From Galois to Hopf Galois: Theory and Practice*, Contemporary Mathematics, 649 (2015)

T. Crespo, A. Rio, M. Vela, *The Hopf Galois property in subfield lattices*. Comm. Algebra, 44 (2016), 1, 336-353

Theorem on transitivity

K/k separable, $\tilde{K}$ normal closure, $G = Gal(\tilde{K}/k)$, $G' = Gal(\tilde{K}/K)$
Let us assume that G' has normal complement in G
Then, for intermediate $K \subseteq F \subseteq \tilde{K}$

K/k and F/K Hopf Galois $\Longrightarrow$ F/k Hopf Galois



$\tilde{F}$ closure of F/K, $\tilde{F} \subseteq \tilde{K}$

R regular subgroup of $Sym(\, Gal(\tilde{F}/K)/Gal(\tilde{F}/F)\,) \simeq S_r$ normalized by $Gal(\tilde{F}/K)$

N regular subgroup of $Sym(G/G') \simeq S_n$ normalized by G

$N \times R$ regular subgroup of $Sym(\, G/Gal(\tilde{K}/F)\,) \simeq S_{nr}$ normalized by G

Relative Hopf Galois

Is the condition F/K Hopf Galois redundant? No

$Hol(A_5) = A_5 \rtimes \mathrm{Aut}(A_5) = A_5 \rtimes S_5$ has a subgroup G of order 3600 which is a transitive subgroup of S_{60}: $\langle \tau, \sigma \rangle$

$$\begin{aligned}
\tau &= (1,53)(2,55)(3,54)(4,34)(5,14)(6,42)(7,57)(8,12)(9,11)(10,13)\\
&\quad (16,43)(17,45)(18,44)(20,29)(21,52)(23,37)(24,36)(25,38)(26,59)\\
&\quad (27,58)(28,60)(30,40)(31,48)(32,50)(33,49)(35,39)(41,51)(47,56)\\
\sigma &= (1,45,49,6,4)(2,5,37,15,34)(3,25,60,59,19)(7,27,16,14,29)\\
&\quad (8,23,31,51,9)(10,58,39,11,47)(12,43,54,13,24)(18,38,40,52,42)\\
&\quad (20,48,55,33,46)(22,26,36,30,50)(28,56,32,41,57).
\end{aligned}$$

$\widetilde{K}/\mathbb{Q}$ Galois with group S_{60} $\quad k = \widetilde{K}^G$ $\quad G' = \mathrm{Stab}_G(i)$ $\quad K = \widetilde{K}^{G'}$

$Gal(\widetilde{K}/k) = G \subset Hol(A_5) \subset S_{60} \implies K/k$ Hopf Galois

$G' \simeq A_5$ $\quad G'' \subset G'$ of order 12 $\quad F = \widetilde{K}^{G''}$

F/K separable degree 5 with Galois group $A_5 \implies F/K$ not Hopf Galois

Relative Hopf Galois

Is the condition F/K Hopf Galois redundant? No

$Hol(A_5) = A_5 \rtimes \mathrm{Aut}(A_5) = A_5 \rtimes S_5$ has a subgroup G of order 3600 which is a transitive subgroup of S_{60}: $\langle \tau, \sigma \rangle$

$$\begin{aligned}
\tau &= (1,53)(2,55)(3,54)(4,34)(5,14)(6,42)(7,57)(8,12)(9,11)(10,13) \\
&\quad (16,43)(17,45)(18,44)(20,29)(21,52)(23,37)(24,36)(25,38)(26,59) \\
&\quad (27,58)(28,60)(30,40)(31,48)(32,50)(33,49)(35,39)(41,51)(47,56) \\
\sigma &= (1,45,49,6,4)(2,5,37,15,34)(3,25,60,59,19)(7,27,16,14,29) \\
&\quad (8,23,31,51,9)(10,58,39,11,47)(12,43,54,13,24)(18,38,40,52,42) \\
&\quad (20,48,55,33,46)(22,26,36,30,50)(28,56,32,41,57).
\end{aligned}$$

$\widetilde{K}/\mathbb{Q}$ Galois with group S_{60} $\quad k = \widetilde{K}^G \quad G' = \mathrm{Stab}_G(i) \quad K = \widetilde{K}^{G'}$

$Gal(\widetilde{K}/k) = G \subset Hol(A_5) \subset S_{60} \implies K/k$ Hopf Galois

$G' \simeq A_5 \quad G'' \subset G'$ of order 12 $\quad F = \widetilde{K}^{G''}$

F/K separable degree 5 with Galois group $A_5 \implies F/K$ not Hopf Galois

Composition of Hopf Galois extensions

Theorem concerns intermediate extensions between K and its closure $\widetilde{K}$

$k = \mathbb{Q} \qquad K = \mathbb{Q}(\sqrt{5})$

- $K/\mathbb{Q}$ Galois $\Longrightarrow$ Hopf Galois
- F/K cubic $\Longrightarrow$ Hopf Galois

$$y^3 - 3(1+\sqrt{5})y^2 + \frac{9}{2}(5+3\sqrt{5})y - \frac{27}{2}(1+\sqrt{5}) \in K[y]$$

- Composition $F/\mathbb{Q}$ of degree 6

$$x^6 - 6x^5 + 9x^4 + 243x^3 - 729x^2 + 1215x - 729 \in \mathbb{Q}[x]$$

Galois group $F_{36} \Longrightarrow F/\mathbb{Q}$ not Hopf Galois

Example: Frobenius family

$$
\begin{array}{c}
\tilde{K} \\
{\scriptstyle G'_d}\big| \\
K_d \\
{\scriptstyle d}\big| \\
K_0 \\
{\scriptstyle p}\big| \\
k
\end{array}
$$

$p \geq 5$

$G = Gal(\tilde{K}/k) = F_{p(p-1)}$ Frobenius group

$G' = Gal(\tilde{K}/K_0)$ a Frobenius complement

$d|p-1$ proper divisor

$G'_d \subset G'$ index d subgroup

- K_0/k prime degree and its closure has solvable Galois group
- K_d/K_0 is Galois since $\tilde{K}/K_0$ is cyclic

Thm $\implies$ All the K_d/k are Hopf Galois extensions (type $C_d \times C_p$)

Example: Frobenius family

1. K_d/k almost classical $\iff gcd(\frac{p-1}{d}, d) = 1$
2. K_d/k has Hopf Galois structure of cyclic type C_{pd} and of Frobenius type F_{pd}
3. Almost classical structures are of Frobenius type
4. For both types Galois correspondence is one-to-one

There exist Hopf Galois extensions which are not almost classically Galois but may be endowed with a Hopf Galois structure such that the Galois correspondence is one-to-one.

Crespo, T.; Rio, A.; Vela, M.: On the Galois correspondence theorem in separable Hopf Galois theory, Publ. Mat. 60 (2016) 221-234.

Induced Hopf Galois structures

K/k Galois
$G = Gal(K/k)$
$G' = Gal(K/F)$

$$\begin{array}{c} K \\ | \\ F \\ | \\ k \end{array}$$

Assume G' has normal complement in G

If N_1 gives a Hopf Galois structure for F/k and N_2 gives a Hopf Galois structure for K/F, then

$$N_1 \times N_2 \subseteq Sym(G/G') \times Sym(G') \subseteq Sym(G)$$

gives a Hopf Galois structure for K/k Induced

Crespo, T; Rio, A; Vela, M: Induced Hopf Galois structures. J. Algebra 457 (2016) 312-322.

Induced Hopf Galois structures

A Galois extension K/k with Galois group $G = G_1 \rtimes G'$ has at least one split Hopf Galois structure of type $G_1 \times G'$

$$\lambda(G_1) \times \rho(G') \subset Sym(G)$$

Split structures are induced

Assume

- K/k Galois with Hopf Galois structure $N_1 \times N_2$
- N_1, N_2 are $G-$stable
- $F = K^{N_2}$ and $G' = Gal(K/F)$
- G' has normal complement in G

Then,

N_2 gives a Hopf Galois structure for K/F, N_1 gives a Hopf Galois structure for F/k and the given Hopf Galois structure of K/k is induced by those two.

Induced Hopf Galois structures. Examples

- Galois extensions with group $G = S_3 = C_3 \rtimes C_2$ have Hopf Galois structures of type $N = C_6$
- Galois extensions with group $G = D_{2n} = C_n \rtimes C_2$ have Hopf Galois structures of type $N = C_n \times C_2$
- Galois extensions with group $G = S_n = A_n \rtimes C_2$ have Hopf Galois structures of type $N = A_n \times C_2$
- Galois extensions with group $G = A_4 = V_4 \rtimes C_3$ have Hopf Galois structures of type $N = V_4 \times C_3$
- Galois extensions with group $G = Hol(M)$ have Hopf Galois structures of type $N = M \times Aut(M)$
- Galois extensions with group G a Frobenius group have Hopf Galois structures of type Frobenius kernel $\times$ Frobenius complement
- Galois extensions with group of order $2p^k$ ($p \geq 3$) or $4p^k$ ($p \geq 5$) have split extensions induced from the unique p–Sylow subgroup

Split non induced

$$G = \{\pm 1, \pm i, \pm j \pm k\} = \langle i, j \rangle \simeq H_8$$

$$\lambda(i) = (1, i, -1, -i)(j, k, -j, -k) = (1, i, i^2, i^3)(j, ij, i^2j, i^3j)$$
$$\lambda(j) = (1, j, -1, -j)(i, -k, -i, k) = (1, j, i^2, i^2j)(i, i^3j, i^3, ij)$$

$$\lambda(G) = \langle \lambda(i),\ \lambda(j) \rangle \subset Sym(G)$$

normalizes

$$N = \langle (1, i^2)(i, i^3)(j, i^2j)(ij, i^3j),\ (1, i^3)(i, i^2)(j, ij)(i^2j, i^3j), (1, i^3j)(i, j)(i^2, ij)(i^3, i^2j) \rangle$$

regular subgroup of $Sym(G)$ isomorphic to $C_2 \times C_2 \times C_2$

Enumeration

- $e(A_4) = e(A_4, A_4) + e(A_4, V_4 \times C_3)$
  $e(A_4, A_4) = 10$ (Carnahan, Childs)
  $e(A_4, V_4 \times C_3) \geq 4$ (Induction)
- G non abelian group of order $4p$ ($p \geq 5$)
  G' its 2−Sylow subgroup. It has normal complement in G
  From Kohl, number of abelian split structures:

	Type $C_4 \times C_p$	Type $V_4 \times C_p$
$G' \simeq C_4$	p	p
$G' \simeq V_4$	$3p$	p

  All of them are induced

Enumeration

- Galois group G of order pq $(p > q)$
  - $q \nmid p-1 \implies$ order is a Burnside number and the classical one is the unique Hopf Galois structure (Byott)
  - assume $q \mid p-1$
    1. $G \simeq C_{pq}$.
       one split structure, the classical one, and $2q-2$ nonsplit structures of type $C_p \rtimes C_q$
    2. $G \simeq C_p \rtimes C_q$ Unique p–Sylow and p different q–Sylows G'
       Each G' unique induced (split) Hopf Galois structure

Obtain p induced structures of cyclic type $C_p \times C_q$

According to Byott results, all the split structures

Particular case: D_{2p}

Enumeration

- p a safe prime: $p = 2q + 1$, q prime (Byott, Childs)

  K/k Galois with group a Frobenius $F_{p(p-1)}$.

  Assume $q > 2$, otherwise case $4p = 20$

  G has

  - one p–Sylow
  - p conjugate subgroups G' cyclic of order $p - 1 = 2q$

  $K/K^{G'}$ has

  - classical structure (cyclic)
  - 2 Hopf Galois structures of dihedral type (Byott)

$\Longrightarrow$ K/k has

- p induced structures of type $C_{p-1} \times C_p$
- $2p$ of type $D_{p-1} \times C_p$

All split Hopf Galois structures are induced

Normality

- $G = Gal(K/k)$
- $N \subseteq Sym(G)$ regular subgroup giving Hopf Galois structure for K/k
- $P \triangleleft N$ stable under $\lambda(G)$ conjugation
- F/k intermediate extension corresponding to P under Hopf Galois correspondence
- $J = Gal(K/F)$

Assume J is a normal subgroup of G

Then, N/P provides a Hopf Galois structure for F/k

A. Koch, T. Kohl, P.J. Truman, R. Underwood: Normality and short exact sequences of Hopf-Galois structures, Communications in Algebra, 2019.

Combine induction and reduction

- $G = Gal(K/k)$ order n
- G' index d and such that $\bigcap_g gG'g^{-1} = 1$
- N order n having unique subgroup N' of index d ($\Longrightarrow$ normal)

If N provides a Hopf Galois structure for K/k,
N' is stable under $\lambda(G)$ conjugation
F the corresponding subfield under the Hopf Galois correspondence

If we know that a separable extension of degree d with Galois group G has not Hopf Galois structures of type N/N', then we get a contradiction

G can't have Hopf Galois structures of type N.

A_4

- Assume $Gal(K/k) \simeq A_4$
- 5 possible Hopf Galois types: alternating A_4, dicyclic $C_3 \rtimes C_4$, cyclic $C_{12} = C_3 \times C_4$, dihedral $D_{12} = C_3 \rtimes V_4$, direct product $C_3 \times V_4$
- Classical $\implies A_4$ type
- $A_4 = V_4 \rtimes C_3 \implies$ induced $C_3 \times V_4$ type
- Since $Hol(Dic_3) = Hol(D_{12})$, we are left with cyclic and dicyclic types

N' the 3−Sylow subgroup $\implies N/N' \simeq C_4$

$Hol(C_4)$ has order 8. An extension of degree 4 with Galois closure A_4 has not Hopf Galois structures of type C_4

K/k has not cyclic, dicyclic or dihedral Hopf Galois types

S_4

- Assume $Gal(K/k) \simeq S_4$
- 15 different possible types
- n_3 number of $3-$Sylow subgroups
  - $n_3 = 1 \implies$ type is $C_3 \rtimes S$, S a group of order 8. 12 types
  - $n_3 = 4 \implies$ types S_4, $SL(2,3)$ and $A_4 \times C_2$
- F/k degree 8 with normal closure $S_4 \implies$ only Hopf Galois type $C_2 \times C_2 \times C_2$ (Crespo, Salguero)
- Normality $\implies$ Rule out 9 types
- $S_4 = A_4 \rtimes C_2 \implies$ induced structures of type $A_4 \times C_2$
- $S_4 = V_4 \rtimes S_3 \implies$ induced strucutures of types $S_3 \times V_4$ and $C_6 \times V_4$
- $Hol(SL(2,3))$ has not subgroup isomorphic to S_4

A_4 and S_4

$$Gal(K/k) = A_4, S_4$$

The Hopf Galois structures are the classical one and induced structures

$C_3 \times V_4$ for the alternating group

$C_6 \times V_4,\ S_3 \times V_4,\ C_2 \times A_4$ for the symmetric group

Crespo, T.; Rio, A.; Vela, M.: Hopf Galois structures on symmetric and alternating extensions. New York J. Math. 24 (2018) 451-457.

A_5

- Assume $Gal(K/k) \simeq A_5$
- 13 different possible types
- $N \neq A_5$ has a unique 5−Sylow subgroup N'
- Groups of order 12 have holomorph of order not divisible by 60

The only type of Hopf Galois structures on K/k is A_5

Classical Galois structure realizes this type

(Byott) A Galois extension K/k with Galois group a non-abelian simple group G has exactly two Hopf Galois structures: the Galois one and the classical non-Galois one.

S_5

- Assume $Gal(K/k) \simeq S_5$
- 47 different possible types
- There are induced structures of type $A_5 \times C_2$
- $N \neq SL(2,5)$ has a unique $p-$Sylow subgroup N' $(p = 2, 3, 5)$
- Extensions of degree 15,24,40 with normal closure S_5 are not Hopf Galois
- $Hol(SL(2,5))$ has not transitive subgroup isomorphic to S_5

The only types of Hopf Galois structures on K/k are S_5 and the split one $A_5 \times C_2$

The classical Galois structure realizes the first type and the second type is realized as the induced Hopf Galois structure by an almost classical Hopf Galois structure on $K^{\langle\tau\rangle}/k$, where τ denotes a transposition in S_5.

S_5

Carnahan, Childs
$e(S_n, S_n) =$ twice the number of even permutations in S_n of order at most 2
$e(S_n, A_n \times C_2) =$ twice the number of odd permutations in S_n of order 2.

Corollary

A Galois field extension with Galois group S_5 has precisely 52 Hopf Galois structures: 32 of type S_5 and 20 of type $A_5 \times C_2$

$S_n \quad n \geq 5$

Holomorph of a cyclic group is a solvable group

$$\Downarrow$$

a Galois extension with Galois group S_n $(n > 5)$ has not Hopf Galois structures of cyclic type

Byott's query: extension with nonsolvable Galois group admits a Hopf Galois structure of solvable type?